Master Innovation & Development Plan

Digital Innovation Appendix

AUTHOR: Sidewalk Labs

ABSTRACT:

The Digital Innovation Appendix (DIA) provides updates to the Master Innovation and Development Plan (MIDP) which reflects the Threshold Issues resolution process. The DIA also provides further detailed information on the digital innovation proposals included in the MIDP, and provides an overview of Sidewalk Labs' approaches to responsible data use and inclusive design. The DIA also includes additional information on enabling the growth of the Canadian urban innovation ecosystem, and provides an overview of Canadian and international policies and approaches for smart cities and digital governance.

Digital Innovation Appendix (DIA)

Document purpose

This Digital Innovation Appendix (DIA), delivered to Waterfront Toronto and its Digital Strategy Advisory Panel (DSAP) on November 14, 2019, aims to accomplish two things:

1. Provide the latest information on the digital innovation components of the Sidewalk Labs draft proposal, *Toronto Tomorrow* — the draft Master Innovation and Development Plan (MIDP) — including updates that have resulted from discussions with Waterfront Toronto
2. Address requests from experts and the public for more information and context about the digital innovation components of the proposal

The primary audience for this document are expert reviewers of the proposal, including Waterfront Toronto and Waterfront Toronto's DSAP (an advisory body made up of Canadian leaders across disciplines), as well as interested members of the public. The review that DSAP performs will be based on this document, along with supplemental materials from Waterfront Toronto and references to the original proposal when appropriate.

Waterfront Toronto has confirmed that, as part of the next round of public consultation, they will be generating materials to explain and seek engagement on the digital innovation components of the proposal.

TABLE OF CONTENTS

Note: In this document, we have referred readers to links to third-party websites that are not owned or maintained by Sidewalk Labs. Therefore, we cannot guarantee that these linked websites are WCAG 2.0 compliant.

EXECUTIVE SUMMARY

Document background

On June 24, 2019, Sidewalk Labs submitted *Toronto Tomorrow* to Waterfront Toronto, the publicly-mandated corporation that selected Sidewalk Labs as Innovation and Funding Partner in 2017. Since this date, there have been multiple important contributions to public discourse that have all productively helped shape the further evolution of the project, including:

- On June 24, 2019, Steve Diamond, the Chairman of Waterfront Toronto's board, issued an open letter laying out Waterfront Toronto's "threshold issues" to be resolved, including approaches to data collection, data use, and digital governance.
- On June 28, 2019, Waterfront Toronto published a "A Note to Reader" for the draft MIDP, including key questions from Waterfront Toronto on digital innovation.
- On September 10, 2019, DSAP issued a "Preliminary Commentary and Questions" on the draft MIDP. Much of this commentary sought additional, clarifying information about the concepts put forward in the draft MIDP.
- On September 19, 2019, Waterfront Toronto issued the Feedback Report on the first round of public consultation on the draft MIDP.
- On October 31, 2019, Waterfront Toronto's Board of Directors approved resolutions on a set of "Threshold Issues" with Sidewalk Labs and moved Waterfront Toronto to the formal evaluation stage of the process.

The DIA is responsive to all of these sources of feedback.

The Threshold Issues resolution process results in updates to the Sidewalk Labs proposal

As codified in the document approved by Waterfront Toronto's board, there are four substantive changes to the Sidewalk Labs proposal that have a bearing on digital innovation, including:

1. A revised geographic scope
2. A new, Waterfront Toronto-led approach to data governance that is grounded in Canadian law
3. An expanded patent pledge that not only includes Sidewalk Labs' Canadian hardware and software patents covering digital innovations, but also foreign patents of the same subject matter
4. A shift from profit-sharing to net revenue-sharing in the proposed value-sharing arrangement between Waterfront Toronto and Sidewalk Labs

Below is a summary of these four updates.

1. A revised geographic scope

The MIDP proposed that Sidewalk Labs lead development (with local partners) in Quayside and Villiers West, and provide optional services for a broader geography called the "IDEA District." Based on ongoing discussions with Waterfront Toronto, the geographic scope of the project is focused on Quayside as an initial stage of the project. Based on the performance at Quayside, Waterfront Toronto recognizes that there could be substantial public benefits by providing for an area of future expansion of the initial phase beyond Quayside to the area such as Villiers West to further Waterfront Toronto's objectives, particularly in relation to economic development. Expansion to other lands would be subject to future Waterfront Toronto approvals and any applicable land disposition processes required by the City of Toronto. There will be no further use of the term "IDEA District." Instead, an "Innovation Plan," designed to achieve project objectives, would be applied in the project geography. These geographic updates impact digital innovation in that they determine the scale of services proposed and the language used to describe the project throughout this document

2. A Waterfront Toronto-led approach to data governance that is grounded in Canadian law

One of the most consistent themes of feedback has been encouragement for existing, government-established entities to take the lead on data governance. While many reviewers appreciated the underlying intent behind Sidewalk Labs' proposal for an Urban Data Trust, which was meant to ensure responsible data use and support trusted data sharing, the clear feedback was that a new standalone entity for these functions was not a preferred path for this project. The agreed-upon approach from the "Threshold Issues" resolution process is responsive to this feedback, reaffirms Sidewalk Labs' commitment to comply with all applicable Canadian law, and recognizes that Waterfront Toronto is working to advance responsible data use by Sidewalk Labs and all other private-sector companies working on the waterfront, along with creating opportunities for trusted data sharing. Below are some details of this approach:

- Waterfront Toronto, with its government stakeholders, will take the lead on data governance, enabling responsible data use throughout the designated waterfront area, as well as supporting trusted data sharing.

- Through consultation with government shareholders and the community, Waterfront Toronto has developed [Draft Digital Principles] to inform the evaluation of project proposals, including that of Sidewalk Labs. The core foundation of these Draft Digital Principles is that any project proposed to Waterfront Toronto must represent ethically responsible innovation that reflects public values and preserves or enhances the public good.

- The draft principles include:
    1. Everyone will have access to, and benefit equally from, digital solutions
    2. Digital solutions will be open, ethical and resilient
    3. Everyone will be able to understand how their data is being collected and used, and how organizations can and will be held accountable for their practices
    4. Strong privacy protections will be in place at all times
    5. Data and systems will remain under local control and be subject to local laws

- Building on these principles, Waterfront Toronto is developing “Intelligent Communities Guidelines” that will apply to private companies deploying digitally enabled solutions in the designated waterfront area. Similar to Waterfront Toronto’s existing Minimum Green Building Requirements that have raised the bar for sustainability, these Intelligent Communities Guidelines will be enforced through contracts with private companies in the designated waterfront area.

- Waterfront Toronto’s Draft Intelligent Communities Guidelines include a robust process of:
    - Privacy Impact Assessments
    - Algorithmic Impact Assessments (as applicable)
    - Threat Risk Assessments
    - De-Identification at source by default
    - Privacy by Design
    - Other privacy-enhancing practices

- These draft guidelines will be consulted upon and further developed with input from government stakeholders, industry, and the broader community.

- The guidelines will require public consultation and review by experts, including DSAP.

- The guidelines will foster trusted data sharing, and Sidewalk Labs is committed to contributing data, technological expertise, and resources to this effort. As stated in the MIDP, Sidewalk Labs recognizes that data collected in the public realm is a public asset, and is committed to making it publicly available by default.

- Finally, the guidelines will require providers of digitally enabled solutions in the designated waterfront area (including but not limited to Sidewalk Labs) to store and process personal information collected from such solutions (prior to de-identification) in Canada, and to use commercially reasonable efforts to store and process environmental data collected from such solutions in Canada, with exceptions to be determined on a case by case basis by Waterfront Toronto.

- As a planned operator of certain digitally enabled solutions in the designated waterfront area, Sidewalk Labs supports the development of the Intelligent Community Guidelines and will comply with those guidelines. Furthermore, Sidewalk Labs commits to identifying and providing information related to specific digital components as part of the development application process with the City of Toronto.

- Sidewalk Labs and Waterfront Toronto have agreed not to pursue establishing the Urban Data Trust as a new entity for this project, recognizing that the underlying objectives of ensuring responsible data use and supporting trusted data sharing can be achieved through supporting the strength of existing government bodies and a shared commitment to the pursuit of innovative models for trusted data sharing. Similarly, Sidewalk Labs will not use “urban data” as a term, and instead will rely upon existing Canadian legal constructs, and the concepts to which the Intelligent Community Guidelines will apply.

3. An expanded patent pledge to support Canadian-resident innovator

In the MIDP, Sidewalk Labs offered a patent pledge that would allow innovators to build on top of any hardware or software patents covering digital innovations that Sidewalk Labs filed in Canada. While many people in the tech ecosystem appreciated the general intent of this pledge, there was concern that restricting it exclusively to Canada would limit the potential growth of Canadian-resident companies that might take advantage of the pledge, since one of the most significant challenges facing Canadian innovators is reaching substantial scale and expanding beyond the Canadian market.

Based on this feedback, rather than limiting the pledge to Canadian patents, Sidewalk Labs has decided to also include any corresponding patents worldwide, ensuring that the pledge in fact aligns with the foundational objectives of supporting Canadian-resident innovators. In practice, this pledge means that a Canadian company could build on a hardware or software patent covering digital innovation filed by Sidewalk Labs in any country, greatly expanding the company's potential for innovation and growth. This pledge would go into effect immediately after the signing of Principal Implementation Agreements with Waterfront Toronto.

4. Shifting from profit-sharing to net revenue-sharing with the public sector

In the draft MIDP, Sidewalk Labs proposed entering into a first-of-its-kind profit-sharing agreement in which the public sector would receive a share of Sidewalk Labs’ global profits on “Testbed Enabled Technologies” for a period of 10 years starting from the first sale to a second customer.

Concerns were raised by DSAP and others about anchoring this agreement to profit rather than revenue. Based on

Waterfront Toronto's request, Sidewalk Labs has agreed to shift to a revenue stream on products and services piloted in Waterfront Toronto-facilitated testbed area, based on global net revenues, where net revenue will mean all consideration received by Sidewalk Labs less agreed upon deductions. The percentage and time frame for the value share will be finalized before entering into the Principal Implementation Agreements.

The DIA provides additional details on digital innovations in the MIDP

Responding to requests from Waterfront Toronto and DSAP, the DIA provides more information on the digital innovation components included in the draft MIDP. This material is broken into four sections:

Section 1 — Integrating digital technology into development planning at Quayside

This section begins with Sidewalk Labs' approach to integrating digital technology into planning, including how all work has been grounded in Waterfront Toronto's priority outcomes: economic development, sustainability, housing affordability, new mobility, and urban innovation. This section is anchored by a comprehensive list of all digitally enabled services proposed in the MIDP, including what data is anticipated to be collected and by whom. This list is augmented with diagrams to illustrate physical and digital infrastructure proposed for Quayside. The section also goes into depth on proposed digital infrastructure that is designed to support the digitally enabled services, as well as approaches to open standards, security, and resiliency.

Section 2 — Sidewalk Labs' approaches to responsible data use and inclusive design

This section begins with diagrams that document existing conditions for digital technology in public spaces, streets, and buildings. This context grounds a discussion of Sidewalk Labs' commitment to ethical and responsible data practices, including a detailed explanation of how Sidewalk Labs applies its internal Responsible Data Use Guidelines through Responsible Data Use Assessments. Second, this section demonstrates how Sidewalk Labs practices inclusive and participatory planning and design.

Section 3 — Growing the Canadian urban innovation ecosystem

This section makes clear that the strength of the greater Toronto region's local innovation ecosystem was a primary reason for embarking on this project, and that the project's success relies upon partnering with Canadian innovators. The roadmap details initiatives that would begin immediately following the signing of Principal Implementation Agreements with Waterfront Toronto, through the long-term, enduring impact of establishing a global hub for urban innovation anchored by Canadian values and companies.

Section 4 — Overview of existing policies and approaches for smart cities and digital governance

The Sidewalk Toronto project is part of a larger discussion taking place across Canada and internationally about the best ways to use technology responsibly to improve cities. This conversation necessarily brings together government, civil society, and the private sector. Government is actively leading on new policies, and there are strong precedents in Canada and internationally to build upon. This section aims to provide this global context, and also to contribute to a broader civic discussion on smart cities.

DIA section summaries

Below are detailed summaries of each section within the DIA.

Section 1 — Integrating digital technology into development planning at Quayside

The integration of digital technology into urban development requires different approaches to planning and design. Fundamentally, responsible data use and the digitally-enabled services for a place must be addressed as core to development planning, similar to other long-standing areas such as program, built form, and economics. For that reason, Sidewalk Labs has structured its development planning work differently from standard approaches, fully integrating planning, design, and digital innovation.

For the Quayside project, this integrated team has worked together to develop proposals that aim to achieve the fundamental public policy objectives established by Waterfront Toronto. Sidewalk Labs believes that such an approach is important for ensuring that digital technologies are only proposed when directly linked to key quality-of-life outcomes, and that the important ethical questions raised by the integration of technology and urbanism are addressed in all facets of a project.

Section 1 consists of a detailed overview of Sidewalk Labs' integrated approach to digital and physical planning for Quayside. The section discusses the Quayside development proposal as an overall matter and the specific proposals for new digital infrastructure.

Quayside development planning process

This subsection details the timing and content of the integrated development proposal for Quayside, and it also provides the specific stages in the Quayside development process at which Sidewalk Labs will furnish additional information on digitally-enabled services and estimated timing. Sidewalk Labs is targeting 2020 for submitting its initial development application, which would commence a reviews, revisions, and approvals estimated to be completed in approximately two years.

Proposed digitally enabled services for Quayside

This subsection provides an exhaustive listing of Quayside's digitally enabled services and a series of detailed illustrative conceptual site diagrams depicting how the digital and physical aspects of Quayside's proposed systems would be integrated. Below are some details found in this section:

- A comprehensive list describes Quayside's digitally enabled services and the principles underlying their deployment. The objective of this list is to not only describe the "what" and the "why," but also the "how" and "who" for each service. It also can help provide a clear, single source for what data collection activities are proposed — and importantly, what activities are not. Sidewalk Labs agrees to work with Waterfront Toronto and its government stakeholders in good faith to ensure each digitally enabled solution will not impede (and where feasible, will foster) accessibility in Quayside, freedom of association, freedom of expression, equitable treatment of marginalized groups, public engagement and participation and other fundamental rights and freedoms, as applicable.

- The list describes each system's purpose, structure, methods, responsible parties, including oversight, and relationship to the growth of innovation ecosystem.

- This section articulates the core principles underlying the digital innovation strategy. These include (but are not limited to): digital restraint, where Sidewalk Labs identified and proposed only digital solutions that directly and materially advance Waterfront Toronto's priority outcomes; and data minimization, security, and de-identification by default, where Sidewalk Labs restricts the collection, use, and misuse of data, especially personal information. As noted in the subsection, Sidewalk Labs has separately committed to not use data for advertising, nor sell it to third parties.

- In summary, the digitally enabled services proposed in the list reflect 18 major services/systems with 52 subsystems.
  - 82% of these services/systems have existing precedents (i.e. they have already been partially or fully implemented in an existing project, either in Toronto or elsewhere around the world).
  - 75% would be substantially purchased from third parties (with only 25% anticipated to be built by Sidewalk Labs).

- Conceptual site diagrams illustrate the integrated digital and physical layers of Quayside's proposed systems. These diagrams supply early insights into the spatial location of sensors and related technology for each of the digitally enabled services on the list.

- An illustration shows the more comprehensive information expected as the development application process continues, providing sample information for the Mobility Management System, Dynamic Curb Sub-System.

Proposal for digital infrastructure that supports digitally enabled services and enables testbed conditions

This subsection provides an in-depth discussion of Sidewalk Labs' proposal for digital infrastructure at Quayside. Sidewalk Labs envisions ubiquitous connectivity in Quayside, integrating abundant, secure, and seamless connectivity both indoors and outdoors for people, infrastructure, and devices. The advanced digital infrastructure is designed to enhance security, increase resiliency, and enable adaptability — powering the quality-of-life improvements envisioned for the neighbourhood. In particular, the subsection details the following four proposed aspects of the digital infrastructure:

- **Koala, a new standardized outdoor mount that provides access to power, connectivity and connection points to reduce costs and improve adaptability.** Koala would provide power and network connectivity to devices without requiring new electrical wires or extended street closures. Koala supports aspects of Waterfront Toronto's *Digital Principle #2: Digital solutions will be open, ethical and resilient* by making it possible for infrastructure managers to easily deploy and use a wide range of devices in the public realm. It also supports Waterfront Toronto's *Digital Principle #4: Strong privacy protections will be in place at all times* by enabling greater control over data collection efforts, as well as security breaches. The subsection reviews existing market solutions, offers technical specifications, and lays out proposals for risk-mitigation to address potential security threats and vulnerabilities.

  The subsection also addresses questions about how Koala might achieve adoption at scale to become a new standard, particularly in advance of the anticipated global rollout of 5G. As provided in a detailed Koala development roadmap, Sidewalk Labs expects to complete the initial proofs of concept for Koala by the end of 2020 and to complete testing for wide release by the end of 2022.

- **Neighbourhood-scale Software-Defined Networks ("SDN") that enable a more secure and resilient network infrastructure.** SDNs support aspects of Waterfront Toronto's *Digital Principle #1: Everyone will have access to, and benefit equally from, digital solutions* by making it easier for residents and consumers to access secure, high-performance internet connections throughout the development and Waterfront Toronto's *Digital Principle #4: Strong privacy protections will be in place at all times* by providing greater control over connected devices, and by enabling greater visibility of and control over any potential security breaches.

The subsection details SDN benefits, including improved internet access through ubiquitous Wi-Fi, reduced costs, and improved security; offers a technical overview of SDN, including its advantages for security and resiliency, the scope of existing technologies, and limitations of these technologies; discusses the process for completing an SDN development roadmap; and outlines implementation scenarios for Quayside.

- **Super Passive Optical Network ("Super-PON"), to enable internet service at least on par with existing service while requiring less cable, equipment, and energy.** Super-PON supports aspects of Waterfront Toronto's *Digital Principle #1: Everyone will have access to, and benefit equally from, digital solutions* by increasing the capacity to provide secure, high-performance internet connections throughout the development and Waterfront Toronto's *Digital Principle #2: Digital solutions will be open, ethical and resilient* by advancing an open-source solution that provides a path for future network upgrades and capacity improvements while minimizing costs.

  This subsection provides a technical summary comparing conventional PON and Super-PON, and offers a discussion of implementation for Quayside. Notably, Sidewalk Labs does not intend to serve as the ISP of record and expects a third party to administer the Super-PON, if a local provider chooses to incorporate it. The subsection highlights that Sidewalk Labs has had discussions with Beanfield Metroconnect, Waterfront Toronto's telecommunications partner, which has expressed interest in Super-PON technology.

- **Distributed Verifiable Credentials, an emerging and promising privacy-preserving technology that provides individuals with control and transparency over the personal information they share in order to access digitally enabled products and services.** As part of a set of digital infrastructure proposals for Quayside, distributed verifiable credentials support aspects of Waterfront Toronto's *Digital Principle #3 : Everyone will be able to understand how their data is being collected and used, and how organizations can and will be held accountable for their practices* by providing people with an innovative way to control how their personal data is used and accessed by others and Waterfront Toronto's *Digital Principle #4: Strong privacy protections will be in place at all times* by advancing a technological infrastructure that limits the collection and use of personal information while enabling access to services.

This subsection provides a technical summary of a desired architecture for distributed verifiable credentials, highlights use cases, and outlines benefits for individuals and organizations. The subsection also highlights developments in privacy-preserving technology, and the work of researchers and policy-makers who are advancing the deployment of distributed verifiable credentials and other forms of secure digital identity. The subsection also reviews research conducted by Sidewalk Labs, as well as engagement with many of the researchers and companies in this ecosystem, which informs confidence that distributed verifiable credentials is a viable privacy-preserving technology that will likely be developed by the burgeoning ecosystem for deployment in Quayside.

Sidewalk Labs' approach to open and resilient technology design and implementation

Sidewalk Labs acknowledges concerns around the potential for technological lock-in and risks related to security and resiliency of digital systems. This subsection highlights best practices and approaches to address these issues, and confirms our commitment to applying the principles that were outlined in the MIDP for openness, standards, resiliency, and security, as well as to working with other organizations and institutions already advancing these principles.

These approaches support aspects of Waterfront Toronto's *Digital Principle #1: Everyone will have access to, and benefit equally from, digital solutions* by enabling participation in digital activities through open digital processes and the sharing of data as appropriate. They also support *Digital Principle #2: Digital solutions will be open, ethical and resilient* by advancing open standards, interoperability and protocols that do not foster vendor lock-in and dependency.

Sidewalk Labs' approach to digital reliability emphasizes three design goals:

1. prevent disruption and loss of functionality
2. enable rapid detection of actual loss or increased risk of loss of functionality
3. prepare to rapidly restore functionality to services that are disrupted

Additionally, Sidewalk Labs is committed to:

- adhering to Waterfront Toronto's emerging Intelligent Community Guidelines regarding data residency as they apply to all proponents in the designated waterfront area; and
- maintaining appropriate network and data security safeguards as required by existing privacy law (e.g. PIPEDA), as well as following industry best practices generally to prevent breaches of digital systems.

Section 2 — Sidewalk Labs' approaches to responsible data use and inclusive design

We are surrounded today by digital technology embedded in buildings and the public realm that is often invisible. Travelling through a downtown area, or on a visit to a popular public gathering space, one could encounter security cameras, traffic cameras, pedestrian or bicycle counters, Wi-Fi access points, or occupancy sensors that turn on exterior lights or open doors — to name just a few typical systems.

This technology has the potential to improve many aspects of our lives — it can help keep us safe, reduce traffic, aid in the planning of city infrastructure, provide reliable access to the internet, or make spaces more accessible. This is just as true in Toronto as in most big cities around the world.

But there is often a lack of transparency around these implementations. Furthermore, the pace of digital technology development requires a robust approach to privacy and responsible data use beyond thinking about the point of collection with notice and consent. Sidewalk Labs believes that a higher standard of data governance in cities is possible, and that the public should know how and why data is being collected and used in streets and public space.

Section 2 details Sidewalk Labs' dedication to ethical and responsible data practices, including in developing and following internal Responsible Data Use Guidelines. The section also explains Sidewalk Labs' approach to inclusive and participatory planning and design.

Having processes in place that guide decision-making and actions

This subsection describes the underlying rationale for establishing ethics and responsible data use. Among other things, these protocols establish a culture that resists "technology for technology's sake," guides "institutional reflexes," ensures that data use is linked to a compelling public purpose and appropriate protections, and helps protect the public from unintended consequences.

Responsible Data Use

This subsection offers an overview of **Sidewalk Labs' internal Responsible Data Use Guidelines**. Specifically, the subsection provides:

- A description of the guidelines, which include beneficial purpose, transparency, openness, proactive engagement, community trust, and people first. The guidelines, which evolved over the past two years based on consultations with experts and community feedback, apply to all data activities by Sidewalk Labs. The guidelines are used internally for assessing proposed pilots and projects that involve data.

- An exploration of how Sidewalk Labs brings these guidelines into its practices through **Responsible Data Use Assessments (RDUAs)**. The approach builds on an existing tool—Privacy Impact Assessments (PIAs), which identify and mitigate the potential privacy risks of programs involving personal information—to address impacts from the use of data not just on individuals, but on broader segments of society. The RDUA was developed by Sidewalk Labs with the Information Accountability Foundation — an independent global think tank focused on data governance — and provides a mechanism for complying with all applicable privacy requirements, while going further than existing law in considering beneficial uses, risks, and ethical questions related to data. The RDUA tool is made public with the DIA, and is available for others in the community to use, if they choose.

Sidewalk Labs triggers an RDUA process for its data collection activities, even if they do not include personal information. The RDUA process addresses: the purpose of the data collection; the sources of the data; legal compliance and data ethics; and the risks and benefits associated with the project and data collection activity. To enhance accountability, Sidewalk Labs currently publishes RDUA summaries on its website for pilots and products that have launched. This allows the public to assess the conclusions and the analysis conducted for a given activity.

This subsection also provides an overview of Sidewalk Labs' approach to **responsible Artificial Intelligence** (AI). The development and increasing use of AI systems raise certain digital governance challenges that go beyond privacy. Specifically, the subsection provides:

- The overarching framework guiding Sidewalk Labs' AI approach. Inspired by the proliferation of AI principles that have emerged in the past several years, Sidewalk Labs developed six principles that are designed to be contextual, progressive, and technology-neutral: fairness and equity; accountability: transparency and explainability; relevance; value alignment; and respect for human dignity and safety.

  These principles have been informed by keeping abreast of the research and policy landscape, and engaging on best practices with external experts and consultants. To put these principles into practice, Sidewalk Labs will convene an internal multidisciplinary team and incorporate the responsible AI assessment into its practices.

Further, this subsection delineates the four stages of the RDUA process, using a case study on a completed RDUA for an existing pilot to illustrate the process. Specifically, the section discusses:

- The "three lines of defense" model for data governance applied by Sidewalks Labs. The "first line" consists of the business teams and the heads of product and legal, who commit to applying RDUA principles in their decision-making process. The “second line” is the privacy and data governance team, which leads the privacy and data ethics reviews, establishes policies and guidance, and serves as a first point of contact for all privacy and technology ethics matters. The “third line” is Sidewalk’s engagement with external stakeholders, experts, and consultants.

- The commitment to continuously update RDUAs as circumstances change and as application and technology uses evolve.

- A case study RDUA process for the launch of a public realm sensing pilot at Sidewalk Labs’ workspace, 307. Sidewalk Labs explored a solution that uses a privacy-by-design approach to measure the flows of people and transportation modes through streets and open spaces. The RDUA process facilitated discussions with Numina, the civic tech company that developed the technology, about its privacy-centric design. The case study offers an example of how the RDUA process drives Sidewalk Labs’ decisions on its potential technology partners and ensures that we share the same values.

Inclusive and participatory planning and design

Sidewalk Labs has incorporated inclusive and participatory planning and design into its work in Toronto from the beginning, and worked to ensure opportunities for ongoing participation and co-creation over time.

This subsection describes the mix of approaches, principles, capacity building, and new tools that Sidewalk Labs has used to help make planning and design more inclusive. It provides more information on these approaches, addressing questions raised by Waterfront Toronto, their Digital Strategy Advisory Panel, and the public. Specifically, the subsection discusses:

- **Inclusive usability testing.** Sidewalk Labs has financially supported Code for Canada’s GRIT Toronto program, which recruits Toronto residents from diverse backgrounds, lived experiences, and technical skill levels to test and participate in technology design. This initiative seeks to ensure that new digital solutions in Quayside are built with neighbourhood needs in mind.

- **Co-designing for accessibility.** As a result of over 75 hours co-designing with over 200 members of the disability and accessibility communities in Toronto, Sidewalk Labs has drafted 22 accessibility principles and incorporated over 100 recommendations for improvement in our ideas. The principles will continue to adapt and expand to incorporate input and additions from the community, including through a working group integrated with the next phase of planning and design.

- **Prototyping digital transparency in the public realm (DTPR).** DTPR attracted more than 100 participants from several cities to co-create a visual language (a set of icons) to help inform people on how and why data is being collected and used in the public realm, and provides a digital channel for learning more and providing feedback. While the project does not address all issues around consent in data collection, it seeks to advance a broader conversation around data transparency.

- **Prototyping inclusive civic tech tools.** Over the past two years, Sidewalk Labs has built prototypes that aim to support the work of civic innovators. These tools, which would be available but not required for use by the community in Quayside, include:

    - Collab, a digital tool developed with Toronto non-profit Digital Public Square that allows community members to propose choices for events in public spaces and evaluate the trade-offs associated with each proposal—in other words, how their individual choices could impact the community. Collab is designed to increase community participation and facilitate more inclusive and collaborative decisions.
    - Commonspace, an open-source digital prototype developed with the non-profit Gehl Institute and used by Thorncliffe Park Women's Committee that makes it easier for community groups to collect reliable data on how people use public spaces.

Additionally, this subsection discusses Sidewalk Labs' commitment to integrating **social infrastructure** in planning, a critical ingredient for designing truly inclusive, participatory spaces. Sidewalk Labs has engaged in proactive, holistic planning and co-creation with local community, government, and business partners to imagine what these spaces might look like. To inform its inclusive design principles, Sidewalk Labs commissioned research from Toronto-based partners:

- Park People, Canada's leading public space advocacy charity, and Doblin, Deloitte's human-centred design and innovation practice, produced a study, "North of the Water," on people-first public space design.
- Ryerson University's School of Urban and Regional Planning conducted research on retail trends in Toronto from 2007 to 2017.
- Toronto firm Idea Couture led research with community members and service providers, resulting in a report, "Living Well on the Waterfront," on the future of well-being and health.

This section further addresses how community input shaped, and will continue to shape, Sidewalk Labs' plans to facilitate equitable access to services, technology, and participation in Quayside. Initial proposals include the Civic Assembly, which would provide gathering spaces, access to digital tools and experts, and spaces for performance, creation, and fabrication; and the Care Collective, which would provide spaces for the delivery of health care and community services, a health resource centre, and a quiet sanctuary space dedicated to mental well-being. Upon approval of the MIDP, Sidewalk Labs would form planning relationships with partner organizations to help lead a participatory process for design, program development, and tenant identification.

Section 3 — Growing the Canadian urban innovation ecosystem

Few cities can match the greater Toronto region's unique set of assets: a vibrant ecosystem of innovative technology businesses and accelerators; an exceptional talent pool and world-class academic institutions; and an open and diverse society that values inclusive growth, civic engagement, and forward-looking city-building. This was a foundation for Waterfront Toronto's Quayside RFP, which sought to catalyze the innovation ecosystem growing on the waterfront.

Recognizing that a thriving urban innovation ecosystem is essential to the success of the project, as part of a comprehensive deal, Sidewalk Labs is committed to supporting Canadian innovators at all stages of Sidewalk Toronto's evolution, including through a series of targeted initiatives designed to create long-term value for the Canadian ecosystem.

Section 3 lays out the initiatives Sidewalk Labs has proposed to support the growth of Toronto's urban innovation ecosystem.

Section 3 begins by explaining how Sidewalk Labs' business model aligns with the development of a more robust innovation ecosystem:

- First, we seek to build urban developments that incorporate quality design and technologies into placemaking to improve urban life. Core to this business is the integration of leading technologies from existing companies, and supporting the development and distribution of these solutions to address common urban challenges globally. To implement the Quayside project, Sidewalk Labs is committed to prioritizing Canadian companies by extensively engaging the ecosystem in sourcing and breaking ties in their favour.

- Second, where there are unmet needs in the market — such as gaps that would prevent the project from achieving critical outcomes — we develop products to address them. Through a global patent pledge for Canadian-resident innovators, open standards, and a net-revenue sharing agreement with the public sector, the Sidewalk Labs proposal would leverage the success of these new products to benefit the local innovation ecosystem and community into the future.

- Third, through a venture capital fund and infrastructure-focused affiliate, Sidewalk Labs will hold, acquire, invest in, and enable financing for, strategic partners that we see as integral to the future of cities. This approach will create expanded opportunities for startups and later-stage Canadian companies to access new capital for growing or expanding their businesses, constructing cutting-edge infrastructure, and bringing new products to market.

Conditions of a successful urban innovation ecosystem

This subsection provides an overview of the growing urban tech industry, the conditions for developing a successful urban innovation ecosystem, and Canada's strong position to become a global leader in this space. The conditions for success include access to capital and talent, market access, and ecosystem innovation capacity.

Sidewalk Labs' proposed initiatives for growing the Canadian urban innovation ecosystem

This subsection discusses Sidewalk Labs' plans to invest capital, intellectual property, and talent. Specifically, it discusses the following notable initiatives that would come into effect with Principal Implementation Agreements:

- **A venture capital fund focused on Canadian companies in the urban innovation space**. Infusing more capital and expertise into early-stage companies will enable them to scale more quickly, thereby providing more opportunity for these companies to grow larger at home and retain the intellectual property in Canada for the benefit of the Canadian tech sector over the long term. The fund's goal is also to unlock capital and support from other players in the ecosystem around this vertical. Canada has a strong base of companies at the seed and Series A stages, and by launching the fund, Sidewalk Labs can help accelerate the growth of these companies to become global leaders.

- **Sidewalk Infrastructure Partners (SIP).** With initial co-anchor partners Alphabet and the Ontario Teachers' Pension Plan, SIP will be available to provide financing for operators of advanced infrastructure systems, enabling access to capital for innovative projects that may have non-traditional risk profiles.

- **A patent pledge that supports Canadian-resident innovators advancing solutions globally.** To stimulate innovation in urban development, we will make our patented digital urban innovations available to Canadian-resident innovators, enabling them to leverage our proprietary technologies (software or hardware).

This subsection discusses the mechanisms through which the Sidewalk Toronto project would support market access through procurement from Canadian businesses and promoting these partners abroad. These include prioritizing Canadian companies to participate in procurements, and then supporting the global distribution of Canadian partners. Specifically, the subsection discusses:

- **The priority treatment of Canadian companies in procurement during implementation in the Sidewalk Toronto project.** Based on initial estimates from the design and engineering that informed the MIDP, there are 18 major digitally enabled services, including over 50 subsystems, envisioned for the Quayside project. Many services and subsystems contain extensive hardware and software components that Canadian companies will be well-positioned to deliver. In procurements led by Sidewalk Labs, we are committed to extensive local engagement to raise awareness of procurement opportunities, sourcing local companies as proponents whenever possible and to breaking ties in Canadian companies' favour to the extent permitted by law.

- **Support for distributing Canadian technologies globally.** Sidewalk Labs aims to support scaling of innovations successfully implemented in Quayside, including those developed by local partners. Such efforts would benefit emerging and established Canadian companies by accelerating routes to global markets and new customer acquisition.

This subsection also discusses the contributions Sidewalk Labs intends to make to develop local innovation capacity and support the growth of the urban innovation sector in Canada. The strength of this ecosystem is essential to the success of the Sidewalk Toronto project. To support ongoing innovation and leadership across the ecosystem, Sidewalk Labs is proposing a series of initiatives that contribute to strengthening the ecosystem foundations. Specifically, the section discusses the following initiatives that would come into effect with Principal Implementation Agreements:

- **Sidewalk Labs' contribution of $10 million in seed capital to establish an Urban Innovation Institute (UII).** This institute could serve as a hub for research focused on urban challenges, including the many social and ethical implications of technology in our cities today, and potentially oversee access to datasets as well. Meant to complement programs at existing Toronto institutions — ranging from leading research institutions like University of Toronto, innovation hubs such as MaRS, and non-profits like Evergreen — the UII is intended to help firmly establish Toronto as a world leader in the research and development of urban solutions. The UII and its partners will independently select avenues of research, and will keep with participating institutions' own intellectual property policies.

- **Fostering innovation across sectors through trusted data sharing.** Greater data sharing can substantially improve public policy outcomes and city operations, and spur new forms of knowledge and value creation. But data sharing also introduces certain risks to personal privacy and the potential for group harm. There are already many organizations and companies in Toronto, Ontario, and Canada working to pilot new responsible data sharing frameworks. To further the goal of data as a public asset, Sidewalk Labs suggests that a hub for data collaboration be created (potentially anchored at UII) and be operated collaboratively with cross-sector partners to support the data access needs of the public and third parties.

- **Sidewalk Labs' commitment to support Canadian-led standards setting.** Data standards set in Quayside — which represent values of inclusiveness, openness, public interest, and respect for individual rights and privacy — have the potential to shape approaches to data openness and privacy globally and be used in smart city projects around the world. With the leadership of governments working with Waterfront Toronto, non-profits, Canadian businesses, and other stakeholders, Sidewalk Labs will contribute to precedent-setting open standards that will form the basis of the Quayside implementation and establish a precedent for future smart cities projects around the world.

- **Potential development of the Villiers West Urban Innovation Campus.** Economic clusters show that cross-pollination from a few successful businesses can cause other businesses in related fields to grow — as knowledge, talent, and capital flow within a tight geographic and relational network. Toronto's eastern waterfront is already emerging as an important corridor of innovative activity; first-movers include Corus Entertainment, George Brown College, the Daniels City of Arts, MaRS, and others. Based on the performance at Quayside, Waterfront Toronto recognizes that there could be substantial public benefits by providing for an area of future expansion of the initial phase beyond Quayside to the area such as Villiers West to further Waterfront Toronto's objectives, particularly in relation to economic development. Expansion to other lands would be subject to future Waterfront Toronto approvals and any applicable land disposition processes required by the City of Toronto. Designed as an innovation campus for startups and civic innovators, Villiers West could be anchored by the permanent home for the UII and an expanded Google Canadian headquarters, and would be connected to neighbouring businesses, institutions, and communities.

- **A net revenue-sharing agreement with the public sector.** In the draft MIDP, Sidewalk Labs proposed entering into a first-of-its-kind profit-sharing agreement in which the public sector would receive a share of Sidewalk Labs' global profits on "Testbed Enabled Technologies" for a period of 10 years starting from the first sale to a second customer. Based on Waterfront Toronto's request, Sidewalk Labs has agreed to shift this arrangement to instead share a portion of net revenue rather than profit. The percentage and time frame for the value share will be finalized before entering into the Principal Implementation Agreements.

Next steps for engaging the urban technology ecosystem

This subsection outlines Sidewalk Labs' next steps for engaging different stakeholder groups within the Canadian innovation space, including incubators and accelerators, academia, civil society, and Canadian companies.

Section 4 — Overview of existing policies and approaches for smart cities and digital governance

Waterfront Toronto, its advisors, and the public have asked Sidewalk Labs to address how the MIDP was implicated by, and situated within, the existing policy landscape for digital governance and technology. Recognizing that this field is rapidly evolving, and will continue to evolve over time, Sidewalk Labs aims to provide this context and to contribute to the broader civic discourse on smart cities, in particular the political and ethical concerns they raise.

Section 4 provides an overview of the existing policy landscape in Canada and internationally, and offers case studies as precedent for smart city development.

Critical topics in digital governance and technology

This subsection provides a brief overview of four critical topics in digital governance and technology:

- **Privacy and Surveillance.** How is privacy preserved? How are security risks reduced?
- **Ethics and Inclusion.** Who has a voice? How can cities ensure equitable access to services? How do

ethics and values play a role in technology development?

- **Transparency and Accountability.** Who is accountable? How are decisions made? How is data controlled, shared, and retained?
- **Adaptability.** What makes cities flexible and able to accommodate change?

Existing privacy regulations in Canada, Canadian digital policy landscape, and opportunities in existing and emerging practices

These subsections offer a snapshot of the range of policy responses, approaches, and tools being developed respectively in Canada and around the world by the government, academic, civic, and private sectors. These include privacy principles; digital rights, ethics, and tools; responsible data sharing models; data trust models; and inclusive and participatory practices, such as digital literacy initiatives, participatory tools, open source standards, and modular procurement.

Digital innovation precedents from Canada and around the world

This subsection includes short case studies that describe inspiring precedents for responsible smart city development:

- Estonia (X-Road; Digital ID)
- Montreal (AI ethics; integrated mobility, Civic Innovation Lab for Regulatory Testing)
- New York City (Guidelines for IoT, the Automated Decision Task Force; Open Data);
- Chicago (Tech Plan; Array of Things)
- Amsterdam (Data Sharing; IoT Registry; Holiday Rental Registry; Data Exchange; TADA Manifesto)
- Barcelona (Ethical Digital Standards; Barcelona Digital City; Decidim)

Sidewalk Labs appreciates the feedback from Waterfront Toronto, DSAP, and the public. We are grateful for experts who have reviewed and provided input on portions of this document as it has evolved over the past three months.

Section 1

Integrating Digital Technology into Development Planning at Quayside

Abstract

This section begins with Sidewalk Labs' approach to integrating digital technology into planning, including how all work has been grounded in Waterfront Toronto's priority outcomes: economic development, sustainability, new mobility, affordability, and urban innovation. This section is anchored by a comprehensive list of all digitally enabled services proposed in the MIDP, including what data is anticipated to be collected and by whom. This is augmented with diagrams to illustrate physical and digital infrastructure proposed for Quayside. The section also goes into depth on proposed digital infrastructure that is designed to support the digitally enabled services, as well as approaches to open standards, security, and resiliency.

Table of Contents

Figures

Tables

Section 1: Integrating Digital Technology into Development Planning at Quayside

1.1 Sidewalk Labs and its role in Toronto

Sidewalk Labs is an Alphabet company founded in 2015 for the purpose of delivering improvements in urban life — on the belief that tackling these challenges is possible with careful integration of emerging innovations and people-first urban design. To fulfill that mandate, Sidewalk Labs assembled a team from across the worlds of urban planning, urban development, and digital technology. This diverse team shares a set of beliefs and founding principles about what makes cities great, with a company mission "to combine forward-thinking urban design and cutting-edge technology to radically improve urban life."

Together the team has developed a unique approach to urban innovation, broadly defined as the integration of physical, digital, and policy advances into the urban fabric to improve quality of life in cities. More than just the pursuit of isolated efficiencies associated with "smart cities," urban innovation requires a thoughtful interdisciplinary approach that sits at the intersection of two of the defining trends of the 21st century: global urbanization and technological change.

Sidewalk Labs team members focus first on key challenges faced by cities, such as sustainability and affordability, only after which do they identify innovations that might address these challenges. This means engaging deeply with key policy discussions and following technologies that are beginning to be deployed to improve life in cities, drawing inspiration from the cutting-edge work being done by urban planners and designers around the world, as well as from the capabilities being developed by leading technologists.

Critically, this approach does not presume that Sidewalk Labs alone would develop all the innovations a city might need. On the contrary, Sidewalk Labs aims to create the open conditions for ongoing improvement — recognizing that the best solutions to urban challenges come from a wide variety of actors and sources.

Of course, in proposing a project that includes digital technology as one tool (among many) to help drive innovation, questions about data collection and management are critical. Sidewalk Labs recognizes that information collected in public space must be put to use for the greater good, protected by a transparent and independent process and robust privacy safeguards, and made publicly accessible for anyone to build on.

Finally, while a mission-driven company, Sidewalk Labs is also a private entity and has developed a business model that concentrates on three key areas.

Each of our business's key activities has the potential to benefit Canadian innovators.

- First, we seek to build urban developments that incorporate quality design and technologies into placemaking to improve urban life. This area has sees revenues from the sources traditionally associated with real estate projects: rental revenue and income from the sale of condominiums and individual buildings.
- Second, we develop and implement technology systems and products that drive improvements to the quality of life in cities.
- Third, through a venture capital fund and infrastructure-focused affiliate, Sidewalk Labs will hold, acquire, invest in, and enable financing for strategic partners that we see as integral to the future of cities.

1.1.1 Why Sidewalk Labs is in Toronto

Waterfront Toronto was formed by the three levels of Canadian government to unlock the social and economic potential of the waterfront by using best practices in urban planning and innovative development approaches — and to advance core public priorities, such as economic opportunity, sustainability, and affordable housing. The organization has guided roughly 2.5 million square feet of development (completed or planned) and leveraged initial government funding to spur $4.1 billion in economic output for the Canadian economy.

In spring 2017, Waterfront Toronto issued a Request for Proposals (RFP) for an Innovation and Funding Partner that identified Quayside and the broader eastern waterfront as a "unique opportunity for governments, private enterprise, technology providers, investors and academic institutions to collaborate on [the] critical challenges [of affordability, sustainability, inclusivity, economic opportunity, and mobility] and create a new global benchmark for sustainable, inclusive and accessible urban development." The RFP was a recognition that more of the same development would no longer be sufficient for inclusive growth in the city.

Seeing great alignment between the Waterfront Toronto goals and Sidewalk Labs' mission, Sidewalk responded to the RFP and after a rigorous evaluation process was selected as Waterfront Toronto's Innovation and Funding Partner. Winning the RFP gave Sidewalk Labs the opportunity to develop and submit the draft Master Innovation and Development Plan (MIDP), which was provided to Waterfront Toronto and released publically at the end of June 2019. The draft MIDP was developed based on discussions with tens of thousands of thoughtful and engaged Torontonians[1]. Sidewalk Labs' work in Toronto would be a flagship project, showcasing the full breadth of what's possible when applying responsible innovation to all dimensions of a neighbourhood. The work of Sidewalk Labs in other places would likely advance specific elements of what's integrated in Toronto. This is why it is so important to get the project in

[1] For details on stakeholder engagement, please see Sidewalk Labs, Master Innovation and Development Plan, Volume 0, June 2019, Pages 66 - 87

Toronto right, and why the opportunity exists for Canada to shape design and policies that will influence work globally.

The submission of the draft MIDP was not the end of the process. Based on initial feedback from Waterfront Toronto and its Digital Strategy Advisory Panel, this Digital Innovation Appendix has been prepared to provide additional information on the plans, and we understand that Waterfront Toronto intends to further consult the public on the proposals and run an evaluation process through winter and spring 2020. Further, the MIDP provides conceptual plans and designs, and these will require multiple iterations of design development. Should both parties agree to move forward, both the physical and digital components of the plans will undergo further development and be subject to relevant municipal, provincial, and federal approvals, and further public review. Sidewalk Labs' commitment to this process is outlined further below.

1.2 Quayside development planning process

The integration of digital technology into urban development requires different approaches to planning and design. Fundamentally, responsible data use and the digitally-enabled services for a place must be addressed as core to development planning, similar to other long-standing areas such as program, built form, and economics. It is because of this that Sidewalk Labs has structured its development planning work differently than standard approaches, with planning, design, and digital innovation all integrated as one. For the Quayside project, this integrated team has worked together to develop proposals that aim to achieve the fundamental public policy objectives established by Waterfront Toronto. Sidewalk Labs believes that such an approach is important for ensuring that technologies are only proposed when directly linked to key quality of life outcomes, and that the important ethical questions raised by the integration of technology and urbanism are addressed in all facets of a project — from privacy to human agency to public interest.

1.2.1 Sidewalk Labs' commitment to integrating physical planning, urban design, and digitally-enabled services

The Quayside Development Plan, as presented in Volume 1 of the Master Innovation and Development Plan (MIDP), incorporates a build program, site plan, and development strategy at a conceptual level. It does not reflect the detailed level of design that is required as part of [the formal development application submitted to the City of Toronto].

Similarly, throughout the various Volume 2 Urban Innovation chapters, including the "Digital Innovation" chapter, the MIDP provides conceptual plans detailing the types of data and digital infrastructure required to implement the proposed innovations that allow Sidewalk Labs to meet Waterfront Toronto's priority outcomes. It also does not reflect the detailed design of the full digitally-enabled service that is proposed to be built in Quayside. That digitally-enabled service would be further detailed and designed in parallel with the development of the Quayside build program.

Therefore, subject to the approval of the MIDP, Sidewalk Labs would work with a full design and engineering consultant team to prepare a detailed development plan and accompanying infrastructure and transportation master plan for Quayside, as currently required by the development application process. The detailed development plan would advance the plans as conceptualized in the MIDP to a sufficient level of detail needed to proceed with the approvals process, which includes the completion of development applications subject to formal review by various government staff and agencies, public consultation, and final approval by the City of Toronto Council.

Building on the need to integrate physical planning with the design of digitally-enabled services, Sidewalk Labs plans to prepare a series of drawings and illustrations that articulate the integration of digitally-enabled services in the physical building and systems design, as part of the detailed development plan. Sidewalk Labs sees these digital planning materials as necessary for fully understanding the integration of physical and digital systems, and to ensure these systems are responsibly implemented and have appropriate evaluation and consultation.

1.2.2 How Sidewalk Labs plans to provide digital planning materials within the development application process

It is notable that the existing regulatory development process does not require the type of specific study or report focused on the digital and data-collecting components of the proposed development mentioned above. As a result, the underlying digitally-enabled services in developments are typically not comprehensively understood either during or after the development application process or after approvals are granted.

In an effort to provide clarity and transparency on the digitally-enabled services proposed for Quayside, Sidewalk Labs is planning to prepare additional materials as part of the development application process. These materials will detail the underlying digital components and data-collecting systems as the overall Quayside project is designed and undergoes municipal approvals. These consolidated digital planning materials would strive to provide a strong understanding of the digital components and data-collecting systems proposed in the development. The following section describes in more detail the existing process for Toronto development applications, and the stages at which additional digital planning materials would be provided.

The submission of a development application for Quayside falls within the first proposed project stage gate, as described in Volume 3 of the Master Innovation and Development Plan

(MIDP) (Page 210[2]). With an initial submission date targeted for 2020, it is estimated that the development application process would take two years, which is typical of similar-sized projects. The application would include the submission requirements for a zoning by-law amendment (ZBA), official plan amendment (OPA),and draft plan of subdivision (SUB), as detailed by the City of Toronto. It would incorporate information such as unit mix, minimum percentage of affordable housing, sustainability requirements, public realm area, and non-residential uses, depicted in a series of studies and reports including a Planning Rationale, Geotechnical Study, Energy Strategy, and architectural drawings.[3][4]

Following a zoning by-law amendment, official plan amendment, and draft plan of subdivision application, site plan control (SPA) applications would also need to be submitted for review by the City of Toronto. While the zoning by-law provides the numerical standards, site plan control regulates the layout, function, and qualitative aspects of a proposed development. As a result, a site plan control application for the development parcels in Quayside would provide a further level of detail and examine the design and technical components, including entrances and exits to parking, material of the buildings, and landscaping. Upon approval by the City of Toronto, the site plan control drawings, plans, and conditions would be secured through a legal agreement between the landowner and the City of Toronto.[5]

As part of the approval process of the plan of subdivision,[6] the City of Toronto may (and typically does) impose conditions on developments, which need to be achieved at specific stages of design and construction. The city also can impose conditions[7] to ensure that specific infrastructure elements are built to City standards and would undergo more detailed City review and approval prior to construction (for example, a typical condition of approval is that a tree planting plan specifying exact locations and species of trees be approved by the Forestry Division) prior to receiving a building permit.

The design and development of the innovation components and advanced systems identified in the MIDP (such as tall timber, stoa, dynamic streets, waste management, energy systems) are integrated in the development plan, and thus would be encompassed within the development application through the various studies and reports. For instance:

- The Energy Strategy would incorporate details on the advanced power grid and thermal grid;
- The Stormwater Management Report would incorporate details on the active stormwater management;

[2] Sidewalk Labs, Master Innovation and Development Plan Volume 3, June 2019, Page 210.
[3] City of Toronto, "Official Plan and Zoning by-law Amendment," Planning and Development, 2019.
[4] City of Toronto, "Draft Plan of Subdivision," Planning and Development, 2019.
[5] City of Toronto, "Site Plan Control Applications," Planning and Development, 2019.
[6] Government of Ontario, "Subdivisions," Citizen's Guide to Land Use Planning, August 27, 2019.
[7] City of Toronto, "Draft Plan of Subdivision," Planning and Development, 2019.

- The architectural drawings and Planning Rationale would incorporate details on tall timber and the stoa; and
- The Traffic Operations Assessment, Transportation Impact Study, and the Public Utilities Plan would incorporate details on dynamic streets.

The City allows for the ongoing advancement of the development's design throughout the approval process. The City's review and approval process results in increasingly detailed drawings being prepared and required conditions being set as the design of all the development components proceeds.

Similar to other submission requirements, digital planning materials planned to be created by Sidewalk Labs would respond to feedback from consultation. The increased level of detail of the digital planning materials would advance in tandem with the application stages and could include elements, such as plans, renderings, data flow diagrams, and other studies, as appropriate.

The approach presented here represents Sidewalk Labs' intent. However, it is understood that this may be amended through specific direction from Waterfront Toronto and/or the City of Toronto.

Example of level of detail required through the development application stages

As projects move through the various development application stages, details on elements of proposed developments are currently required for numerous items. For example, landscaping is regulated as follows:

- At the zoning by-law amendment, official plan amendment, and draft plan of subdivision stage, a tree preservation plan and concept site and landscape plan are required. In regard to landscaping, the concept site and landscape plan includes the "general location of existing and proposed planting on the site and on adjacent road allowance."[8]
- At the site plan control stage, a tree preservation plan and a landscape and lighting plan are required. The landscape and lighting plan provides further detail, including "location and planting details for proposed trees and other plantings," "location and dimension of significant landscaping features and species list," "green roof planting details," and "proposed plantings on the site including all street frontages, public walkways, driveways and easements, open areas, and on adjacent road allowance."[9]

[8] City of Toronto, "Application Support Material: Terms of Reference, Concept Site and Landscape Plan," Planning and Development, 2019.

[9] City of Toronto, "Application Support Material: Terms of Reference, Concept Site and Landscape Plan," Planning and Development, 2019.

The digital planning materials that Sidewalk Labs would provide would identify, classify, and map physical locations of the digitally-enabled services that are encompassed within the Quayside Development Plan, and include a list of associated data that could be collected. All proposals to collect or use data would still need existing processes (such as PIAs and TRAs), any processes required through Waterfront Toronto's Intelligent Communities Guidelines, and other assessments as required by City or Provincial regulators, to ensure that the digitally-enabled services achieve responsible data use and abide by regulatory requirements. The progression of these materials is initially envisioned as follows:

- **Level 1 - Digital design goals defined with basic layouts:** This was the level reached for a number of systems at the time of MIDP submission.

- **Level 2 - Digitally-enabled services generally defined allowing design flexibility for each element:** Systems components for purchase, partnership, or in-house development are identified. Relevant communication standards are identified and designs are underway. System function objectives are identified and an array of solutions are identified, although final physical location of equipment is not yet fixed (example: function of identifying locations of vehicles, pedestrians, and bicycles is fixed, and an array of solution options are identified to realize that function).

- **Level 3 - Specific location, purpose, type, and communication protocol for each digitally-enabled service complete:** Full system diagrams, the types of devices and associated data flows are designed. The standards each component will follow, or use to communicate with each other, are identified. Specifications are near ready for Request for Proposals for vendors.

- **Level 4 - Specifications and construction drawings:** Specific elements (e.g. SKUs) are specified. Responsible Data Use Assessments are complete, including changes based on regulatory reviews. Detailed testing and resiliency plans are complete.

In moving through the development application stages, the level of detail of digital planning materials would advance, culminating with a final set of drawings before a building permit is issued, that identify the sensor locations, types, and uses. At all stages, if Waterfront Toronto or the City so chooses, they could use these materials for consultation by advisory bodies or the public.

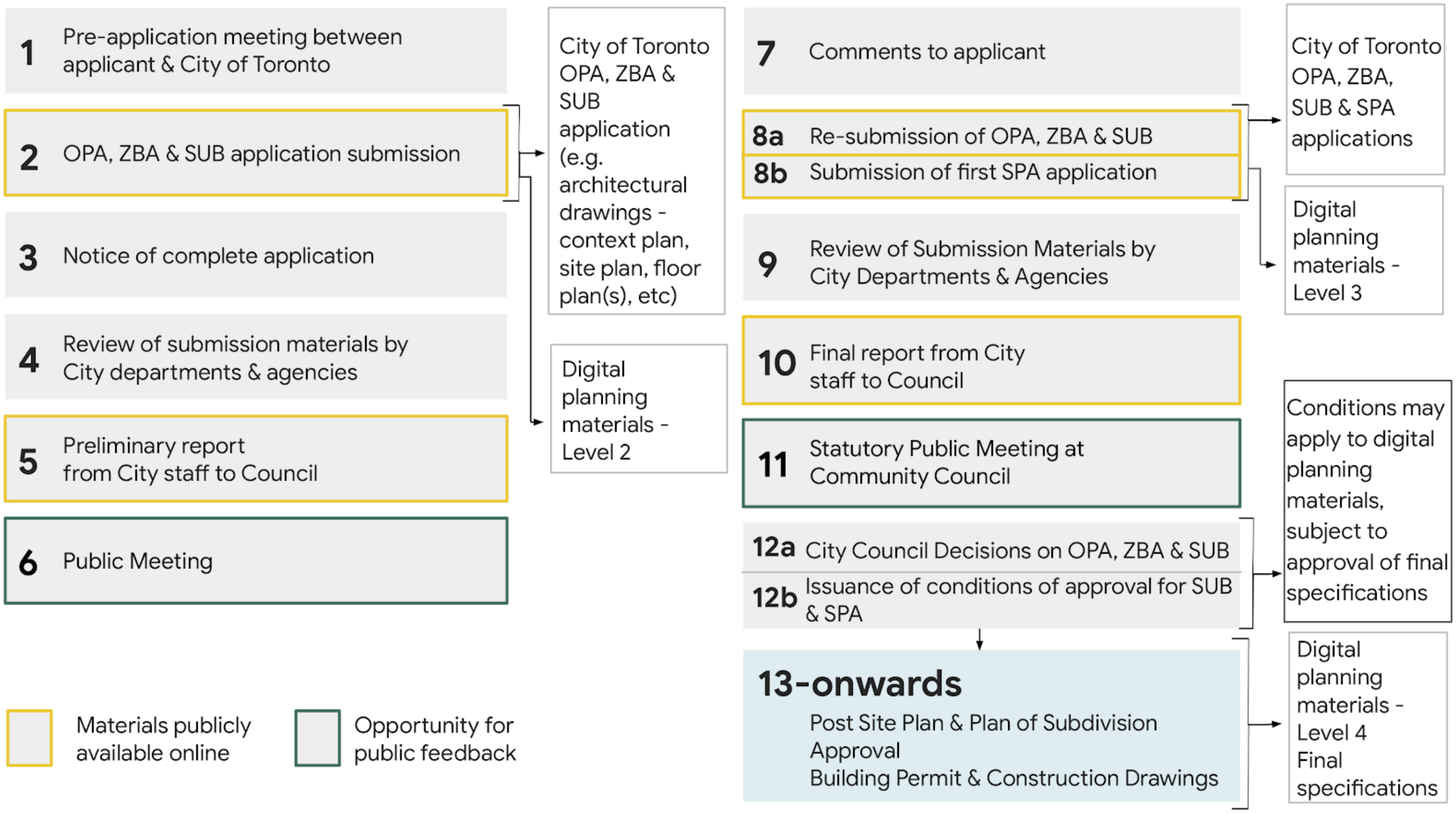
The diagrams below show how this maps to work completed to date and in the upcoming year(s), and also how it could map to the overall development application process. Sidewalk Labs looks forward to working with Waterfront Toronto and the City to refine an appropriate approach to the scope and timing of such digital planning submittals during the development application process.

Table: The Master Innovation and Development Plan (MIDP) — Work to Date and Planned Development Application

					IF PROJECT IS APPROVED					
Oct / Nov	**June**	**July / Sept**	**Summer / Fall**	**Fall / Winter**						
2017	2019	2019	2019	2019-20	**2020**					**2021-22**
RFP Awarded	**Draft MIDP Released** **Digital Design Goals Defined**	**MIDP Presentations to DSAP**	**Waterfront Toronto Public Consultation & Evaluation** **DSAP MIDP Reviews**	**WT Evaluation and Board Decision**	**Hire full design and engineering consultant team**	**Further address DSAP and WT comments** (from MIDP evaluation)	**Further address City comments** (from MIDP evaluation & pre-application meeting)	**Development Application DSAP** (series of presentations)	**Development Application Submission** (including further additional consultation) **Digitally-enabled Services Generally Defined**	**Development Application Process** (including further additional consultation) **Specific Digitally-enabled Services Designs Underway**

Should a positive Waterfront Toronto Board vote be achieved, Sidewalk Labs would start the preparation of Development Application materials. Progressively detailed digitally-enabled services designs would be prepared as part of the submission materials throughout the Development Application process.

Figure: City of Toronto Development Application and the progression of Digital Architecture Materials



Sidewalk Labs will provide further detailed digital planning materials for City official and public stakeholder reviews as part of the Submission of Application and Application Revision steps, prior to any final City Council decision.

Sections 1.3.1 and 1.3.2 below provide further information on the digitally-enabled services and proposals for the project as outlined in the MIDP, and section 1.3.3 further illustrates the type of content that could be included in future digital planning materials (sensor locations and the flow of data in a sample use case).

The typical conditions of the approval process would allow the City to identify requirements on the design, maintenance, and operation of the digitally-enabled services, if appropriate, as is done with many physical elements of a development. Sidewalk Labs welcomes the ongoing engagement that this process would provide, with Waterfront Toronto, with the City and the Province, and with the public, as a constructive means by which to further develop and refine the ideas presented in the MIDP.

1.3 Proposed digitally enabled services for Quayside

1.3.1 A more comprehensive list of digitally enabled services that support Waterfront Toronto's Priority Outcomes

The Master Innovation and Development Plan (MIDP) proposes a wide set of urban innovations designed to positively impact quality of life in Quayside from day one. The "Digital Innovation" chapter in MIDP Volume 2[10] provided an initial list of digitally enabled "launch services" to support achieving Waterfront Toronto's "priority outcomes" of Jobs and Economic Development, Sustainable and Climate Positive Development, Housing Affordability, New Mobility, and Urban Innovation. Recognizing that this list was not exhaustive, Sidewalk Labs has compiled one unified account of digitally enabled innovation services proposed for Quayside, and referenced throughout Volumes 1 and 2 of the MIDP: the Quayside Digitally Enabled Services List. This represents the first step in the development of a comprehensive set of digital innovation materials for the project, and provides a base for iterative design, development, and reviews by the City and other stakeholders moving forward.

The objective of this list is to not only describe the "what" and the "why," but also the "how" and "who" for each service. It also can help provide a clear, single source for what data collection activities are proposed — and importantly, what activities are not. Sidewalk Labs agrees to work with Waterfront Toronto and its government stakeholders in good faith to ensure each digitally enabled solution will not impede (and where feasible, will foster) accessibility in Quayside, freedom of association, freedom of expression, equitable treatment of marginalized groups, public engagement and participation and other fundamental rights and freedoms, as applicable.

Building on the information provided in the MIDP, the Quayside Digitally Enabled Services List provides early-stage information on the structure and components of each proposed service, an illustrative sense of what their Responsible Data Use Assessments could emphasize, and the types of third-party innovations that they might make possible. This includes:

- **Purpose:** A mapping of services and systems to Waterfront Toronto priority outcomes, and an outline of detailed subsystem objectives (beneficial purpose);
- **System structure:** Subsystems, components and digitally enabled functions of the service, existing precedents for solutions, and anticipated data collection;
- **Methods:** Data collection equipment, relevant data standards, and whether it is anticipated that the technology would be built by Sidewalk Labs, by others, or both;

[10] Sidewalk Labs, Master Innovation and Development Plan Volume 2, Chapter 5, June 2019, Page 444-447.

- **Responsible parties:** Typical operational oversight of a system/subsystem, suggested operational oversight, and proposed lead for procurement;
- **Innovation and ecosystem growth:** Third parties that could build on the data to realize further innovation and the related industry ecosystem.

(Detailed definitions of data included are provided immediately preceding the List below.)

As noted above, this Quayside Digitally Enabled Services List concentrates on those technologies and systems included as part of the innovation agenda proposed for Quayside. Sidewalk Labs also anticipates that Quayside would require digitally enabled technologies associated with "traditional" development happening today — examples include digital elevator control systems, emergency response systems, and automatic door opening sensors, to name just a few. As described in section 1.2.2 above, Sidewalk Labs would work with Waterfront Toronto and city staff through each phase of the development application process to identify the set of digital planning materials appropriate for submission at each project phase, through to building permits.

Summary statistics for digitally enabled Services proposed in the list:

- 18 major services/systems with 52 subsystems.
- 82% subsystems with existing precedents (i.e. they have already been partially or fully implemented in an existing project).
- 75% subsystems would be substantially purchased from third parties (with 25% only built by Sidewalk Labs).
- 60% subsystems do not generate personal information. Any subsystems that do generate personal information do so in order for the service to enable a Waterfront Toronto Priority Outcome.
- 0 subsystems planned to use facial recognition.

Sidewalk Labs' additional commitments for personal information

In addition to the approaches in relation to digital services development outlined in the Quayside Digitally Enabled Services List — found below — Sidewalk Labs would like to clarify again its commitment to the protection of personal information. Sidewalk Labs will comply with all applicable privacy laws at all times, including those that apply to sharing of information with service providers. Additionally, Sidewalk Labs has made the following commitments in connection with the MIDP, including the Quayside Digitally Enabled Services:

1. Sidewalk Labs will not sell personal information.
2. Sidewalk Labs will not use personal information for advertising.
3. Sidewalk Labs will not share personal information with third parties, including other Alphabet companies, without explicit consent.

1.3.1.1 Sidewalk Labs' approach to digitally enabled services

Sidewalk Labs' approach to envisioning digitally enabled services has been grounded in a series of core principles based on responsible data use and digital ethics, support for Canadian innovation, and operational oversight consistent with existing structures. Below, these principles, and how they have shaped the proposed services, are highlighted.

Digital restraint

Sidewalk Labs recognizes that technology alone cannot solve urban challenges, and that digital technology should only be proposed when it truly can make a meaningful impact on key public policy outcomes and risks can be managed. For this reason, this list is not hundreds of different gadgets or speculative ideas. Rather, it emerged from a rigorous process deeply grounded in identifying urban challenges — agnostic of technology — and then only proposing digital solutions that were deemed especially valuable, informed by consultation. As opposed to many "smart city" projects, Sidewalk Labs deeply values "digital restraint" in its work. Each digitally enabled service proposed for Quayside maps back directly to one of Waterfront Toronto's Priority Outcomes, and the "objectives" (beneficial purpose) of each system and subsystem have been further refined to show how these components work to achieve these quality-of-life goals. Sidewalk Labs is focused on the outcomes that these systems can help to achieve, not implementing tech for tech's sake.

Data minimization, security, and de-identification by default

Sidewalk Labs is committed to collecting the minimum amount of data needed to achieve the beneficial purpose of proposed services, and to using the least invasive technology available to achieve the beneficial purpose. The Digitally Enabled Services List provides early information on the anticipated data to be collected and the technologies used for collection, based on the planning performed to date.

As the List shows, the majority of services do not collect personal information. Moreover, the vast majority of data that would be created is non-personal, aggregate, or de-identified. Personal information collected by the Digitally Enabled Services would not be used for surveillance purposes, sold to third parties, or used for advertising. It is also worth re-stating that Sidewalk Labs has committed to comply with all present — and future — Canadian privacy and data governance laws, regulations, and policy.

For a limited number of district-wide infrastructure services proposed for Quayside, account holders would be required to provide personal information for operational and billing purposes. These systems are designed to achieve objectives for both community and individual good — most specifically to realize a climate-positive neighbourhood, reduce energy use and cost, and create less congested, safer roads, and cleaner air. These proposed systems are:

- **Energy Home Scheduler** - Residents and tenants would provide limited information for billing purposes, and unit-level energy usage data would be collected. This is similar to information required by utilities today.

- **Waste Management** - Residents and tenants would provide limited information for billing purposes, and unit-level waste disposal data would be collected for the automated pay-as-you-throw systems. Trash would be analyzed based on weight and content, but not through methods that would collect personal information or link waste to individuals. This is similar to how pay-as-you-throw works today, where residents pay for each bag of trash.
- **Logistics/Freight Management** - Residents and tenants would provide limited information (name, address) for delivery purposes, similar to that provided to public and private carriers today. Data characteristics of the mail and freight packages moving through the system would be collected for systems operations, similar to the data gathered today by public carriers for registered mail and by commercial carriers.

The personal information gathered for these systems would be restricted for privacy purposes, and restricted to use only for the delivery and improvement of the service.

Building on best practices from Canada and beyond

For many of the services proposed in the list, some form of precedent exists relative to policy, products, systems design or components either in Toronto, in Canada, or beyond. Wherever possible, Sidewalk Labs plans to build on this precedent to de-risk the project and adopt lessons learned from earlier pilots or implementations, whether it be green infrastructure used for district-wide stormwater management, a bicycle green wave, or environmental sensors used to monitor outcome-based code in building applications.

Civic tech tools used in Quayside would build on successful precedents in Toronto and globally, where non-profits, community groups, or government deploy technologies to achieve better service delivery and resident engagement. Like other civic tech initiatives, data would be owned by the group deploying the technology and made open by default.

Buy rather than build, including prioritizing Canadian companies wherever possible

As noted in the Master Innovation and Development Plan (MIDP),[11] rather than building new technologies itself, Sidewalk Labs prefers to purchase third-party technology — or partner with third parties to create (or enhance) it — whenever there are existing companies that have the capability and incentives to implement the systems required. The List of services envisioned for Quayside illustrates that in the great majority of cases systems components — or even entire systems — are anticipated to be sourced from third parties. This presents a tremendous opportunity for the local ecosystem, as Sidewalk Labs would preference Toronto, Ontario, and Canadian companies whenever possible by breaking ties in procurement bids in their favour. Section 3 of the DIA provides further more details on how this project is designed to benefit Canadian innovators.

[11] Sidewalk Labs, Master Innovation and Development Plan Volume 2, Chapter 5, June 2019, Page 382.

Operational oversight consistent with existing structures
Sidewalk Labs proposes that the great majority of district-wide infrastructure services proposed for Quayside be overseen and managed by the same bodies as today: government, non-profits, or other regulated bodies such as private utilities. Significantly, this is true for systems located in public spaces and right-of-way such as mobility, outdoor comfort, and open space management systems, and notably this approach is similar to business-as-usual today, where an agency such as city transportation manages traffic lights and collects data on street usage; city parks department or non-profits such as Evergreen Brick Works and The Bentway Conservancy manage public space usage and operations; and a utility such as Toronto Hydro monitors energy usage to determine billing. Buildings-related services and systems are privately owned and operated today, and depending on the final project structure, Sidewalk Labs may act as primary owner of these systems — again, in line with common practice today.

Approaches for procurement
The list provides information on which services would have procurement led by Sidewalk Labs, and which by Waterfront Toronto or other government agencies. In accordance with the "Innovation Plan", to be reviewed and approved by Waterfront Toronto, Sidewalk Labs would design and procure the Advanced Infrastructure systems for which it arranges financing. Waterfront Toronto, taking the lead on municipal systems, would procure parks and public realm-related systems, communications networks, and digital models of underground utilities. If the proposals are accepted, it is envisioned that government agencies responsible for privacy and data governance policy would lead the procurement of any digital credentials technology and a registry of relevant digital technology located at the site.

As one potential example of how overall procurement and operational oversight would work for advanced systems: in the case of the waste management systems, Sidewalk Labs would manage the design and engineering, subject to reviews and approvals by the City. Sidewalk Labs would procure and manage construction based on the approved plans, and as permitted by the City. In operation, waste would be picked up by a hauler at a consolidation center on Quayside.

Services that others can build on
Engagement with Torontonians identified a strong belief that data generated in cities might reasonably be considered a collective public asset, and in response Sidewalk Labs has committed to making data generated by relevant services and systems accessible to others (to the extent that SWL is in control of data collected by the system and once reasonably protected - for more see section 3.2.3). The full List of services proposed for Quayside builds on the MIDP[12] to provide further ideas around the possible applications for this data, and the wider ecosystem of public and private actors that development of the innovation, or provision of related data, may support.

---

[12] Sidewalk Labs, [Master Innovation and Development Plan Volume 2, Chapter 5](), June 2019, Page 444-447.

1.3.1.2 Quayside Digitally Enabled Services List definitions

The following provides a short definition for each of the columns of the Quayside Digitally Enabled Services List:

- **MIDP volume, chapter, page:** Provides a reference to the key section in the MIDP where the relevant service is described in detail.

- **Proposed service**: Provides a list of all proposed digitally enabled services in Quayside, as listed in Volumes 1 and 2 of the MIDP.

- **Waterfront Toronto Priority Outcomes:** Maps the service, system and subsystem components to the five Waterfront Toronto Priority Outcomes: Jobs and Economic Development, Sustainable and Climate Positive Development, Affordable Housing, New Mobility, and Urban Innovation (see Volume 0 of the MIDP[13]). Urban Innovation contains two sub-classifications: items marked "Urban Innovation" are primarily stand-alone digital products, whereas items marked as "Urban Innovation — Inclusive Communities" include Public Realm and Social Innovation-related services and systems.

- **Subsystem:** Lists all major subsystems that work to support the corresponding Services. The majority of these subsystems are described in both Volumes 1 ("Quayside Plan") and 2 of the MIDP.

- **Subsystem objective(s):** Describes a detailed key objective set for each subsystem (a "beneficial purpose" as described in section 1.3.1 above), intended to advance the Waterfront Toronto priority outcomes.

- **Subsystem components**: Lists the key digital components that make up the subsystems — this information provides a more granular breakdown of equipment and starts to identify sensors and other equipment.

- **Digitally enabled function(s):** Provides detail on the key digital function performed by each subsystem or component.

- **Is there municipal precedent? (and where it is found in Canada or around the world?):** Outlines examples of precedents for systems, subsystems, components, or related policy, found in Canada or around the globe.

- **What data would be collected?:** Provides details on four types of data that may be collected as defined in the MIDP: Non-personal data, De-identified data, Aggregated data, or Personal Information. All Personal Information is indicated as "Restricted data — not published for privacy reasons," and the other three data types may be similarly restricted for privacy or

[13] Sidewalk Labs, Master Innovation and Development Plan Volume 0, June 2019, Page 162-193.

security reasons. *For further definitions of these data types, see the next page.

- **How would the data be collected?:** Provides early-stage information on sensor, or other equipment types, used to collect data for the relevant system.

- **Buy/build**: Indicates if Sidewalk Labs is intending to buy (purchase or contract through a third party in which Sidewalk Labs has no controlling interest), build (develop in-house or have controlling interest or ownership), or buy/build (purchase and integrate third party components or partner to co-develop where some pieces of the IP may be retained) to create this subsystem or component.

- **Relevant, existing data standards (such as storage and interface):** Lists any known relevant data standards related to the service/system. Where existing standards are developed and adopted or moving towards adoption, Sidewalk Labs plans to build on these standards rather than develop bespoke.

- **Typical operational oversight of usual subsystem:** Lists the typical responsible party for the service/system/subsystem. This could be: Public — Government, Non-Profit, Private — Third Party (not Sidewalk Labs), Private — Building Owner, or Private — Sidewalk Labs. In select cases, specialized owners (such as Private — Energy Service Providers, Toronto Hydro) are listed.

- **Suggested operational oversight of proposed subsystem:** Lists the party proposed to be responsible for the service/system/subsystem in Quayside, utilizing the same categories as those listed for typical oversight.

- **Proposed lead for procurement:** Lists the proposed party to lead procurement of the system/subsystem.

- **Possible third-party applications that could build on this data:** Based on the approach that many of these data sets may have public value and (providing appropriate security steps have been taken) be made publicly accessible, this column provides examples of the types of third parties that may be interested to utilize the data for a wide-ranging set of public and private endeavours.

- **What existing ecosystem the innovation supports (names are illustrative only)**: Provides information on the ecosystem of public and private groups, industries, and parties that development of the innovation, or provision of related data, may support.

The four types of data collected by the proposed services [14]

Non-personal data is data that does not identify an individual and can include other types of non-identifying data that is not about people. Some examples of non-personal data are aggregated data sets, machine-generated data (such as weather and temperature data), or data on maintenance needs for industrial machines.

Aggregate data is data that is about people in the aggregate and not about a particular individual. Aggregate-level data is useful for answering research questions about populations or groups of people. For example, aggregate counts of people in an office space can be used in combination with other data, such as weather data, to create an energy-efficiency program so consumption is controlled, with the goal of saving money and reducing energy use.

De-identified data is data about an individual that was identifiable when collected but has subsequently been made non-identifiable. Third-party apps and services may wish to use properly de-identified data for research purposes, such as comparing neighbourhood energy usage across a city.

Personal information has a legal definition in Canada and is the subject of privacy laws, including the Personal Information Protection and Electronic Documents Act (PIPEDA).[15] The broad legal definition of personal information includes any information that could be used, alone or in combination with other information, to identify an individual or that is associated with an identifiable individual.

The table on the following page, depicts a screen capture of the List, which is published as an online spreadsheet. The columns described above are labelled at the top of the spreadsheet. A screen reader version is also provided in attachment A.

[14] Sidewalk Labs, Master Innovation and Development Plan Volume 2, Chapter 5, June 2019, Page 417.

[15] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Table: Quayside Digitally Enabled Services List

(screen capture of the list below; [the list can be found at this link]() and in attachment A of this document)

Proposed Service	Waterfront Toronto Priority Outcomes	Subsystem	Subsystem Objective(s)	Subsystem Components	Digitally-enabled Function(s)	Is there Municipal Precedent? *(and where it is found in Canada or around the world)*	What data would be gener
Dynamic Streets - Mobility Management	New Mobility	Real-Time Traffic Operational System	More efficient flow of traffic. Faster travel times for vehicles, pedestrians, and cyclists.	Traffic management system algorithms and software	System would analyze travel patterns in real time to coordinate the operation of signals, lanes, crosswalks, pick up and drop off zone functions, and the Bicycle Green Wave.	Yes, though pick up and drop off zone functions and Bicycle Green Wave management functions are not included. Existing precedents: Traffic cameras, computer vision cameras that de-identify at source, traffic control center, pedestrian push buttons, bicycle counters, ride-hail/Taxi based GPS data	The Real-Time Traffic Operat inputs from the Adaptive Tra Dynamic Curb sub-system a perform system functions.
	New Mobility	Bicycle Green Wave	Enhanced safety for cyclists and decreased travel time.	Bicycle detection sensors and green LED lights. The Bicycle Green Wave sub-system integrates with the Adaptive Traffic Signals sub-system.	Bicycle detection sensors detect the presence and speed of bicycles. Bicycle Green Waves are indicated using in-pavement LED lights.	Yes - bicycle green waves are found in Amsterdam and Copenhagen. Aarhaus uses RFID tags on bicycles to trigger green lights as cyclists approach an intersection. Toronto's Lascelles Blvd has implemented bicycle detection and priority systems.	Aggregate: Cyclist counts. De-identified: Cyclist velocit Personal info: None.
	New Mobility	Adaptive Traffic Signals	Coordination of all travel modes. Enhanced safety for cyclists and decreased travel time. Safer intersections for pedestrians and reduced traffic.	Connected traffic lights, vehicle detection sensors, transit signal priority receivers, and an optimization control system. Also uses data from Bicycle Green Wave and Real-Time Crosswalks sub-systems. The Adaptive Traffic Signals sub-system integrates with the Real-Time Traffic	Adaptive signals use an optimization control system to make real-time adjustments based on data from connected traffic lights, vehicle detection sensors, transit signal priority receivers, the Bicycle Green Wave sub-system, and the Real-Time Crosswalks	Yes - adaptive traffic signals are utilized all over the world. Precedents: adaptive traffic signals on King Street Corridor providing transit signal priority. For pedestrian movement, in Singapore, certain crosswalks enable pedestrians to trigger a	Non-personal: vehicle prese transit vehicle speed, pedes De-identified: pedestrian pre Personal info: None.

1.3.2 Quayside — Illustrating the integration of the digital layer with the physical environment

1.3.2.1 Conceptual Site Diagrams for Quayside site

An approach for visualizing the physical and digital layers of the Quayside site

As noted in section 1.2 above, the MIDP provides a conceptual, master plan-level proposal, for both the built environment and the digitally-enabled services for Quayside. If approved, both physical and digital designs would be further developed and reviewed with the City and stakeholders as part of the regular City of Toronto development application process.

In line with this approach, Sidewalk Labs has developed an initial set of conceptual axonometric and section diagrams illustrating the integrated digital and physical layers of Quayside's proposed systems. These diagrams, prepared by an integrated team of planners, infrastructure and building engineers, product designers, and software/hardware engineers, are intended to provide an early understanding of the spatial location of sensors and related technology in the neighbourhood. Each diagram illustrates one single instance of each of the digitally enabled services included in the Quayside Digitally Enabled Services List, including related operational systems, subsystems and systems components. For example, the figure on the next page provides one example of the locations of each of the subsystems and components necessary to realize the proposed innovations for new mobility in Quayside: the Mobility Management Systems' bicycle green wave, adaptive traffic signals, real-time crosswalks, dynamic curb, and electric vehicle (EV) charging, and the Mobility as a Service (MaaS) application.

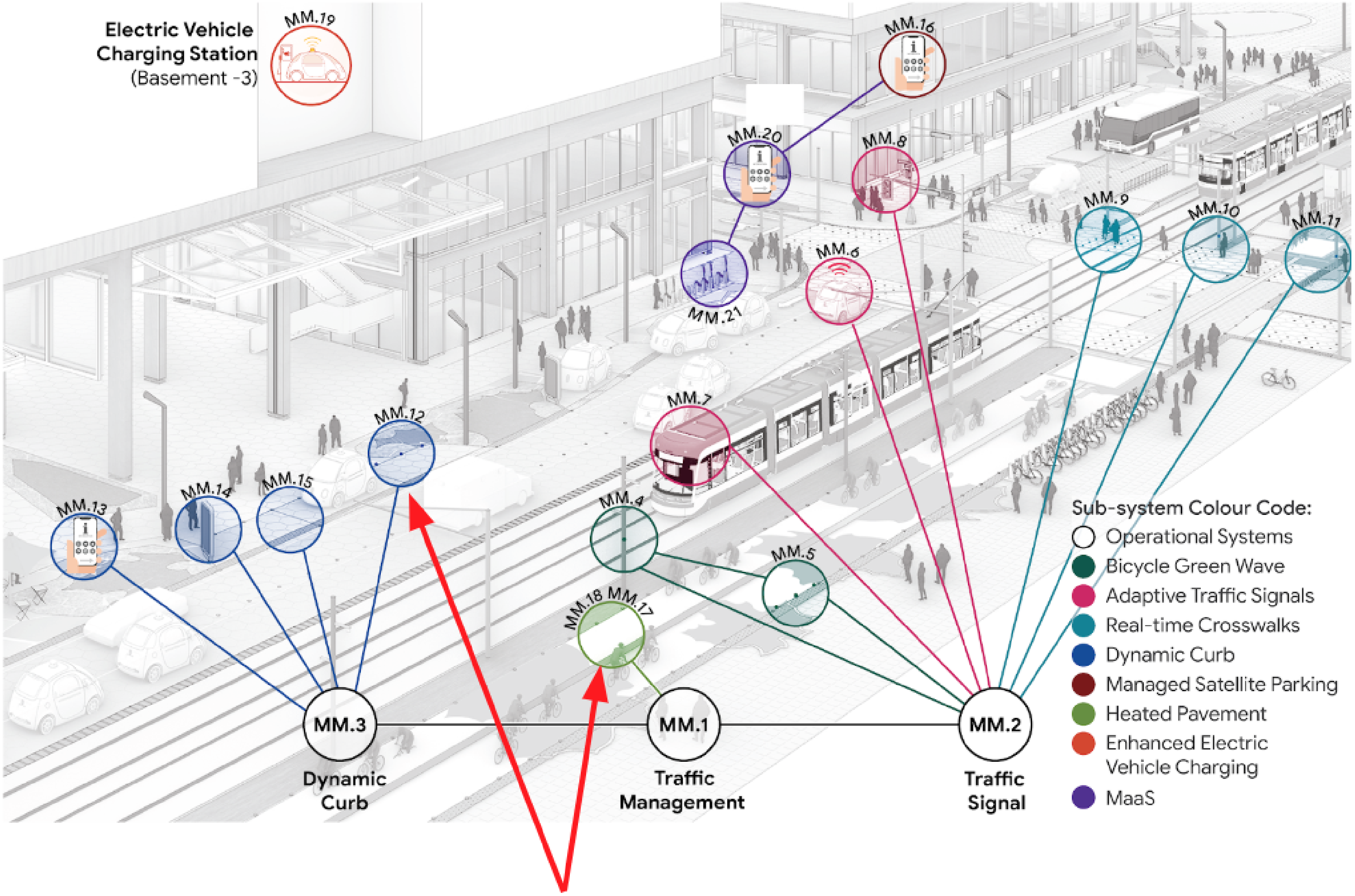
Please note that these diagrams provide examples of all services that have some physical manifestation at the site. Systems that exchange, or are provided with information coming from on-site physical devices, such as the Mobility as a Service (MaaS) system, are also included. Services included in the Quayside Digitally Enabled Services List that are solely digital in nature — and therefore lack a spatial location/dimension — are not included in the diagrams (for example, Collab or the Digital Housing Application System).

How to read the Conceptual Site Diagrams

Quayside Conceptual Site Diagrams — Axonometric and Section Diagrams

The following legend provides an explanation of how to read the Quayside Conceptual Site Diagrams provided below.

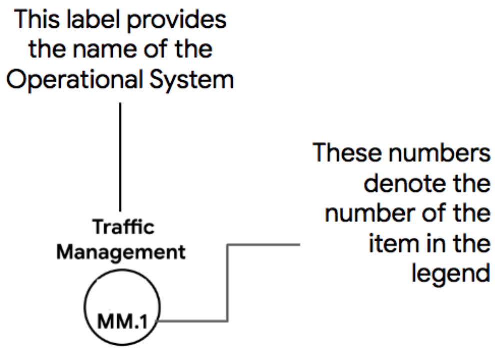
Figure: Quayside Conceptual Site Diagram Icons and Nomenclature



The location of coloured icons in the axon drawing illustrate the planned location of the component in the built environment. For example, in this drawing, MM12 is showing the location of technology for vehicle detection. MM17 is showing the location of technology for heated pavement.

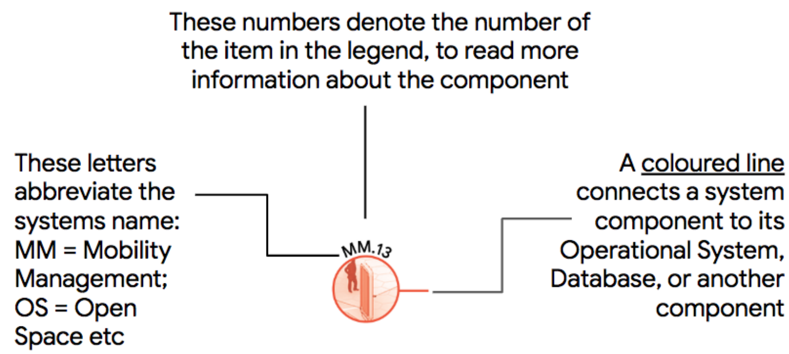
Quayside Conceptual Site Diagrams — Table Legend

A white icon like this below denotes a **operational system** of a major system or subsystem. These are **virtual** components and not located spatially on the site.



Note on system abbreviations:

A coloured icon like this below denotes a **physical** system component such as a sensor, radar, light, etc. found in a specific physical location on the site.



MM = Mobility Management Systems
OS = Open Space Systems
GF = Ground Floor Systems
B = Buildings Systems
BE = Building Energy Systems
L = Logistics Systems
W = Waste Systems
SW = Stormwater Systems
DE = District Energy System

Each Quayside Conceptual Site Diagram has a corresponding table that provides detailed information on each of the physical pieces of equipment (components) marked in the diagrams. The following list provides definitions for each of the pieces of data provided in the tables.

- **Subsystem:** Subsystems associated with the initial services proposed for implementation in Quayside, as noted in Volume 1 or 2 of the MIDP. If this cell is white, then this item is a operational system deployed to realize the service; if coloured, then the item is one component of the subsystem.

- **Objective**: The detailed priority outcome/beneficial purpose of the subsystem.

- **No.:** Label number corresponding to items displayed in the diagram.

- **Component Description:** The (often multiple) system components.

- **Purpose:** The Digital Transparency in the Public Realm icon (further details below) that denotes the primary purpose of the subsystem.

- **Types of Sensors:** The Digital Transparency in the Public Realm icons (further details below) that denote the sensors used to perform the required function to realize the service or subsystem (as applicable).

- **Types of Data Collected:** The types of data collected or used by the systems components, including: Non-Personal Data, Aggregate Data, De-Identified-at-Source Data, Personal Data; in cases where data would not be released to any third parties: Restricted Data; and Transactional Data

- **Precedent in Toronto:** Information provided in this column lists known precedents for this subsystem already piloted or implemented in Toronto, nationally in Canada, or in some cases in Europe or the United States.

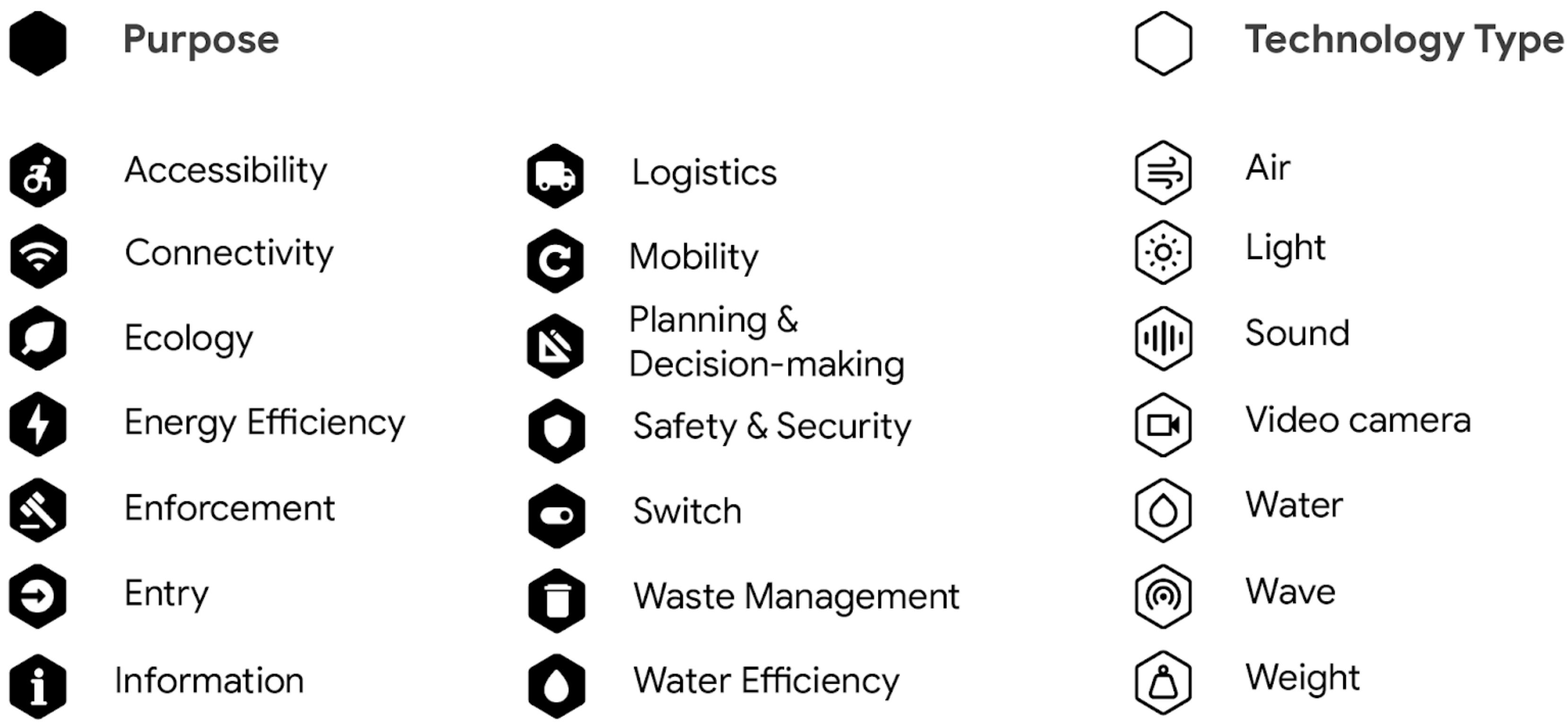
Note: all systems depicted in these diagrams would be subject to Responsible Data Use Guideline and Assessment processes and applicable government reviews and approvals. For more information on Sidewalk Labs' approach to responsible data use, see section 2.2.2.

Quayside Conceptual Site Diagrams — Digital Transparency in the Public Realm Icons

The Quayside Conceptual Site Diagrams utilize a set of "Digital Transparency in the Public Realm" icons developed by Sidewalk Labs in collaboration with academic, government, civic, and industry experts and stakeholders. These icons were created as a first draft of an open standard to provide a visual language for signage in the public realm that alerts the public to the presence of a digital technology, and allows the person-on-the-street to learn more about the technology and provide feedback.

The short definitions of these icons can be found here below, with detailed definitions and additional reference information provided via the open standard's repository on Github. For more on the Digital Transparency in the Public Realm project, see section 2.3.2.4.

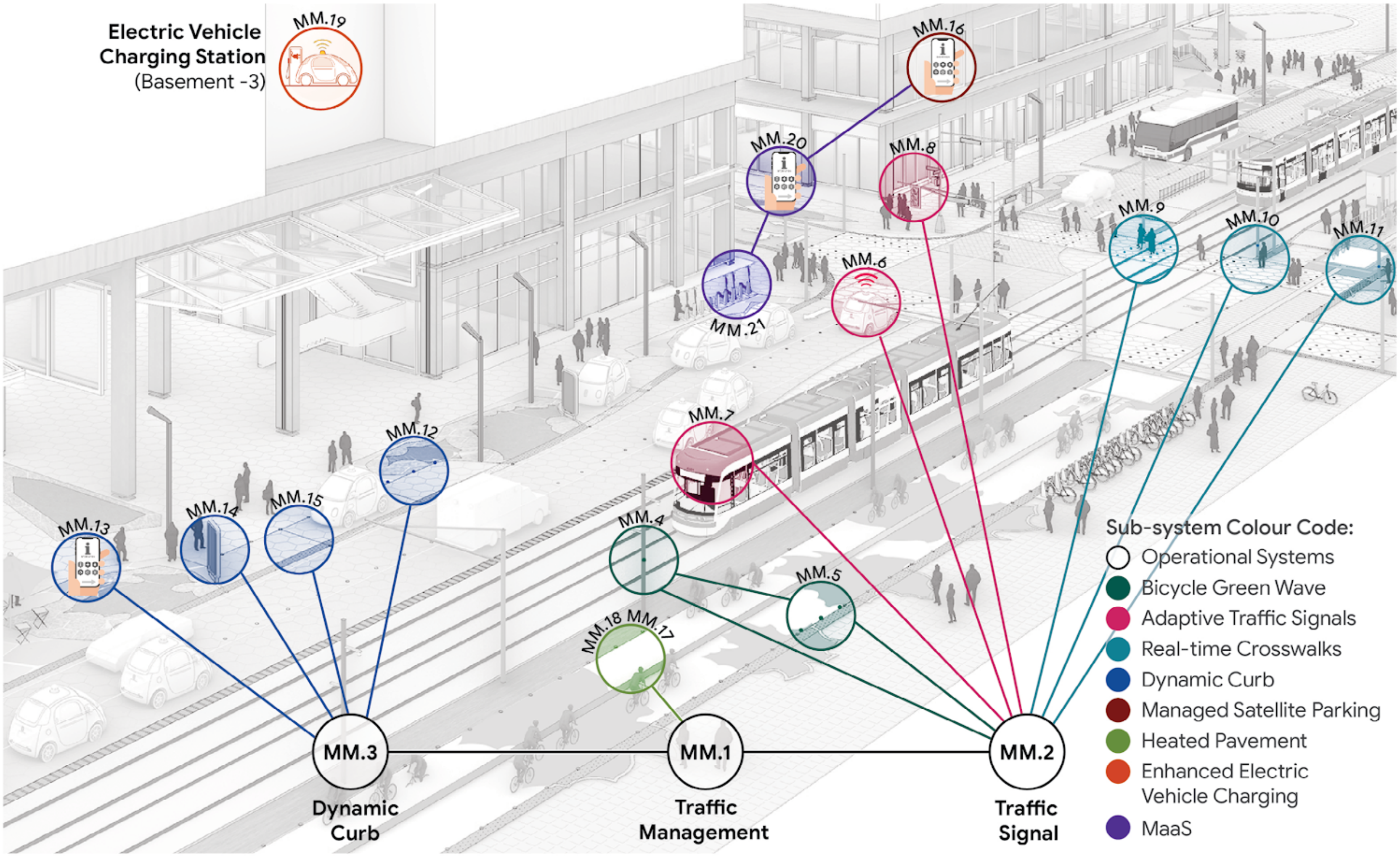
Figure: Digital Transparency in the Public Realm: Icon Definitions (Creative Commons License)[16]
For additional details, please refer to the information for [the open standard on Github.]



[16] Digital Transparency in the Public Realm project contributors. "Digital Transparency in the Public Realm: Icon Definitions." Accessed October 9, 2019. https://github.com/sidewalklabs/dtpr. The Digital Transparency in the Public Realm Icons and Taxonomy are licensed by the Digital Transparency in the Public Realm project contributors under the Creative Commons Attribution 4.0 International (CC BY 4.0) License. Portions of the icons include elements of, or are derived from, the Material icons which are licensed under Apache License 2.0.

Quayside Conceptual Site Diagrams — Integrated Digital and Physical Layer

Figure: Mobility Management Systems — Queens Quay Example



Note: For clarity, the coloured markers indicate a single location where the referenced technology would be installed. The actual number of each type of sensors would be shown in a more detailed plan set.

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Real-Time Traffic Operational System	More efficient flow of traffic: faster travel times for vehicles, pedestrians, and cyclists. Consolidates data flows from all mobility systems.	**Operational System MM.1**	**Traffic Operational System:** Optimization software that interfaces with each mobility system to enhance level of service.	Mobility	N/A	The Real-Time Traffic Operational System uses data inputs from the Adaptive Traffic Signals subsystem, Dynamic Curb subsystem, and other subsystems to perform system functions.	No known precedent in Toronto.
Adaptive Traffic Signal Operational System	Coordination of all travel modes. Enhanced safety for cyclists and decreased travel time. Safer intersections for pedestrians and reduced traffic. Consolidates data flows from traffic-signal-relat ed systems.	**Operational System MM.2**	**Adaptive Traffic Signal Operational System:** Software that uses all Mobility System Data to optimize traffic flows.	Mobility/ Accessibility	N/A	The Adaptive Traffic Signals subsystem uses data inputs from the bicycle greenwave, real-time crosswalks, vehicle and pedestrian detection sensors, and TSP signals to perform system functions.	King Street Transit Pilot aggregates data from traffic monitoring technology as well as transit priority signals.

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Dynamic Curb Operational System	More efficient movement of vehicles: fewer parking spaces, more reclaimed land for the public realm, and reduced overall traffic congestion. Processes data from Dynamic Curb components to operate the system.	**Operational System MM.3**	**Dynamic Curb Operational System:** Operating System for Dynamic Curb functions.	Mobility	N/A	The Dynamic Curb subsystem uses data inputs, and provides outputs, to all components of the Dynamic Curb subsystem to perform system functions.	The closest precedent in Toronto is for parking services (not curb drop-off and pick up): the Green P Mobile app provided by the Toronto Parking Authority allows users to pay for parking and extend their session.
Bicycle Green Wave	Enhanced safety for cyclists and decreased travel time. Bicycle green waves are indicated using LED strips on the pavement.	**MM.4**	**Bicycle Detection:** Electromagnetic loops or radar — embedded passive detectors that pick up and estimate speed.	Mobility	Light	**Aggregate:** Cyclist counts. De-identified: cyclist velocity. **Personal info:** None.	King Street Transit Pilot utilizes smart traffic cameras (including bicycle count) found at various locations, and Lascelles Blvd has implemented bicycle detection and priority systems.

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Bicycle Green Wave		MM.5	**Embedded LED Light:** Indicate optimal pace of travel in bike lanes.	Mobility	N/A	**N/A** - LED lights use data to perform a mobility function. No data collected.	Lighted pavement can be seen at Sugar Beach Park as part of an interactive water feature. (Green wave light precedents are found in Europe.)
Adaptive traffic signals that are controlled to prioritize transit, bicycles, and pedestrians	Adaptive signals make real-time adjustments to balance the needs of different groups, to achieve desired pedestrian safely, transit and bicycle speeds (bicycle green waves).	MM.6	**Detection for vehicles:** Electromagnetic loops or radar — embedded passive detectors that detect the presence of car waiting to use the intersection.	Mobility	Light or radar	**Non-personal:** Detection of the presence of a vehicle; transit vehicle and vehicle speed. Vehicle volume counts. **Personal info:** None.	The City of Toronto currently has red-light cameras operating at 149 locations.
		MM.7	**Transit Signal Priority (TSP) receiver.**	Mobility	Wave	**Non-personal:** Signal change request from LRT. **Personal info:** None.	Wireless transit priority systems are found at various locations along King Street.

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Adaptive traffic signals that are controlled to prioritize transit, bicycles, and pedestrians		**MM.8**	**Adaptive Traffic Signal:** Red-yellow-green sequence transit, bicycle, pedestrian signals.	Mobility	N/A	**N/A** - The Adaptive traffic signals use data to perform a function. No data collected.	The City of Toronto is piloting two types of smart signals (InSync and SCATS) at locations in Yonge Street and Sheppard Ave.
Real-time crosswalks	Safer and more efficient movement of people and public transportation.	**MM.9**	**Embedded LED Light:** Guide pedestrians to a median, where they would wait if a streetcar is approaching, and then continue their crossing after the streetcar has passed.	Mobility/ Accessibility	N/A	**N/A** - LED lights use data to perform a mobility function. No data collected.	Lighted pavement can be seen at Sugar Beach Park as part of an interactive water feature, but lit crosswalks are not yet found in Toronto. (Precedents are found in the US and Europe.)

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Real-time crosswalks	Safer and more efficient movement of people and public transportation.	**MM.10**	**Detection for pedestrians:** Radar, microwave, infrared.	Mobility/ Accessibility	Radar, microwave, infrared	**Non-personal:** Detection of the presence of a pedestrian. **Aggregate:** Pedestrian volume counts. **Personal info:** None.	Motion detectors are used throughout streets, parks and buildings in Toronto. For example, the washroom structure at Bellevue Park has infrared detection sensors installed on it to detect users. But these have not yet been linked to crosswalks in Toronto (Precedents are found in the US and Europe.)
		MM.11	**Push Buttons:** Active detection for pedestrians.	Mobility/ Accessibility	N/A	**Non-personal:** Detection of the presence of a pedestrian.	Typical push button activation for crosswalks. Commonly found at intersections in Toronto.

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Dynamic curb (real-time on-street pick-up and drop-off and flexible curb)	More efficient movement of vehicles: fewer parking spaces, more reclaimed land for the public realm, and reduced overall traffic congestion.	**MM.12**	**Vehicle Detection:** Occupancy and duration detection: magnetic and optical sensors.	Mobility	Light	**Non-personal:** Detection of the presence of a vehicle. Occupancy of total spaces at the curb, average duration of pick-up/drop-off event. **Personal info:** None.	King Street Transit Pilot utilizes smart traffic cameras (including vehicle detection and count) found at various locations along King Street.
Dynamic curb		**MM.13**	**Dynamic Curb Digital User Interface:** Digitized availability, regulation, and pricing information will be consumed by connected vehicles through an API or pushed through bluetooth, WiFi, DSRC or 5G.	Mobility/ Entry	Wave	**De-identified:** Broad trend information on occupancy/ duration to inform regulations or pricing. **Personal info (Restricted - not published for privacy reasons):** opt-in location data to locate parking, opt-in information needed for parking payment	The closest precedent is for parking, not curb drop-off and pick up. In Toronto, various parking applications such as GreenP, Honk Mobile, HangTag and others are operating.

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Dynamic curb						(e.g. payment information, vehicle/licence plate information), opt-in information needed for in-vehicle communication.	
Dynamic curb		**MM.14**	**Digital Signage:** Digitized availability, regulation and pricing information, will be displayed on e-ink or LCD signage and available for navigation app or fleet ingestion through an API.	Info	N/A	**N/A** - Digital signs receive information from the Traffic Management System. No data collected.	Usually static signs are used on sidewalks, but variable digital signs are found on the downtown stretch of the Gardiner Expressway.

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Dynamic curb		MM.15	**LED pavement for flexible curbs:** LED lights help signal changes in street use, making it easier and safer to flex space that would be variably allocated to vehicles or public space.	Mobility	N/A	**N/A** - Lighting at flexible curb edges only receives information from the Traffic Control System. No data collected.	Lighted pavement can be seen at Sugar Beach Park as part of an interactive water feature.
Managed Satellite Parking with eValet Service	Fewer unnecessary cars on the roads, safer and more enjoyable for pedestrians.	MM.16	**e-Valet Digital User Interface:** Access to e-valet parking services through digital user interface.	Info/Entry	Wave	**Personal info (Restricted - not published for privacy reasons):** Opt-in user account linking car with request times and spots.	Multiple parking valet services in Toronto provide service transactions via text or user interface.

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Weather-Responsive Heated pavement	Increased ability to use non-GHG emitting modes of transportation (pedestrian, bicycle) year-round. Heated pavement would conserve energy by only turning on when there is a forecasted storm in the near future and turning off when it detects dry pavement (or simply after a certain amount of time has passed after a weather event).	**MM.17**	**Road surface sensors** to detect if sidewalk/ road/bike lane surface is wet, has snow or slush etc.	Mobility/ Energy Efficiency	Water	**Non-personal:** Data on road/sidewalk/bike lane surface moisture/temperature at specific locations. **Personal Info:** None.	Heated sidewalks for snow and ice prevention, using both electric and hydronic heat delivery and a variety of commercial control systems including road surface moisture detection, have multiple precedents in Toronto.
		MM.18	**Pavement Heating Elements:** Control System for the heated pavement elements.	Mobility	N/A	**N/A** - Heating elements use data to optimize energy efficiency. No data collected.	

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Enhanced Electric Vehicle Charging	Provide more convenient electric vehicle charging by wireless, public charging facilities at bus stops, and/or Pick-up/Drop-off locations.	**MM.19**	**Electric Vehicle Charging Stations:** Plug-in EV charging stations and inductive charging facilities.	Mobility/ Energy Efficiency	Wave	**Personal info (Restricted - not published for privacy reasons):** Users would opt-in to a subscription (i.e. payment data) for a service that would allow them to charge their vehicles with private infrastructure.	Plug-in EV charging stations are commonly found in parking garages around Toronto. No known precedent for induction charging facilities.
Mobility as a Service (MaaS)	Make public transit, ride-sharing, and active modes of transport less expensive and more convenient than owning a car: more residents choose not to own private automobiles; fewer employees choose to drive to work; lower household expenditures on mobility.	**MM.20**	**MaaS User Platform:** A unified mobility package that offers a variety of mobility options.	Mobility	N/A	**Non-personal:** Real-time information of mobility service (e.g. next bus arrival, bike-share availability) and infrastructure conditions (e.g. road congestion). **Aggregate:** total quantity of passes/ rides/rental sessions that subscribers have purchased collectively.	No known precedents in Toronto (although there are precedents in Europe).

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Mobility as a Service (MaaS)						**De-identified (Restricted - not published for privacy reasons):** A user account system that keeps track of subscribers' level of subscription and remaining balance (e.g. how many more car-share sessions is this subscriber entitled to use before end of the subscription period); receives requests from third-party user interfaces or mobility service operators that check the user's remaining balance.	

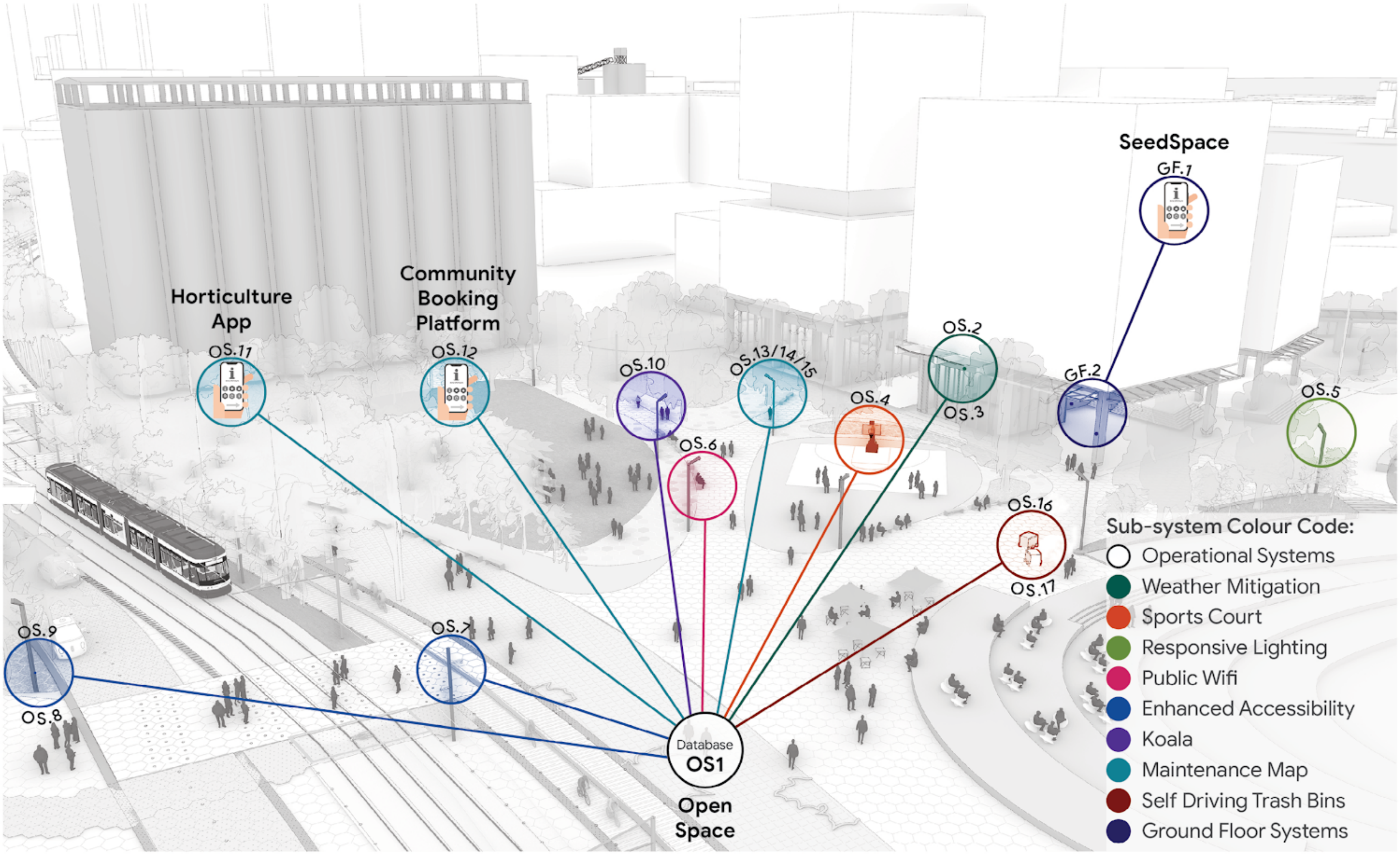
Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Mobility as a Service (MaaS)						**Personal info (Restricted - not published for privacy reasons)**: Users opting-in to a Unified Mobility Subscription would provide payment details to pay for their subscription. Users would opt-in to provide their GPS location for more convenient trip planning, real-time updates, and other functionality.	

Table: Mobility Management Systems — Queens Quay Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Mobility as a Service (MaaS)	Make public transit, ride-sharing, and active modes of transport less expensive and more convenient than owning a car: more residents choose not to own private automobiles; fewer employees choose to drive to work; lower household expenditures on mobility.	**MM.21**	**Bike and Scooter GPS locators:** Apps where bikes/scooter self-report GPS locations.	Mobility	Wave	**Personal info (Restricted - not published for privacy reasons):** Users would opt-in for a subscription to an app where they report their own GPS location for metrics and other benefits.	Toronto Bikes application reports GPS locations of bikes that are docked at their stations.

Figure: Parks, Streetscapes and Ground Floor Systems — Silo Park Example



Note: For clarity, the coloured markers indicate a single location where the referenced technology would be installed. The actual number of each type of sensors would be shown in a more detailed plan set.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Public Realm GIS Database	Aggregate and optimize Public Realm operations, asset, and usage data.	**Data Base OS.1**	**Database:** Central database that collects and stores info with a digital user interface.	Info	N/A	Real-time digital geospatial repository showing condition of the public realm that supports operational uses, including horticulture maintenance and space booking apps. Data received is from multiple system components, for example: evapotranspiration, plant health, moisture, waste bin volume, air quality, asset locations, usage, damage status, sound volumes.	No known precedent in Toronto, although many agencies have general asset databases.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Adaptive Weather Mitigation	Increase time people can comfortably spend outdoors.	**OS.2**	**Weather sensors:** Instruments that collect microclimate data about wind, temperature, rain, and sunlight.	Accessibility/ Info	Light Water Air	**Non-personal:** microclimate data. **Personal Info:** None.	Weather stations are commonplace in urban centers. One can be seen above the mall entrance at the intersection of Yonge and Dundas.
		OS.3	**Dynamic Canopy:** Weather-responsive shading and outdoor comfort elements that would be deployed in response to weather events.	Accessibility	N/A	**N/A** - Dynamic Canopies use data to respond to weather conditions. No data collected.	The Rogers Centre has one of the most impressive dynamic canopy structures in the world that allows for enjoyment of the facility in all seasons.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Sports Court	Maximize the diversity of uses within the park.	**OS.4**	**Push Button:** Low-cost lighting makes it possible to have a single court embedded with light that could redefine its space for basketball or street hockey at the push of a button.	Switch	N/A	**Non-personal:** Frequency of sport court use type. **Personal info:** None.	LED courts for indoor sports have been installed in Toronto.
Responsive Lighting	More efficient use of energy for streetlights.	**OS.5**	**Light Level Sensors:** Street lights adapt to ambient light levels to maintain necessary lumens on the street and sidewalk.	Energy Efficiency	Light	**Non-personal:** Ambient light levels, and street light energy use. **Personal Info:** None.	Light level sensors were observed at Dundas Square and have been installed on the new washroom structure in Bellevue Park.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Public Wi-Fi	Better community programs and broadband access.	**OS.6**	**User Interface:** Public Wi-Fi helps tackle the digital divide and enable new experiences in physical space, such as augmented- or virtual-reality exhibitions.	Connectivity	Wave	**Personal info (Restricted - not published for privacy reasons):** Users consent to User Agreements to access public Wi-Fi. **Aggregate, de-identified:** Wi-Fi Operator may collect data regarding number of users, bandwidth usage, etc.	There are numerous examples of free public Wi-Fi being provided in Toronto, including Toronto Libraries, the subway and Union Station.
Public Realm Enhanced Accessibility Features	More inclusive street design and improved mobility for people who are visually impaired through use of wayfinding beacons and responsive sounds.	**OS.7**	**Navigation Beacons:** Beacons emit signals to broadcast navigational information that can be picked up by smartphones using apps such as BlindSquare for navigational assistance.	Accessibility	N/A	**N/A** - Navigation Beacons use data to provide direction. No data collected.	Beacons to assist visually impaired pedestrians are installed in the Yonge and St. Clair neighbourhood.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Public Realm Enhanced Accessibility Features		**OS.8**	**Pedestrian Detection:** Motion detector communicating with localized speaker.	Accessibility	Light	**Non-personal:** Detection of the presence of a pedestrian. **Personal Info:** None.	No known precedent in Toronto.
		OS.9	**Speaker:** Responsive sounds alert visually impaired to street conditions.	Accessibility	N/A	**N/A** - Speakers use data to broadcast information. No data collected.	No known precedent in Toronto.
Koala	Improve operations of connected devices.	**OS.10**	**Device Operational Data Collection:** Provide a universal mount for urban tech devices to be more easily installed and maintained. That collects data for verification, energy consumption, and device health data of the various connected devices.	Info	Wave	**Non-personal (Restricted data - not published):** Authentication information, timestamps, etc. Security/ anomaly detection. **Transactional Data:** Aggregate: bandwidth/ power usage. **Personal Info:** None.	There is no standard or product that provides all three physical mounting, power, and connectivity features as a complete solution in Toronto.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Koala							Traditional installation consists of individual devices custom-mounted on public infrastructure each with dedicated power and digital connections.
Real-time digital geospatial repository showing condition of the public realm (Maintenance Map)	Collect public realm use data, including programming, usage, etc. to support management and operations.	**OS.11**	**Horticulture Maintenance App**	Ecology	N/A	**Non-personal:** Maintenance records, plant information; data collected about the planting site and other growing conditions. **Personal info (Restricted - not published for privacy reasons):** Data on horticulture staff that are using the app to support their maintenance activities.	No known precedent in Toronto for horticulture, although agencies have general asset databases.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Real-time digital geospatial repository showing condition of the public realm (Maintenance Map)		**OS.12**	**Community Booking Platform**	Info	N/A	**Non-personal:** Reservation date, time, desired use. Data on patterns of actual usage and demand. **Personal info (Restricted - not published for privacy reasons):** User opts in to provide reservation holder name, contact info	City of Toronto Parks, Forestry and Recreation has an online booking platform for select community facilities.
		OS.13	**Air Quality Sensors:** Monitor air quality to detect pollutants and unsafe conditions	Enforcement/ Safety	Air	**Non-personal:** CO2, CO, VOC, lead detection **Aggregate:** aggregated for number of occurrences thresholds exceeded. **Personal Info:** None.	Air quality sensors are installed around Toronto and can be viewed at The World Air Quality Project website.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Real-time digital geospatial repository showing condition of the public realm (Maintenance Map)		OS.14	**Particulate Matter Sensors:** Air sensors to detect particulate matter	Enforcement/ Safety	Air	**Non-personal:** PM 2.5, PM 10. **Aggregate:** Aggregated for number of occurrences thresholds exceeded. **Personal Info:** None.	Air quality sensors are installed around Toronto and can be viewed at The World Air Quality Project website.
		OS.15	**Sound Pressure Level Meters:** Monitor noise levels to ensure tenants are adhering to an acceptable nuisance threshold.	Enforcement/ Safety	Wave	**De-identified:** Noise level detection (no sound recording). **Aggregate:** Aggregated for number of occurrences thresholds exceeded. **Personal Info:** None.	Toronto Public Health conducted an Environmental Noise Study in 2016-2017 by deploying noise level meters in various locations around Toronto.

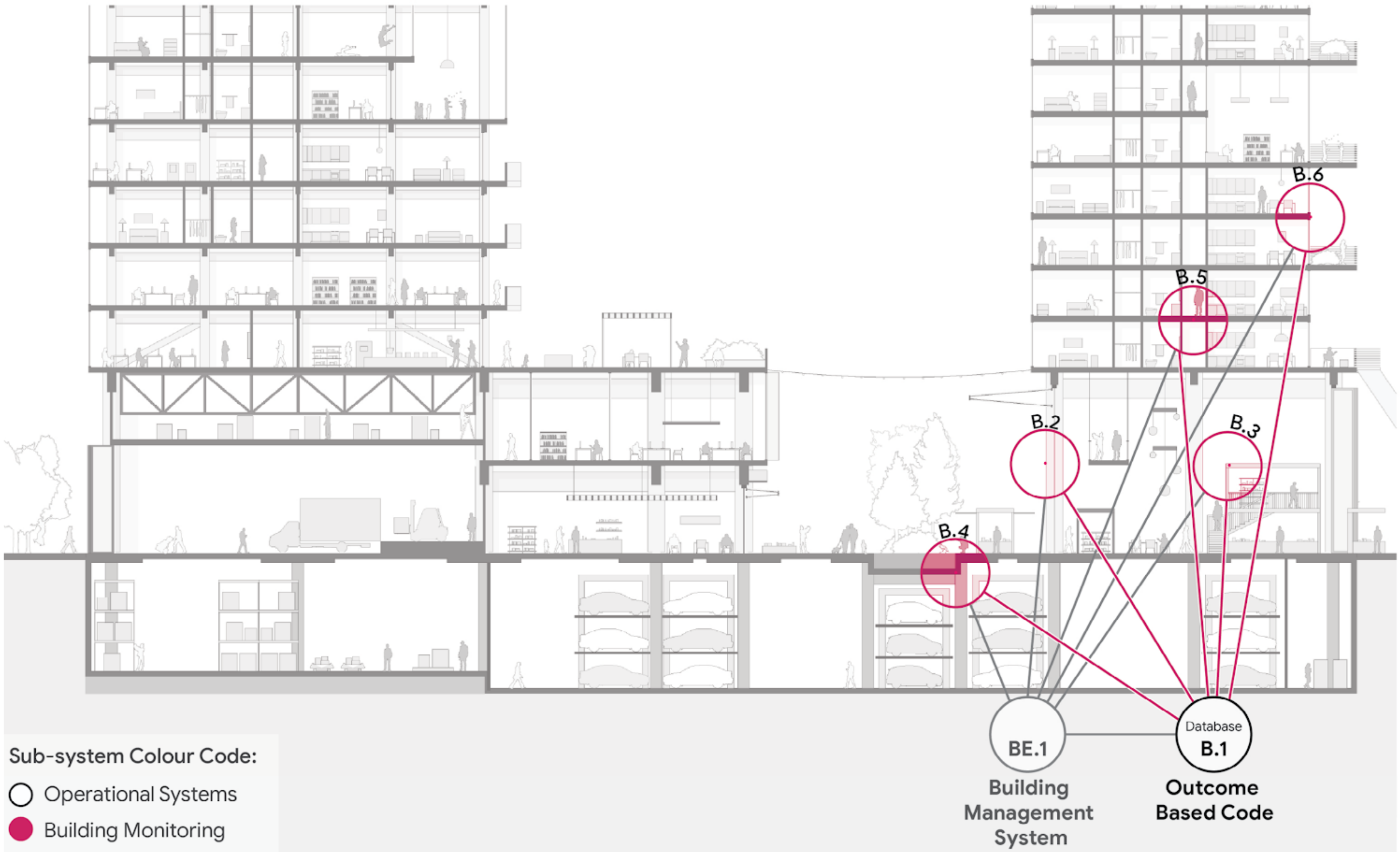
Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Self-Driving Trash Bins	Prevent litter conditions that reduce quality of the public realm and increase maintenance costs. Self-driving trash bins equipped with volume sensors can return to centralized waste disposal inlets to empty themselves.	**OS.16**	**Volume Sensors:** Volume sensors will indicate when the trash bins should empty itself.	Waste	Light	**Non-personal:** Trash volume data **Personal Info:** None.	No known precedent in Toronto.
		OS.17	**Navigation Sensors:** Optical sensors to allow self-driving trash bins to navigate through the public realm.	Mobility	Light	**Non-personal** - GPS location of self driving trash bins reported to Waste Management Operational System **Personal Info:** None.	No known precedent in Toronto.

Table: Parks, Streetscapes and Ground Floor Systems — Silo Park example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Flexible retail platform - "Seed Space"	Increase ground floor activity by making it easier for businesses to launch and operate in brick and mortar. Support businesses by identifying co-tenancy, co-programming, and co-merchandising opportunities.	**GF.1**	**Seed Space APP**	Planning & Decision-making	N/A	**Non-personal**: Space size, availability (launch use case); hours and type of business and aggregated tenant turnover rates (operations use case) **Non-personal (Restricted - not published for commercial reasons):** Leasing, rent, or other commercially sensitive data (launch use case)	Precedents for various aspects of Seed Space do exist, but not as a single platform. Examples include: Platforms like Storefront help tenants find ground floor space. Uppercase offers retail-as-a- service offerings. Platforms like FlexDay provide co-programming opportunities.
		GF.2	**Footfall Sensors:** thermal, LIDAR or infrared sensors provide tenants and landlords with an understanding of foot traffic at different times of day and week.	Planning & Decision-making	Light	**Aggregated and/or de-identified:** Pedestrian counts and heatmaps by time of day/ week	Sensors, cameras, and tools (Wi-Fi, beacons, location services) that interact with mobile devices and provide movement data are found in major malls in Toronto.

Figure: Outcome-Based Code Building Systems - Site 1 Example



Note: For clarity, the coloured markers indicate a single location where the referenced technology would be installed. The actual number of each type of sensors would be shown in a more detailed plan set.

Table: Outcome-Based Code Building Systems — Site 1 example

Subsystem	**Objective**	**No.**	**Component Description**	**Purpose**	**Sensor Types**	**Data Types**	**Toronto Precedent**
Building Management System	**See Building Energy Management System Diagram and Table**						
Outcome-Based Code Database	New approach to planning approval which would allow for different uses to be co-located and thus encourage more diverse space utilization.	**Data Base B.1**	Database that measures building performance by monitoring and measuring energy usage, equipment performance, indoor air quality, etc.	Enforcement	N/A	The Outcome-Based Building Code Monitoring subsystem uses data inputs from the Building Monitoring subsystems and Building Energy Management subsystems to perform system functions.	Nuisance / noise monitoring is typical in site construction to limit disruption to neighboring property, but it is not a common practice to monitor interior conditions. Similar monitoring and reporting occurs often in industrial settings, but is not commonly utilized in residential or office settings.
Building Monitoring	Allow for a more diverse mix of tenants in a given building. Increase the building performance by monitoring and measuring building conditions.	**B.2**	**Air Quality Sensors:** Monitor air quality to detect pollutants and unsafe conditions.	Enforcement	Air	**Non-personal (Restricted):** CO_2, CO, VOC, lead detection. **Aggregate (Restricted):** aggregated for number of occurrences thresholds exceeded. **Personal info:** None.	

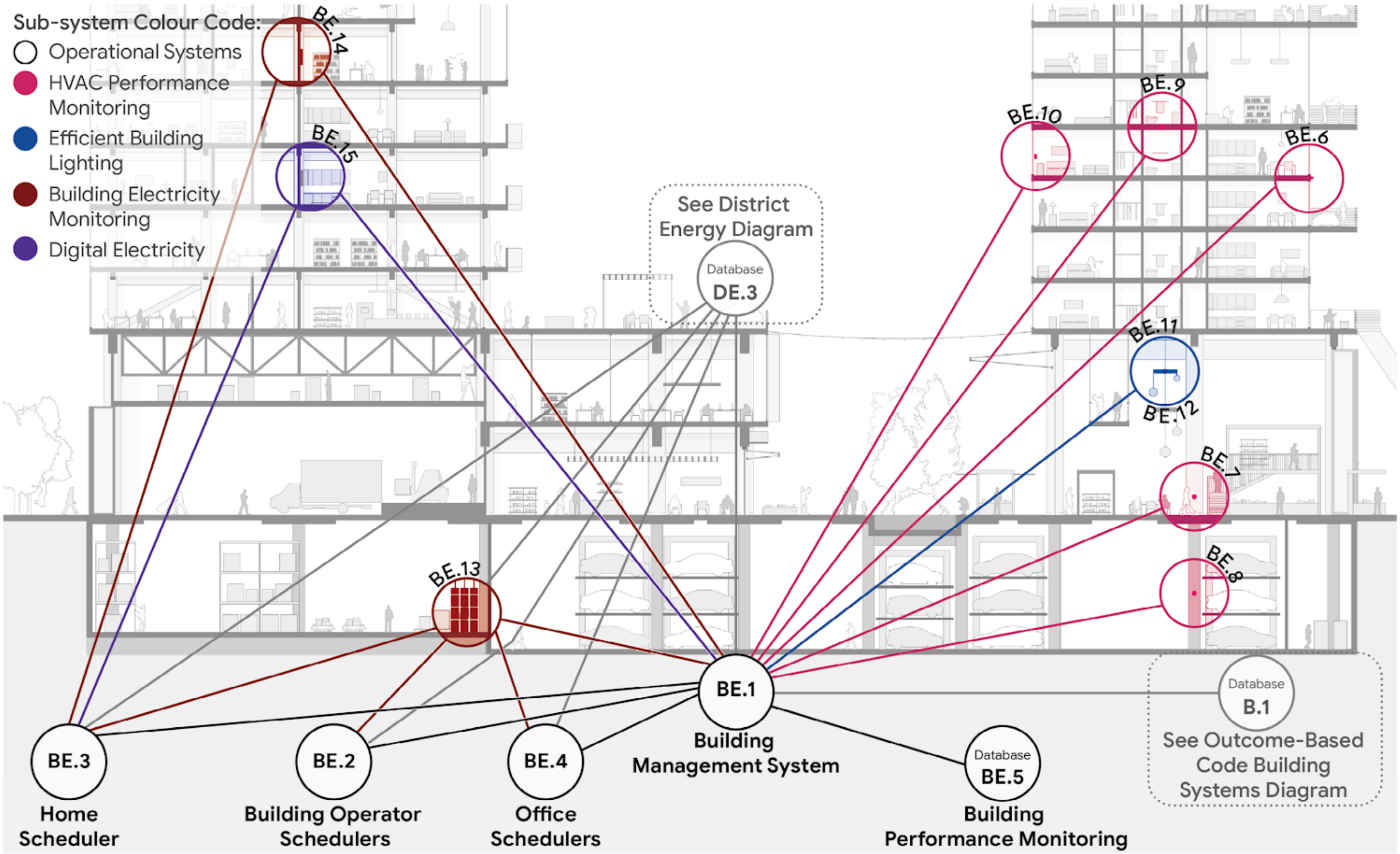
Table: Outcome-Based Code Building Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Building Monitoring		B.3	**Odour Sensors:** Monitor odours in building environments to minimize nuisances.	Enforcement	Air	**Non-personal (Restricted):** Odour data. **Aggregate (Restricted):** Aggregated for number of occurrences thresholds exceeded. **Personal info:**None.	
		B.4	**Vibration sensors:** Monitor building vibration to measure unsafe conditions.	Enforcement	Wave	**Non-personal (Restricted):** vibration detection. **Aggregate (Restricted):** aggregated for number of occurrences thresholds exceeded. **Personal info:**None.	
		B.5	**Load Sensors:** Monitor building loading/capacity to measure structural integrity and unsafe conditions.	Enforcement	Weight/ Strain Gauge	**Non-personal (Restricted):** floor plate loading. **Aggregate(Restricted):** Aggregated for number of occurrences thresholds exceeded. **Personal info:** None.	

Table: Outcome-Based Code Building Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Building Monitoring		**B.6**	**Noise Sensors:** Monitor noise levels to ensure tenants are adhering to an acceptable nuisance threshold.	Enforcement	Wave	**De-identified (Restricted):** Noise level detection (no sound recording). **Aggregate (Restricted):** Aggregated for number of occurrences thresholds exceeded. **Personal info:** None.	

Figure: Building Energy Management Systems - Site 1 example



Note: For clarity, the coloured markers indicate a single location where the referenced technology would be installed. The actual number of each type of sensors would be shown in a more detailed plan set.

Table: Building Energy Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Outcome Based Code Operational System	**See Outcome Based Code Building Systems Diagram and Table**						
Building Management System (BMS)	Increase ease of building operations and life-cycle management by monitoring and maintaining the built environment using a digital model to inform and document facilities management.	**Operational System BE.1**	Computer-based platform that automates building operations	Information	N/A	The Building Management System uses data inputs from the Building Energy Management subsystems, the Outcome-Based Code subsystems, and other subsystems to perform system functions.	These systems are widely implemented throughout Toronto. Less common is the use of an original digital model to aid with building maintenance after the building opens.

Table: Building Energy Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Building Operator Scheduler	Lower electricity use during peak hours. More customer control over utility costs.	**Operational System BE.2**	Optimizes control of central building systems, home owner-controlled systems, and tenant-controlled systems based upon the actual and predicted inputs of occupancy, weather, and energy price, to eliminate energy waste and defer energy consumption until off-peak hours, when fossil fuel-fired power plants are not in use.	Energy Efficiency	N/A	Schedulers receive data inputs from the Building Energy Management subsystems such as HVAC Performance Monitoring, Efficient Building Lighting, Building Electricity Monitoring, Digital Electricity and the Dynamic Rate Engine to optimize end user energy use. **Personal info (Restricted data not published for privacy reasons):** System inputs will include personal data, which would be restricted and not published for privacy reasons.	Building Management Systems and smart lighting, thermostats and shades all have automation capabilities. However, these systems are not currently integrated in most buildings, nor do they respond to utility price, occupancy or weather automatically.
Home Scheduler	Lower electricity use during peak hours. More customer control over utility costs.	**Operational System BE.3**		Energy Efficiency	N/A		London Hydro has tested remote load control of home owner devices in response to electricity price in 1600 homes.

Table: Building Energy Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Office Scheduler	Lower electricity use during peak hours. More customer control over utility costs.	**Operational System BE.4**	Optimizes control of central building systems, home owner-controlled systems, and tenant-controlled systems based upon the actual and predicted inputs of occupancy, weather, and energy price, to eliminate energy waste and defer energy consumption until off-peak hours, when fossil fuel-fired power plants are not in use.	Energy Efficiency	N/A	Through further system development, Sidewalk Labs will identify any data that the schedulers would need to export to optimize district energy performance. All design would be subject to a detailed Responsible Data Use Assessment process.	Commercial tenant spaces have an increasing amount of smart systems and devices, including BMSs. However, they typically lack the integration with other systems that is proposed here.

Table: Building Energy Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Building Performance Monitoring Platform ("Perform")	A digital tool to compare real-time building energy usage against an energy budget, based on Toronto Green Standard performance targets, that adjusts dynamically based on occupancy, the weather, and other factors.	**Data Base BE.5**	Database with visualization and reporting functionality to aggregate building performance data to measure against targets.	Agency	N/A	N/A - This system would use data inputs from the market on energy supply, data voluntarily provided by building operators, public data required by government policy, and data from other subsystems mentioned under Building - Energy Management above.	Ontario requires annual benchmarking on energy efficiency; this would be a much more detailed version of that, and for the same purpose.
HVAC Performance Monitoring	Monitor building HVAC system performance to optimize thermal energy use and lower peak demand.	**BE.6**	**Outside Air Temp (wet bulb):** Building level OA temperature and humidity sensors.	Info/ Energy	Air	**Non-personal:** OA & Humidity data. **Aggregate/ de-identified:** OA & Humidity data **Personal info:** None.	See examples of Toronto existing buildings in:Section 2.2.1 Figure - Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 2

Table: Building Energy Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
HVAC Performance Monitoring		BE.7	**Space Temperature:** Zone temperatures to inform building controls and optimization	Info/ Energy	Air	**Non-personal:** Temperature data **Aggregate/ de-identified:** Temperature data. **Personal info:** None.	Power Infrastructure, Lighting Controls, Heating Ventilation Air-conditioning (HVAC) Systems
		BE.8	**Decibel sensors:** Used to monitor equipment noise levels that could impact user comfort or signify faulty equipment	Info/ Energy	Sound	**Non-personal:** volume level **Aggregate/ de-identified:** volume level. **Personal info:** None.	
		BE.9	**Leak sensors:** Used to detect faulty plumbing and mitigate potential water damage	Info/ Energy	Water	**Non-personal:** Flow rate data **Aggregate/de-identified:** Flow rate data. **Personal info:** None.	

Table: Building Energy Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
		BE.10	**Thermal Energy Metering:** Metering of tenant-level thermal energy use through smart thermostats or thermal meters.	Energy Efficiency	Wave/ Water	**De-identified (Restricted data not published for privacy reasons):** Tenant-level thermal energy metering.	
Efficient Building Lighting	Lower energy consumption and cost by monitoring building lighting use and efficiency.	**BE.11**	**Lighting Sensors:** On/off/ dim - control electricity use.	Energy Efficiency	Light	**Aggregate:** Aggregate, building-level energy use data **Personal info (Restricted - not published for privacy reasons):** Tenant-level lighting and occupancy data. Further system development is needed to identify the data required for Efficient Building Lighting to optimize energy use.	See examples of Toronto existing buildings in: Section 2.2.1 Figure - Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 2 Power Infrastructure, Lighting Controls, Heating Ventilation Air-conditioning (HVAC) Systems
		BE.12	**Occupancy:** Optical sensor to detect if there is a person or persons in an area.	Energy Efficiency	Light		

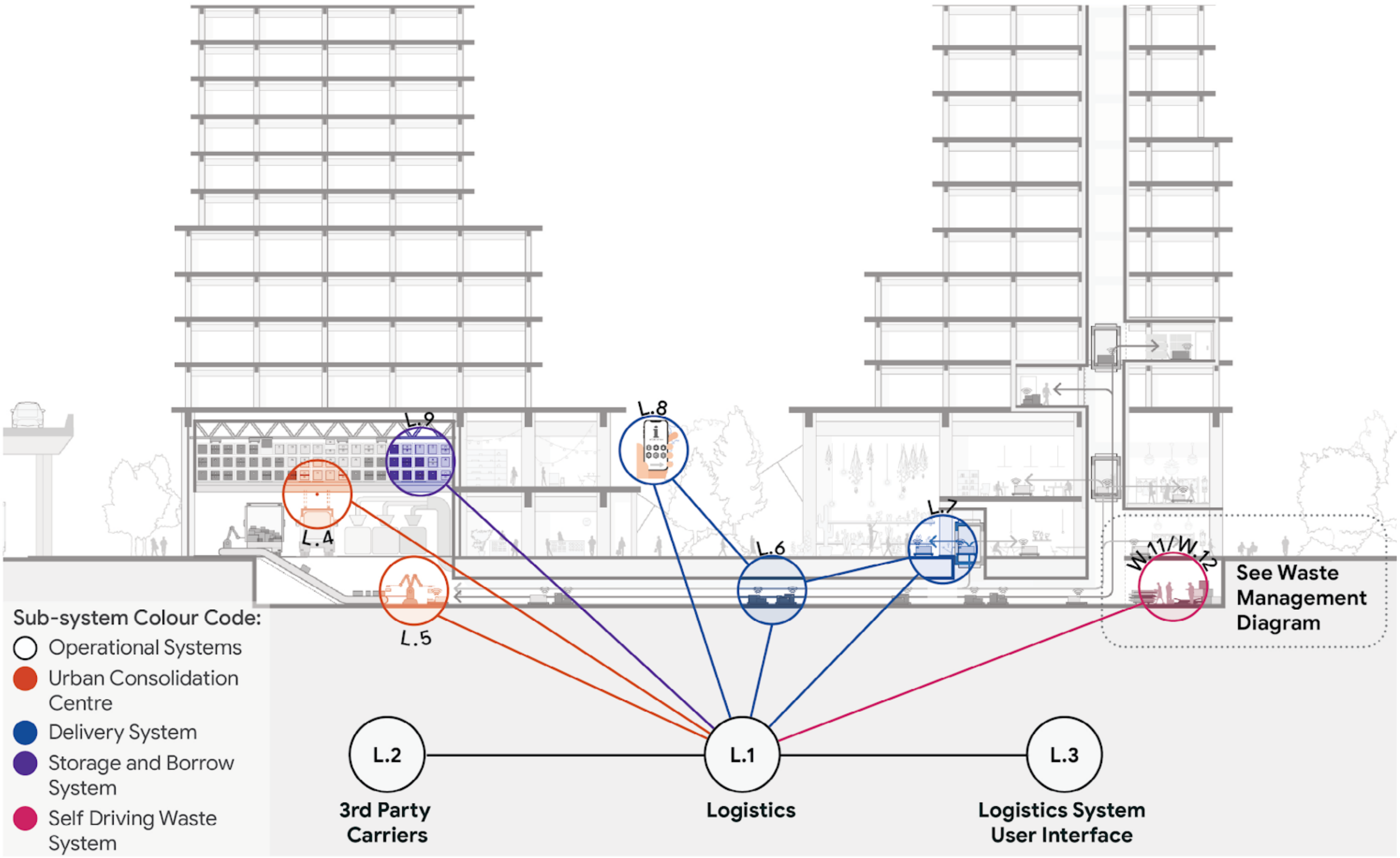
Table: Building Energy Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
Efficient Building Lighting						As this system is further designed, it would be subject to a detailed Responsible Data Use Assessment process.	
Building Electricity Monitoring	Lower peak energy demand by monitoring building electricity use (Grid, Solar, and Battery).	**BE.13**	**Building Electricity metering:** Used to monitor building-level electricity.	Energy Efficiency	Wave	**Aggregate:** Aggregate building-level energy use data.	See examples of Toronto existing buildings in: Section 2.2.1 Figure - Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 2 Power Infrastructure, Lighting Controls, Heating Ventilation Air-conditioning (HVAC) Systems

Table: Building Energy Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types	Toronto Precedent
	Lower peak energy demand by monitoring end-use electricity.	**BE.14**	**Sub-meters:** For suite-level metering that is unable to be accommodat-ed by DE.	Energy Efficiency	Wave	**Personal info (Restricted data not published for privacy reasons):** Tenant-level energy metering. Further system development is needed to identify the data required for Building Electricity Monitoring to optimize energy use. As this system is further designed, it would be subject to a detailed Responsible Data Use Assessment process.	
Digital Electricity	Improved metering capability. Increased electrical control of devices, and enables automated fault detection of plugged-in devices. Cost reduction to materials and building renovations.	**BE.15**	**Digital electricity metering:** Used to monitor energy on a more granular basis.	Energy Efficiency	Wave	**Aggregate:** Aggregate building-level energy use data. **Personal info (Restricted data not published for privacy reasons):** End-use level energy metering.	No precedent in Toronto. (The first major building powered by DE is slated to open in Fort Worth Texas in 2019.)

Figure: Logistics Systems — Freight Management System — Site 1 Example



Note: For clarity, the coloured markers indicate a single location where the referenced technology would be installed. The actual number of each type of sensors would be shown in a more detailed plan set.

Table: Logistics Systems - Freight Management System — Site 1 Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Logistics Operating System	Reduced traffic on the roads and more efficient housing units. Ease of shipping, deliveries, and discarding of waste. Consolidates data flows from all Logistics systems to operate the system.	**Operational System L.1**	**Logistics Operational System:** Operational System that optimizes logistics throughout the development area.	Logistics	N/A	The Logistics - Freight Operational System uses data inputs received from the Urban Consolidation Centre (UCC) & Delivery subsystem, Storage & Borrow subsystem, Specialized Waste subsystem, Third-Party Carriers' operational systems, and the Digital User Interface to perform system functions. **Aggregate and/or de-identified:** aggregate delivery, storage, borrow, and waste trends. **Personal Restricted data (not published for privacy reasons):** Users would provide the same minimum data provided to public and private carriers today (e.g. name, address) and could opt-in to set an individual profile with preferences for delivery and pickup as well as overall use of the digital platform. Users will be able to provide details on their personal preferences, such as bring to me, leave at my office, pick up winter clothes from storage when the temperature hits a certain level, etc.

Table: Logistics Systems - Freight Management System — Site 1 Example

Subsystem	**Objective**	**No.**	**Component Description**	**Purpose**	**Sensor Types**	**Data Types**
Logistics Operating System	Reduced traffic on the roads and more efficient housing units. Ease of shipping, deliveries, and discarding of waste. Consolidates data flows from all Logistics systems to operate the system.	**Operational System L.2**	**3rd Party Carriers Operational Systems:** 3rd Party carriers data interface.	Logistics	N/A	**Non-personal data:** Data from carrier tracking systems in order to integrate delivery tracking into Logistics Digital System. **Personal Info:** None
		Operational System L.3	**Digital user interface:** Provide customer interface for shipping, deliveries, storage, and borrow items.	Info/Entry	Wave	**De-identified:** Broad demographic information on how profiles are set up and managed. Storage: Broad trend information on types of items being stored and borrowed based on aggregate information. **Personal info (Restricted - not published for privacy reasons):** Delivery: Number/size/weight of items delivered to each address. Storage: stored items, the items they have borrowed, and their address for delivery.

Table: Logistics Systems - Freight Management System — Site 1 Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Urban Consolidation Center & Logistics Facilities	Reduce traffic on the roads. Create dolly and smart container use optimization through a central hub.	L.4	**Vehicle Detection:** Presence sensors for loading dock activity.	Logistics	Light/Wave	**Non-personal:** Inbound and outbound truck movement for scheduling deliveries and pickups. Also covers waste hauler pick-ups. **Personal Info:** None.
	Reduce traffic on the roads. Create dolly and smart container use optimization through a central hub.	L.5	**Barcode Scanning:** Conveyor and barcode sensors for package handling.	Logistics	Light	**Non-personal:** Detection of the presence of a package. **Aggregate:** Number of packages moving through the Center, weight and dimensions of each. **Personal Info:** None

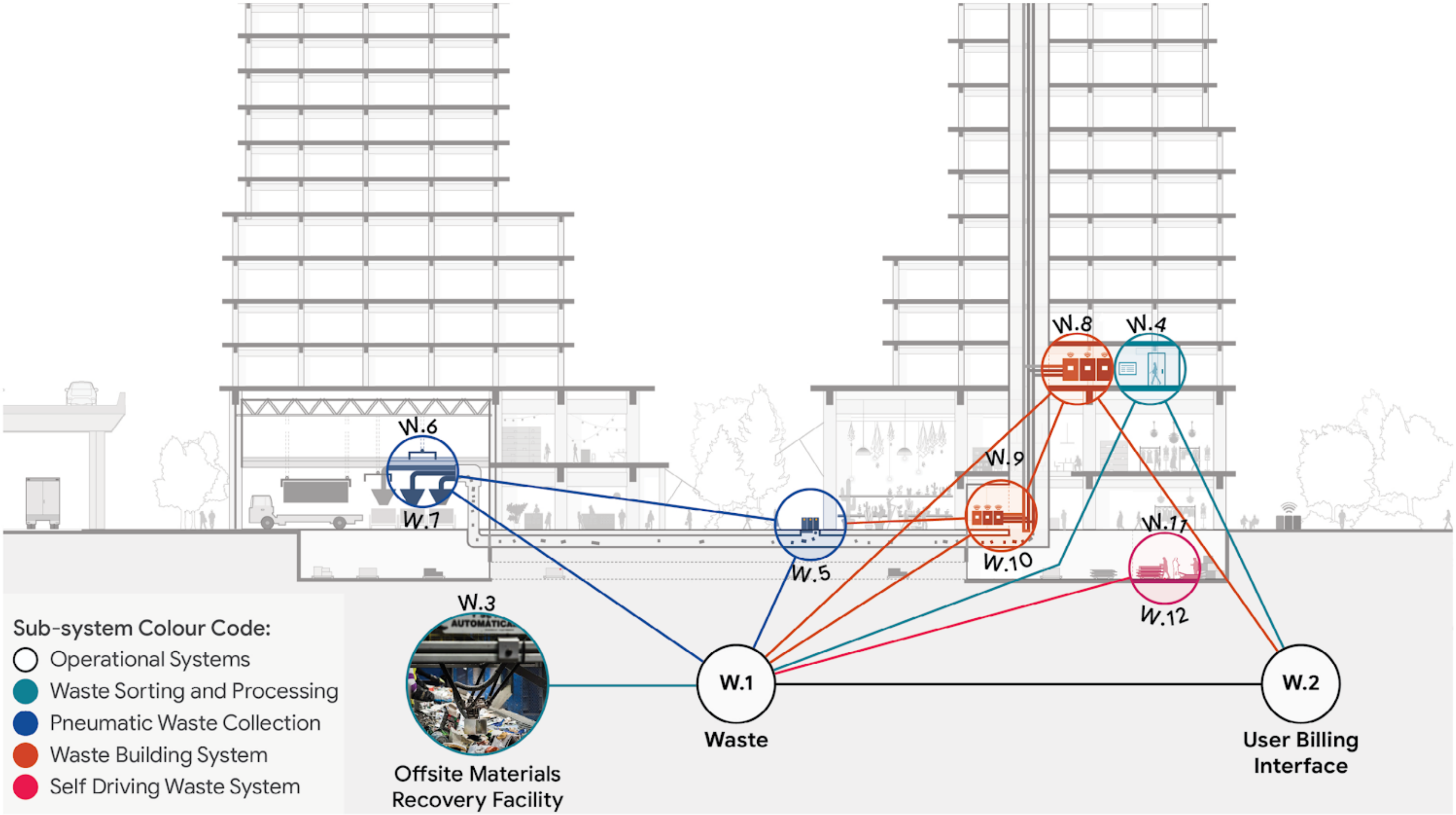
Table: Logistics Systems - Freight Management System — Site 1 Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Delivery System	Reduced traffic on the roads, simplified shipping with guaranteed safe and timely delivery, and more efficient housing units.	**L.6**	**Autonomous Navigation Sensors:** Autonomous Robot Dolly location tracking and guidance sensors.	Mobility	Light	**Non-personal (Restricted - not published for security reasons):** Parcel, container, and robot dollies' location data (which parcel is in which container and which containers are on which robot, as well as where they are located within the neighborhood), data from carrier tracking systems in order to integrate delivery tracking into Freight Control System. **Aggregate:** Number of parcels moving through the Urban Consolidation Centre, weight and dimensions of each parcel. Broad aggregate trends on mail/parcel volumes. **Personal Information (Restricted - not published for privacy reasons)**: Number/size/weight of parcels delivered to each address.

Table: Logistics Systems - Freight Management System — Site 1 Example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Storage and Borrow System	Increases free space in apartments and businesses; simplified storage.	L.9	**An ASRS or Vertical Lift**: used to house items delivered by smart containers and items available for borrowing. There are multiple companies that use different technologies for these systems. Almost all include a barcode and scanner process in addition to proprietary robotic sensors.	Logistics	Light	**Non-personal:** List of items borrowed (frequency, quantity, etc.) to determine what should be removed from or added to the borrow library. **Aggregate**: Broad trend information on types of items being stored and borrowed based on aggregate information. **Personal info (Restricted data not published for privacy reasons):** Users would have an associated profile which would include their stored items, the items they have borrowed, and their address for delivery.
Self Driving Waste System	**See Use Cases W.11 and W.12 on Waste Management Systems**					

Figure: Building Waste Management Systems - Site 1 Example



Note: For clarity, the coloured markers indicate a single location where the referenced technology would be installed. The actual number of each type of sensors would be shown in a more detailed plan set.

Table: Building Waste Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Waste Control System	Improve diversion of waste from landfill by providing users with feedback on recycling stream to improve sorting effectiveness. Improve operations and reduce truck trips. Consolidates data flows from all Waste systems.	**Operational System W.1**	**Waste Operational System:** Provide customer interface for waste management services. Smart chute will connect into waste pricing and billing platform to charge tenants for the waste that they deposit.	Waste	Wave	The Building Waste System uses data inputs from the Waste Sorting, Processing, & Monitoring subsystem, the Pneumatic Waste Collection subsystem, and the Digital User Interface to perform system functions.
		Operational System W.2	**User Billing Interface:** Digital user interface to pay waste bill and track landfill diversion performance	Info	N/A	**De-identified:** anonymized, unit-level waste production for comparing waste trends between typical sized units. **Personal info (Restricted - not published for privacy reasons):** Users would provide login credentials to access the Digital User Interface, and residential address to enable pay-as-you-throw billing.
Waste Sorting and Processing Monitoring	Improve landfill diversion and recycling contamination rates within the district.	**W.3**	**Computer vision software:** Used to distinguish one plastic from another and other non recyclable waste.	Waste	Video	**Aggregate and/or de-identified:** Waste volume, waste weights, waste classification (aluminum, fiber, HDPE, PET, thinfilm) for sorting using computer vision, contamination (miscellaneous, non-recyclable) data

Table: Building Waste Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Waste Sorting and Processing Monitoring						**Personal Info:** None.
		W.4	**Digital Displays:** Video displays at waste chutes communicate performance information about the districts recycling.	Waste/ Info	N/A	**N/A** - Digital Displays use data to provide information. No data collected.
Pneumatic Waste Collection System	Provide a neighbourhood waste collection infrastructure system that will enhance operational efficiencies, reduce building space needed for waste handling, and reduce truck traffic through the district.	**W.5**	**Outdoor inlets - Volume Sensor:** Sensor detects when waste chutes are full and activates the pneumatic collection system.	Waste	Light	**Non-personal:** Trash volume data and frequency of pneumatic activation **Aggregate Data:** Data sets from each inlet and district wide operations **Personal info:** None.
		W.6	**Weight Sensor:** Weights will also be taken at the waste terminal to verify totals, and used in operations for hauling cost and operational efficiencies.	Waste	Wave	**Non-personal:** Trash pressure scales measuring individual unit total weight per waste type **Aggregate Data:** Data sets from each building and district wide operations. **Personal info:** None.

Table: Building Waste Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Pneumatic Waste Collection System		**W.7**	**Pneumatic Operational Controls:** Used to track Operations and waste fraction information volumes/fractions, container change time, mechanical systems controls, odour sensing	Waste	Wave	**Non-personal:** Valve position, volume sensing (per building), air speed, number of discharges or valve openings per minute, waste fractions, peak volumes/fractions, container change time, mechanical systems controls, odour sensing. Inbound and outbound truck movement for scheduling waste hauler pickups. **Aggregate:** All waste volumes from the pneumatic system are building-level. **Personal info:** None.
Building Waste Systems	Provide the necessary building systems on each floor for convenient waste disposal.	**W.8**	**ID Verification:** Used by waste customers to open the trash chutes so that pay-as-you-throw billing can be allocated to the proper customer.	Waste/ Entry	Wave	**Personal info (Restricted data not published for privacy reasons):** Users will subscribe to a user agreement for waste services.

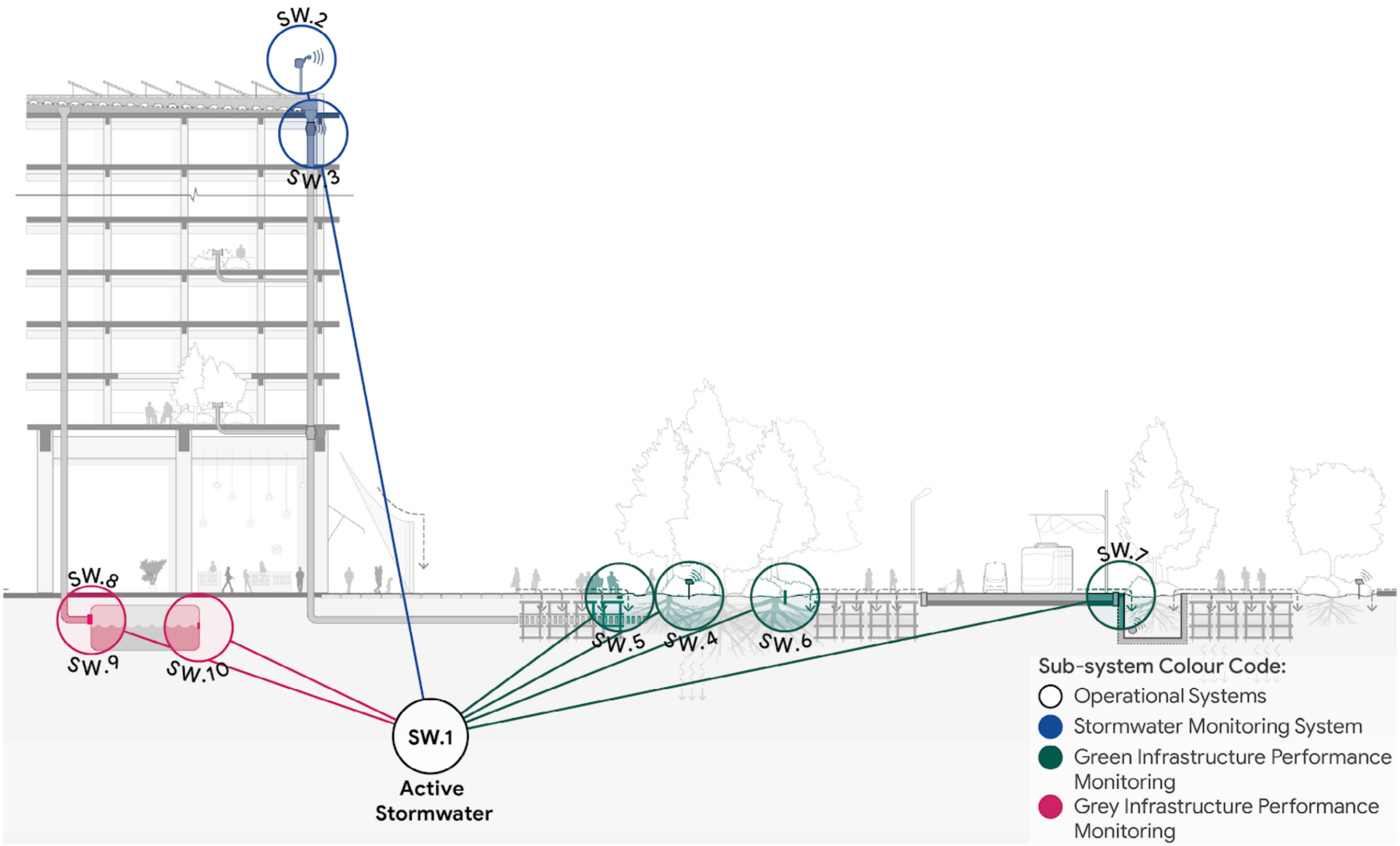
Table: Building Waste Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Building Waste Systems		W.9	**Volume Sensor:** Sensor detects when waste chutes are full and activates the pneumatic collection system.	Waste	Light	**Non-personal:** Trash volume data and frequency of pneumatic activation. **Aggregate Data:** Data sets from each building and district wide operations. **Personal info:** None.
		W.10	**Weight Sensor:** The valve room will have weight sensors that will measure the amount of landfill, recycling, and organics that are thrown away.	Waste	Wave	**Non-personal:** Trash scales (weight). **Aggregate Data:** Data sets from each building and district-wide operations. **Personal Info:** None.
Specialized Waste System	Keep trash separated as it was at the source point.	W.11	**Weight Sensor:** Pressure scales for weight calculation and respective billing.	Waste	Weight	**Non-personal:** Inbound and outbound truck movement for scheduling waste hauler pickups. Volume of specialized waste traveling through the system (location of waste, containers, dollies). **De-identified:** Broad demographic information on volume of cardboard and other non-pneumatic waste generated.

Table: Building Waste Management Systems — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Specialized Waste System	Electric self-driving dollies and smart containers would deliver cardboard (baled in each building basement before being transported) to the Logistics Hub.					**Aggregate Data**: Broad aggregate trends on volume of cardboard and other specialized waste generated. **Personal info (Restricted data not published for privacy reasons):** volume of outbound waste generated by each address
		W.12	**Autonomous Navigation Sensors and Autonomous Robot Dolly with self loading/unloading technology:** Same technology as freight dollies.	Mobility	Wave	**Non-personal** - GPS location of dolly reported to Logistics Operational System. **Personal Info:** None.

Figure: Active Stormwater Management System — Site 1 Example



Note: For clarity, the coloured markers indicate a single location where the referenced technology would be installed. The actual number of each type of sensors would be shown in a more detailed plan set.

Table: Active Stormwater Management System — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Active Stormwater Control System	Enable the use of green infrastructure to manage stormwater. Reduced cost and embodied energy for vertical development and redirection of investment into natural ecosystems located within the public realm.	**Operational System SW.1**	**Optimization and Controller Platform:** Cloud-based optimization and control systems that will be applied to the district.	Water/ Ecology	N/A	The Active Stormwater Operational System uses data inputs from the Stormwater Monitoring System, Green Infrastructure Performance Monitoring, and Grey Water Infrastructure Monitoring to perform system functions. **System operational data** Aggregate: Aggregate system operation data, including inflow/outflow of stormwater and water quality. Aggregate data (Restricted - not published for proprietary reasons): Aggregate, building-level data
Stormwater Monitoring System	Optimize the management of stormwater within the district to minimize grey infrastructure and use water as a resource to its highest and best use.	**SW.2**	**Weather Station:** A solar-powered weather station that sends data to the Optimization and Controller platform.	Water	Air/ Light/ Wave	**Non-personal:** microclimate data **Personal Info:** None.

Table: Active Stormwater Management System — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Stormwater Monitoring System		SW.3	**Automated Control Valve:** Valves are connected to a control panel and automatically operated in real-time by cloud-hosted software.	Water	Wave	**Non-personal:** Status - operational controls (valve and gate status) data **Personal Info:** None.
Green Infrastructure Performance Monitoring	Monitor and enhance maintenance of green infrastructure assets within the district.	SW.4	**Soil Sensors:** Monitoring real-time soil conditions in green infrastructure to manage irrigation demands and monitor plant health.	Ecology	Water	**Non-personal:** Moisture, salinity, and nitrogen data. **Aggregate:** District-wide data sets of soil moisture levels. **Personal Info:** None.
		SW.5	**Flow rate sensors:** Bioretention areas will be equipped with flow rate sensors to manage day to day operations.	Water	Water	**Non-personal:** Flow rate data. **Aggregate:** District-wide data sets of bioretention flow rates. **Personal Info:** None.

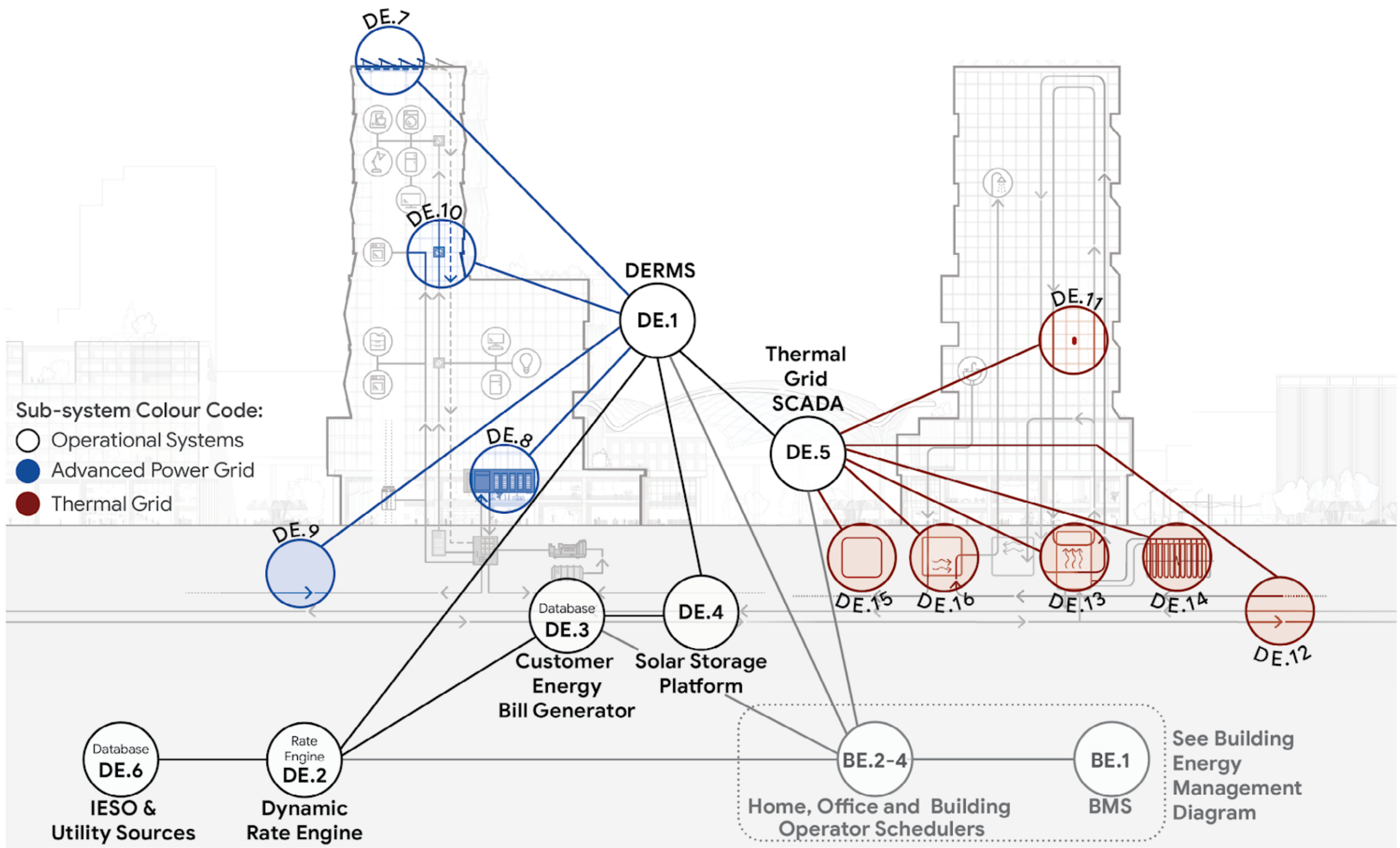
Table: Active Stormwater Management System — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Green Infrastructure Performance Monitoring		SW.6	**Water Level Sensors:** Bioretention areas will be equipped with water level sensors to manage day to day operations.	Water	Water	**Non-personal:** Water-level data. **Aggregate:** District-wide data sets of water levels. **Personal Info:** None.
Green Infrastructure Performance Monitoring		SW.7	**TSS Sensors:** Sensors to monitor Total Suspended Solids (TSS), including sediment, silt, and organic material,and temperature and conductivity to identify saliency.	Water/ Ecology	Light	**Non-personal:** TSS data. **Aggregate:** District wide data sets of TSS. **Personal Info:** None.
Grey Infrastructure Performance Monitoring	Where grey infrastructure systems are needed to meet city requirements, digital technology will be added to them to optimize their use and minimize the amount of grey infrastructure needed to meet requirements.	SW.8	**Automated Control Valve:** Valves are connected to a control panel and automatically operated in real-time by cloud-hosted software.	Water	Wave	**Non-personal:** Status - operational controls (valve and gate status) data. **Personal Info:** None.

Table: Active Stormwater Management System — Site 1 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Grey Infrastructure Performance Monitoring		SW.9	**Flow rate sensors:** Grey infrastructure systems will be equipped with flow rate sensors to manage day to day operations.	Water	Water	**Non-personal:** Flow rate data. **Aggregate:** District-wide data sets of bioretention flow rates. **Personal Info:** None.
		SW.10	**Water Level Sensors:** Grey infrastructure systems will be equipped with water level sensors to manage day to day operations.	Water	Water	**Non-personal:** Water level data. **Aggregate:** District-wide data sets of water levels. **Personal Info:** None.

Figure: District Energy Systems — Sites 3 and 4 example



Note: For clarity, the coloured markers indicate a single location where the referenced technology would be installed. The actual number of each type of sensors would be shown in a more detailed plan set.

Table: District Energy Systems — Sites 3 and 4 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Home, Office and Building Operator Schedulers	**See Building Management Systems**					
DERMS	Management of distributed energy resources connected to the grid to ensure reliability and optimize for GHG and cost outcomes.	**Operational System DE.1**	Manages local distributed energy resources (solar, battery and thermal grid, thermal resources) in response to dynamic hourly price signal.	Energy Efficiency	N/A	Operations System that uses data inputs from the Dynamic Rate Engine sub-system, the Thermal Grid sub-system, the Advanced Power Grid sub-system, and other subsystems to perform system functions.

Table: District Energy Systems — Sites 3 and 4 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Dynamic Rate Engine	Affordable electrification in order to achieve Climate Positive and Affordability. Send energy price signals to the district energy system	**Operational System DE.2**	Dynamic Rate Engine: Hourly energy price calculator that reflects wholesale cost of power generation and fixed infrastructure costs and other utility charges, which will increase proportionally with demand to properly implement load shifting strategies	Energy Efficiency	N/A	The Dynamic Rate Engine uses data inputs from the Independent Electricity System Operator (IESO) and other utility data sources to generate dynamic energy prices.

Table: District Energy Systems — Sites 3 and 4 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Dynamic Rate Engine		**Operational System DE.3**	Customer Energy Bill Generator takes the hourly price from the Rate Engine, net energy use and demand from the schedulers, and solar and storage information to create end user bills	Energy Efficiency	N/A	**Personal info (Restricted data not published for privacy reasons):** suite-level energy use and billing information for billing purposes.
Solar Storage Transaction Platform	Facilitate the transaction of distributed energy resources within the community to optimize value to each end user.	**Operational System DE.4**	Platform that will recommend and facilitate resident purchasing of pre-paid monthly shares of community-sited solar PV and battery capacity to reduce bills and insulate residents from the higher costs of peak-time electricity use.	Energy Efficiency	N/A	The Solar/Storage Transaction Platform would use data inputs from the Customer Energy Bill Generator, namely: **Personal info (Restricted data not published for privacy reasons):** suite-level energy use and billing information for billing purposes.

Table: District Energy Systems — Sites 3 and 4 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Thermal Grid SCADA	Affordable electrification in order to achieve Climate Positive and Affordability. District thermal grid control architecture to optimize district energy use.	**Operational System DE.5**	Thermal Grid SCADA system: Controls the thermal grid in coordination with the DERMS and the Dynamic Rate Engine to use the thermal grid as a demand management tool.	Energy Efficiency	N/A	The Thermal Grid aggregates data inputs from its subsystem components to perform system functions.
IESO & Utility Sources	Use market energy price data to generate dynamic hourly rates.	**DE.6**	Data Inputs of IESO hourly prices, day-ahead demand, and other utility bill charges.	Energy Efficiency	N/A	**Non-personal:** Data inputs of energy price.
Advanced Power Grid	Reduce spending on electricity and reduce GHG emissions.	**DE.7**	**Solar Panel Data Collection:** Digitally enabled equipment that monitors solar panel operations.	Energy Efficiency	Wave	**Non-personal:** Solar panel energy production, operational, and system health data. **Personal data:** None.

Table: District Energy Systems — Sites 3 and 4 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Advanced Power Grid		DE.8	**Battery Storage System Data Collection:** Digitally enabled equipment that monitors battery storage operations.	Energy Efficiency	Wave	**Non-personal:** Energy storage performance, operational, and system health data. **Personal data:** None.
		DE.9	**Grid Power Demand Data:** Campus meter that meters the amount of Toronto Hydro grid power taken from the distribution grid.	Energy Efficiency	Wave	**Non-personal:** Metering of energy taken from the Toronto Hydro power grid. **Personal data:** None.
		DE.10	**Smart Power Sub-Meters:** Suite Level energy meters.	Energy Efficiency	Wave	**Personal info (Restricted data not published for privacy reasons):** Suite-level measurement will require data collection. Will be addressed through further levels of design and RDUA process.

Table: District Energy Systems — Sites 3 and 4 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Thermal Grid	Affordable electrification in order to achieve Climate Positive and Affordability.	**DE.11**	**Thermal Energy Metering:** Suite-level smart thermostats that can meter the amount of thermal energy consumed by each unit.	Energy Efficiency	Wave/ Water	**Personal info (Restricted data not published for privacy reasons):** Suite-level measurement will require data collection. Will be addressed through further levels of design and RDUA process.
		DE.12	**Off-site Heat Exchange Data Collection:** Digitally enabled equipment that monitors off-site heat exchange equipment operations	Energy Efficiency	Wave/ Water	**Non-personal:** Heat exchange equipment operational and system health data **Personal data:** None.
		DE.13	**Parcel Level Thermal Equipment Data Collection:** Digitally enabled equipment that monitors battery storage operations	Energy Efficiency	Wave/ Water	**Non-personal:** Parcel level thermal energy system assets operational and system health data **Personal data:** None.

Table: District Energy Systems — Sites 3 and 4 example

Subsystem	Objective	No.	Component Description	Purpose	Sensor Types	Data Types
Thermal Grid		DE.14	**Geothermal Monitoring**	Energy Efficiency	Wave/ Water	**Non-personal:** Geothermal energy system assets operational and system health data **Personal data:** None.
		DE.15	**Neighborhood Energy Plant Data**	Energy Efficiency	Wave/ Water	**Non-personal:** Neighbourhood energy plant level thermal energy system assets operational and system health data **Personal data:** None.
		DE.16	**Building Waste Heat Recovery Data**	Energy Efficiency	Wave/ Water	**Non-personal:** Building level thermal energy system assets operational and system health data **Personal data:** None.

1.3.3 Developing the next level of detail for the integrated physical and digital plans

As outlined in section 1.2 above, upon MIDP approval, Sidewalk Labs would prepare a formal development application to be submitted to the City of Toronto. The conceptual designs as illustrated in the Master Innovation and Development Plan (MIDP), the Quayside Planning Supplement Technical Appendix, and the Conceptual Site Diagrams provided above, would be further developed, with site plans and section drawings brought to the next level of detail for the formal application by an integrated planning, architecture, and (building, civil, digital) engineering team. It is envisioned that site plans and section drawings would identify, classify, and map key digitally-enabled services encompassed within the Quayside Development Plan (as defined in collaboration with Waterfront Toronto and City staff), and that corresponding detailed data flow and system component drawings would be developed.

The following Mobility Management System — Dynamic Curb Subsystem Site Plan and Logical Data Flow Diagram provide nascent examples of the more comprehensive materials that could be developed for all applicable Quayside systems, as part of the initial development application submission. As the concept of illustrating digitally-enabled services alongside physical space plans and utilizing existing governmental review and regulatory processes to evaluate such plans is not current practice (Sidewalk Labs has not found any jurisdiction in which this is done), Sidewalk Labs looks forward to a cooperative process of working with Waterfront Toronto and the City to determine the appropriate scope of materials to be developed.

The Mobility Management System — Dynamic Curb Subsystem Site Plan shows the installation locations of all subsystems and components required to support the operations of dynamic curb management.

The Mobility Management System — Dynamic Curb Subsystem Logical Data Flow Diagram shows early-stage design for data flows between the components of the system, as well as management entities.

Figure: Mobility Management System, Dynamic Curb Subsystem — Site Plan View

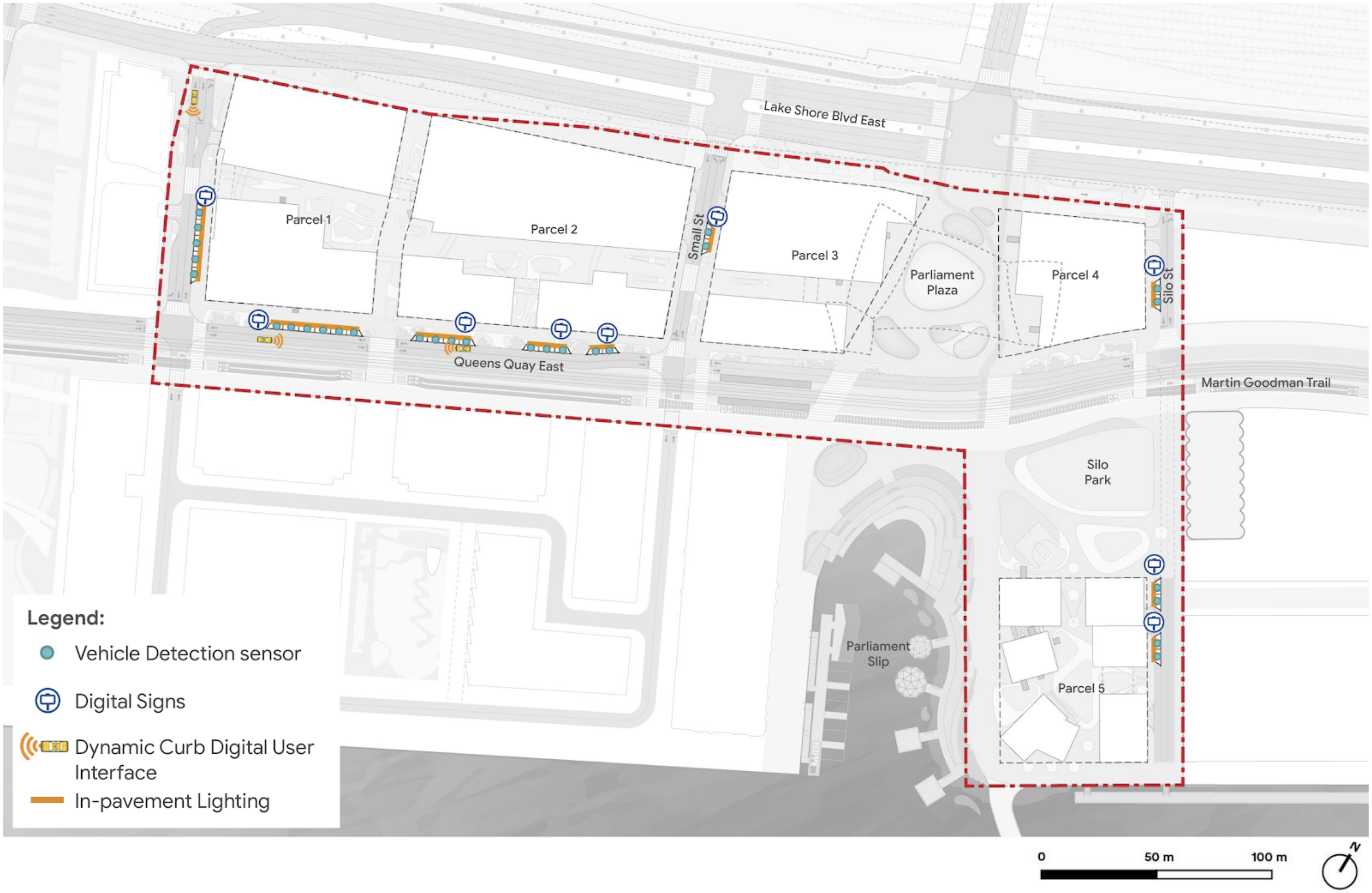
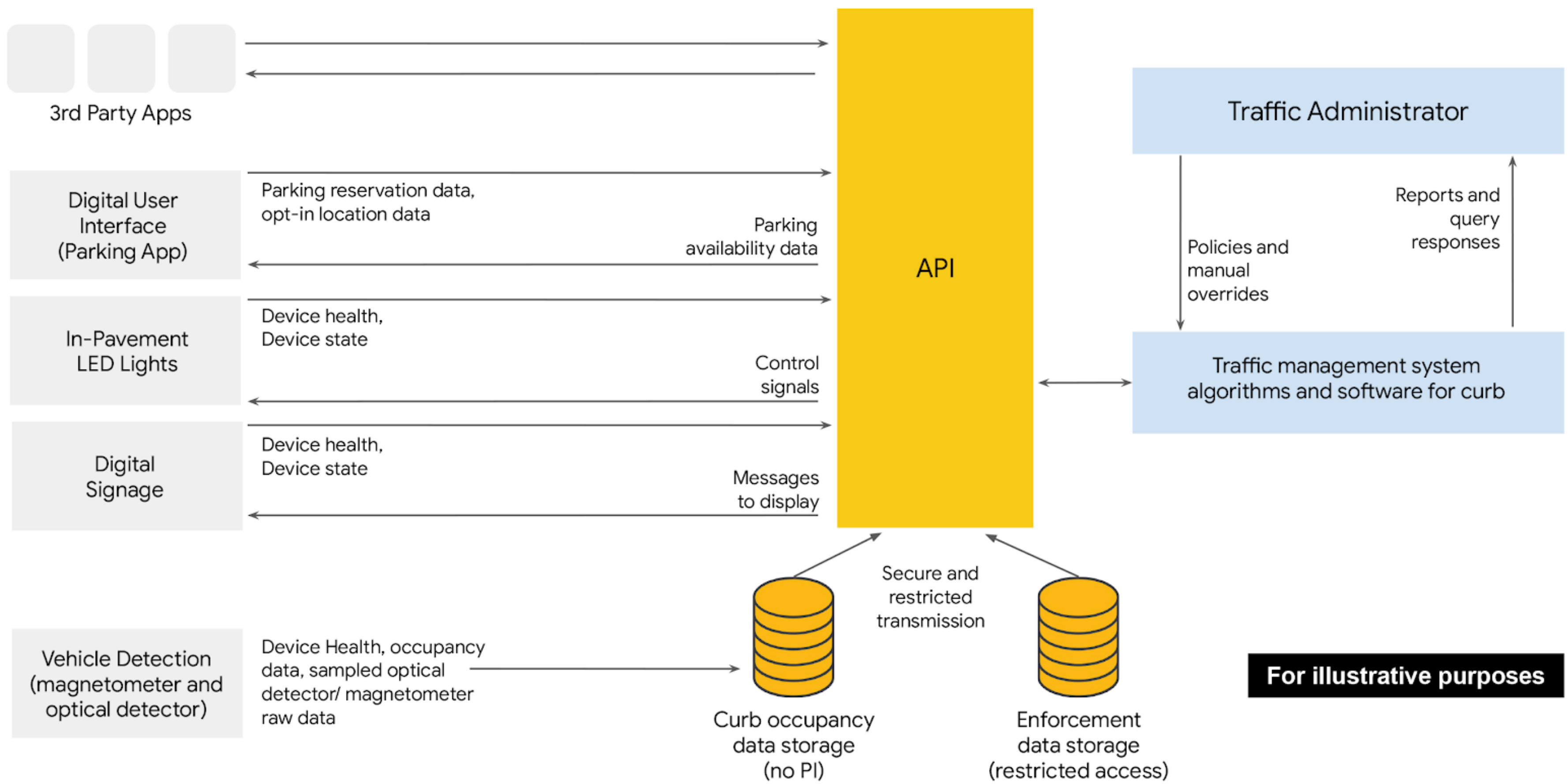


Table: Mobility Management System, Dynamic Curb Subsystem — Site Plan Legend Table

	Component Description	Purpose	Tech Types	Data Types
Vehicle Detection Sensor	Occupancy and duration detection: magnetic and optical sensors.	Mobility	Light	**Non-personal:** Detection of the presence of a vehicle. **Aggregate:** Occupancy of total spaces at the curb, average duration of pick-up/drop-off event. **Personal info:** None.
Digital Signs	Digitized availability, regulation and pricing information will be displayed on e-ink or LCD signage and available for navigation app or fleet ingestion through an API.	Info	N/A	**N/A** - Digital signs receive information from the Traffic Management System. No data collected.
Dynamic Curb Digital User Interface	Digitized availability, regulation and pricing information will be consumed by connected vehicles through an API or pushed through bluetooth, WiFi, DSRC or 5G.	Info/Entry	Wave	**De-identified:** Broad demographic information on how profiles are set up and managed. **Personal info (not published for privacy reasons):** opt-in information needed for parking payment (e.g. payment information, vehicle/licence plate information), opt-in information needed for in-vehicle communication
In-pavement Lighting	LED lights help signal changes in street use, making it easier and safer to flex space that would be variably allocated to vehicles or public space.	Mobility	N/A	**N/A** - Lighting at flexible curb edges only receives information from the Traffic Control System. No data collected.

Figure: Mobility Management System — Dynamic Curb — Logical Data Flow Diagram



1.4 Proposal for digital infrastructure that supports digitally enabled services and enables test bed conditions

1.4.1 The need for digital infrastructure

As detailed in the Master Innovation and Development Plan (MIDP), many of Sidewalk Labs' proposals for improving quality of life rely on digital technology. For a full list of the digitally enabled services that Sidewalk Labs proposes for Quayside and the Waterfront Toronto priority outcomes that they support, see section 1.3.1.

However, the physical environments in cities today are not designed to host digital infrastructure. For example, it is expensive to install, operate, maintain, and upgrade sensors to measure traffic flow or energy use. Connectivity throughout cities is not yet ubiquitous, nor ready to support the use of tens of millions of simultaneous devices, in line with global networking trends projecting massive growth in use.[17]

Together, these digital infrastructure proposals enable reducing the cost and disruption associated with installing and managing digital infrastructure, increasing capacity while increasing flexibility and upgradeability. These proposals will help manage costs of maintaining digital infrastructure over time, as well as ensure that systems can be adapted to changing conditions or modified to achieve desired outcomes.

These digital infrastructure proposals are:

- Koala: a standardized mount for connectivity and power for devices in the public realm;
- Software-Defined Networking: a more secure, flexible way for people and devices to communicate;
- Super-PON: an emerging standard that improves how optical fibre is used to make it faster, longer range, and easier to upgrade over time;
- Distributed Verifiable Credentials: an emerging set of technology innovations that enables the delivery of services in privacy preserving ways that enhance people's control of their data.

This section provides additional detail on each of the digital infrastructure proposals included in the MIDP, as requested by Waterfront Toronto and the Digital Strategy Advisory Panel.

While each of these technologies would be mostly invisible to residents and visitors in the neighbourhood, they support and enable the more visible innovations that the MIDP proposes to achieve Waterfront Toronto's priority outcomes. It is important to note that each of these infrastructures would be deployed and managed in different ways, consistent with existing urban infrastructure. For example, Waterfront Toronto already has an innovative connectivity partner, Beanfield Metroconnect, that has expressed interest in possibly using a technology like Super Passive Optical Network (Super-PON) to advance their service offering. Distributed verifiable

[17] Cisco, "Cisco Visual Networking Index: Forecast and Trends, 2017-2022 White Paper," February 27, 2019.

credentials could manifest in multiple ways, with either the public sector or private sector taking the lead. In each of these sections, the operational expectations for each infrastructure is addressed.

These proposals also form the backbone of the physical and digital infrastructure that Sidewalk Labs believes is necessary to enable the "testbed" characteristic of the neighbourhood requested in Waterfront Toronto's Request for Proposals, by increasing the ability for digitally enabled services to be tested or deployed securely and with a high level of control.

1.4.2 Koala: standardizing access to power, connectivity, and mounts to reduce costs and improve adaptability

As cities around the world increasingly integrate digital technology into the physical environment, enabling flexibility in how devices are deployed will be key to ensuring that systems can be adapted, redistributed, and upgraded as both technology and city needs evolve.

Koala is a proposal for standardizing the way that devices are installed, maintained, and upgraded in the public realm in a way that reduces costs and operational complexity. Koala mounts would be designed to work with any devices that meet its published standards, just like a USB port. As part of a set of digital infrastructure proposals for Quayside, it supports Waterfront Toronto's Urban Innovation priority outcome for Quayside.

Koala supports aspects of Waterfront Toronto's *Digital Principle #2: Digital solutions will be open, ethical and resilient* by making it possible for infrastructure managers to easily deploy and use a wide range of devices in the public realm. It also supports *Digital Principle #4: Strong privacy protections will be in place at all times* by enabling greater visibility and control over data collection efforts and security breaches, by allowing infrastructure managers to permit power and connectivity to devices.

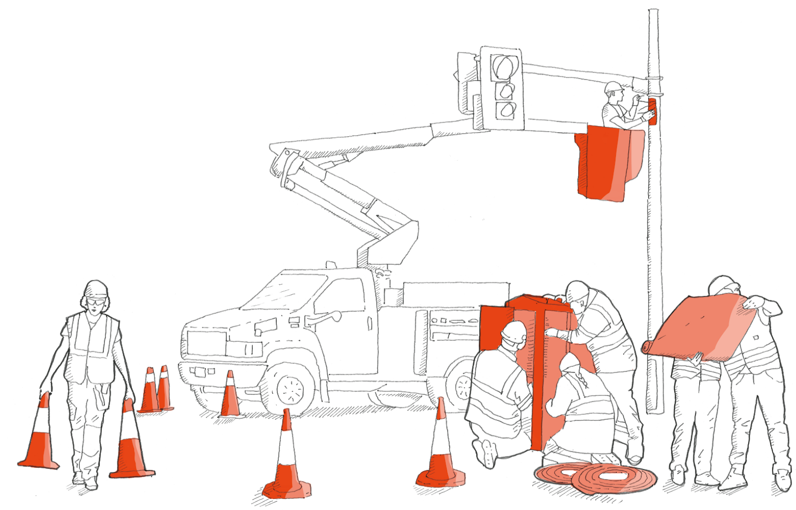
1.4.2.1 What is Koala and why is it innovative?

Koala is a universal outdoor mount that provides power and network connectivity to devices without the need to run new electric wires or close down a street for hours. By providing a standard mount with power and connectivity networking access points or sensors with built-in de-identification, can be added without a bucket truck, additional wiring, trenching, or disrupting mobility.

According to public records, Toronto has at least 11,000 devices mounted to public infrastructure today[18]. Installing these devices often requires significant disruption to street life, creates risks to workers in bucket trucks, and costs thousands of dollars, because light poles and other street fixtures were never designed to host digital hardware.

Currently, adding a single car-counting device to an intersection requires the city to shut down a lane of traffic for hours or even days. A bucket truck with several staff must be sent to the intersection, where they then need to use special clamps to devise a mounting solution to adapt to the particular conditions of a traffic pole while maintaining safety standards. To provide power and connectivity, an electrician needs to shut down the supply to the entire pole and possibly run a network wire, a process that might involve digging a trench to the nearest connection point and repaving afterward. Much of this labour-intensive process is then repeated for repairs or upgrades.

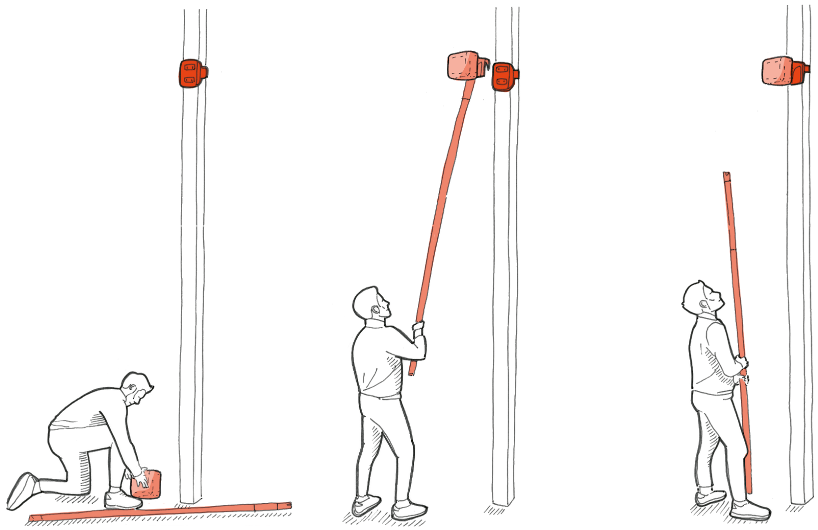
Figure: Traditional Infrastructure Installation



Today, without standardized digital infrastructure, even a basic traffic counter requires hours of work to mount, connect, and test.

[18] Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report. Information and Privacy Commissioner of Ontario, Privacy Investigation Report MC 07-68, March 3 2008; City of Toronto, Red Light Camera; WirelessToronto, Hotspot Map and List. Brochure, December 2007. See also, "How many cameras are watching you? Toronto professor concerned about privacy," CTV News Toronto, February 26, 2015.

Figure: Installation with the Koala System



Koala mounts would make it easy and quick to install, repair, or upgrade sensors for a variety of purposes, from bicycle counting to air-quality monitoring to interactive public art installations.

Koala is digital infrastructure designed to simplify this operational process, by outfitting street furniture like poles with powered, connected mounting points for devices. Once the host connector is installed — a process similar to installation of any powered or networked device today — client devices can be mounted or swapped out within minutes by human operators, without necessitating large equipment or street closures, using a common ladder, or even a reacher grabber. The device has a locking mechanism that locks it down into place.

Sidewalk Labs estimates its mounts would reduce the time needed to mount a device in the public realm by roughly 92 percent — down from 30 hours today to two hours. See section 1.4.2.3 for details.

The Koala mount provides power and connectivity to the wider internet. There are different options for providing connectivity — for example, the network connection could simply be through a local Internet Service Provider (ISP) or it could be provided through a cellular network. Koala is also designed to deliver more than 100 watts of wired power.

In locations like Quayside, where Sidewalk Labs has proposed high-quality, reliable wireless connectivity, most devices might not need hard-wired data connections, but for higher bandwidth tasks or potentially critical items, a wired connection is often preferred. Koala can securely send data (as permitted by privacy regulations and any other applicable data governance rules) back to the cloud or a central server as determined by the device manufacturer.

Koala also provides physical device authentication and data encryption. Security features would allow for infrastructure managers to permit who can turn on devices in the public realm by allowing or denying power and connectivity.

1.4.2.2 Why is a universal mount beneficial?

As digital infrastructure, Koala provides many benefits for cities, public infrastructure managers and building managers, as detailed below, subject to the data governance rules overseeing the permitting and approvals for installation of client devices. Koala also has the potential to support and enable a variety of other sectors — including businesses, industry, media, and academia — to innovate.

Increases flexibility for deploying digital devices
The Koala mount would create a standard connection point that can drive down the costs of installing and maintaining digital hardware, just as USB ports have made it easier for us all to connect devices to computers.

Because the process of deploying digital hardware is onerous, public infrastructure managers and building managers tend to invest in high-priced, ultra-reliable devices that are expensive to repair and upgrade. For example, the average cost per intersection for Adaptive Signal Control is tens of thousands of dollars.[19] [20] These devices are costly because they are expected to last years without needing replacement. That expense means cities can become tethered to outdated hardware and are less able to adopt new, potentially better technology. This leads to slow adoption cycles for new technology and vendor lock-in.

Consumers often buy devices like security cameras, phones, and laptops, then replace them when newer, better, cheaper versions become available — or when their current device breaks. If it was as easy for public infrastructure managers and building managers to deploy, maintain, and upgrade devices in an inexpensive way, they could buy much less expensive technology, replace the small fraction of devices that fail, and provide some redundancy of devices to improve reliability around things like Wi-Fi networks.

Public infrastructure managers and building managers would also be able to allow for technology upgrades on a much more rapid timeline and have more resources to conduct pilots or explorations for new tools and services. In particular, Koala could give public infrastructure managers a more cost-effective option to temporarily deploy a system for testing. Another potential operational benefit is that it would be easier for high-value sensors or systems to be easily redistributed based on need. This could lead to a reduction of lock-in to vendors supplying devices, leading to the opportunity to improve competition and ideally reduce public-sector costs by improving choices.

[19] U.S. Department of Transportation, "The average cost to implement Adaptive Signal Control Technology is $28,725 per intersection," Cost Databases, January 2013.
[20] James Bunch, et al, "Intelligent Transportation Systems Benefits, Costs, Deployment, and Lessons Learned Desk Reference: 2011 Update," National Transportation Library, September 9, 2011.

More convenient and durable than existing options

Why not just use Cat6e and existing power ports? There are a few reasons. Firstly, even if lampposts were outfitted with a regular Ethernet and power connection, there is still no reliable way to safely mount a device without significant disruption to street life. Secondly, many existing quick-connecting Cat6e cable and power connections are not sealed — these connectors can get water, dust, and other elements that create interference at best, and at worst prevent functioning of devices (and while there are some Cat6e cables that are sealed, a bucket truck is still needed to access and connect devices). Power over Ethernet provides at maximum 70 watts of power, which is not enough for many high-power devices such as street lights and antennas. Finally, while some existing lampposts have three-port power plugs, often these are protected by a lock and key, or they are not protected from the elements while in use. The Koala mount is robust to wind, dust, precipitation, temperature, and other environmental challenges.

There are no direct alternative or comparable technologies. The best comparison would be the combination of existing technologies and standards that provide data and power at the client install location. The table below is a simple comparison of these technologies.

More secure and provides more control

Compared to business as usual, Koala provides infrastructure managers a layer of authentication and control for what can be mounted in the public realm through physical device authentication. Security features would allow for infrastructure managers to permit who can turn on in the public realm by allowing or denying power and connectivity.

Currently, if devices on a lamppost malfunction or misbehave, there is no easy way to turn off an individual device without going back up in a bucket truck to disconnect it.
With Koala, devices that are out of compliance with local data governance requirements or have become security threats — for example, those that have been hijacked by a rogue actor or malware — can be quickly quarantined, deactivated, and removed. Summary stats around device behaviour and usage could be shared via a dashboard with public infrastructure administrators.

Without Koala, infrastructure managers would not have the ability to centrally monitor or control devices that are installed in the public realm, unless the device maker has already made available a control interface or APIs that communicate to a central dashboard for their use.

Benefits to other sectors

This type of flexible, standardized infrastructure would be able to host many types of digital products, and do it much more cheaply than the current approach. This benefits not just public infrastructure managers and building managers, but multiple sectors, as listed below.

- Telecommunication companies are competing to roll out next-generation, best-in-class networks as fast as possible. However, current approaches to mounting make deployments and upgrades slow and costly.

These problems may get worse with the introduction of fifth generation wireless networks (5G), which requires more densely deployed base stations than previous networks. Sidewalk Labs has had discussions with telecommunications companies about Koala and there is interest in exploring the solution to support the testing and roll-out of 5G networks. Koala can help quicken adoption of new standards like 5G and greatly reduce overall cost burdens for the city.

- Power utility companies own and operate countless poles in major cities, but have limited access to monitor and manage their infrastructure, including how devices are being mounted on their poles, light outages, and device/network status.

- Device manufacturers are hobbled in their ability to scale up installation of their devices because it is so expensive for cities to deploy them. Reducing deployment costs and making it easier for cities to upgrade equipment can increase the opportunity for these manufacturers to sell their products and improve them over time.

- The flexibility afforded by Koala could also support temporary needs for power and connectivity in the public realm, such as those needed to support street festivals, art installations, or film and media production. Furthermore, Koala could provide an important catalyst for new applications, such as standardized plug-and-play equipment for on-site film production, including lighting and sound equipment combined with direct uploading of digital productions, which could dramatically enhance productions in the City and remove much of the heavy equipment and trucks associated with current production techniques.

- The simplified installation procedure and ease of use will also make it easier for researchers and students studying the urban environment and cities to install monitoring devices for specific periods of time (once the appropriate permissions have been obtained).

Table: A Comparison of the Functionality of Existing Data and Power Connectors Compared to Koala

Device	Mechanical Mount	Hands-Free Connection	Weather-Proof	Power Capacity	Data Bandwidth	Currently Commercially Available	Device Initial Installation Requirement	Device Upgrade Requirements
Koala	Yes	Yes	Yes	200W	Up to 96Gb, currently 3Gb	No, in development	No Bucket Truck Required [21]	No Bucket Truck Required
Cat 6E PoE++	No	No	No	71.3W	1Gb	Yes	Requires Bucket Truck	Requires Bucket Truck
Cat 6E PoE++ with Sealed Shroud	No	No	Yes	71.3W	1Gb	Yes	Requires Bucket Truck	Requires Bucket Truck
Business as Usual	No	No	Yes	Variable, decided by upstream capacity	Determined by existing infrastructure	Yes	Requires Bucket Truck	Requires Bucket Truck

[21] If Koala is not pre-installed at the mounting location, the initial installation of a device will require a bucket truck to install the Koala mount.

1.4.2.3 Implementation scenarios for Quayside

As with Sidewalk Labs' other digital infrastructure proposals, companies would be free to use other mount offerings (that could create their own connections to the local network and power) or stick with the traditional approach.

Expected costs

Sidewalk Labs is not at a sufficiently advanced stage of design to be able to determine expected costs accurately, but expects total costs to be significantly lower than business as usual — that is, as compared to the cost to install typical devices such as Wi-Fi access points, traffic counters, cellular access points, environmental sensors, and public safety cameras that are mounted to public infrastructure.

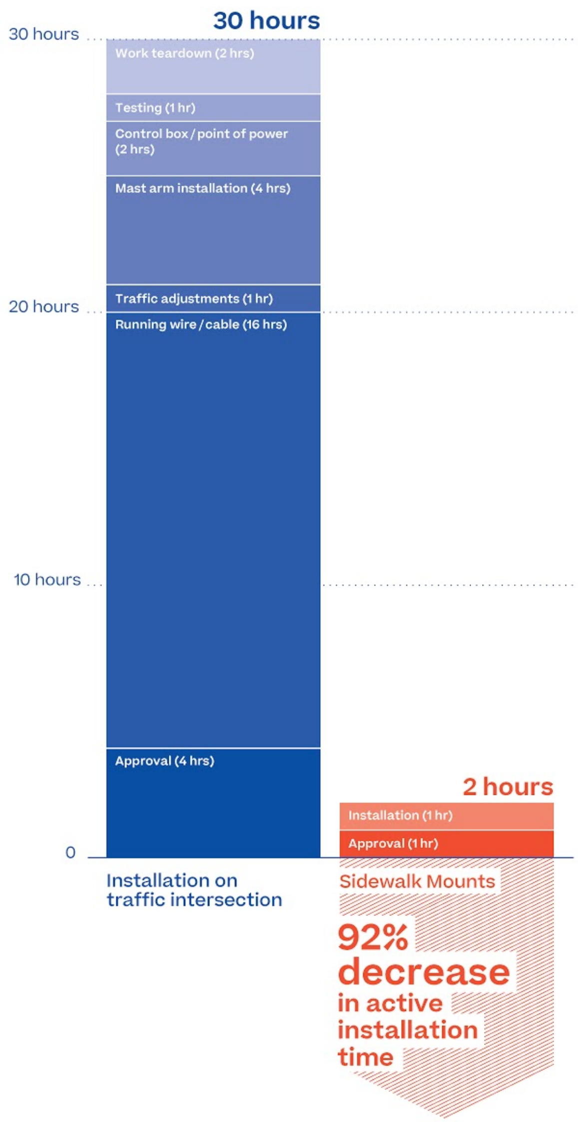
While initial installation costs for Koala are roughly the same as the status quo, Koala offers cost savings in device cost, repair, and replacement.

This cost savings at scale is precisely what would drive market adoption. The infrastructure for fifth generation wireless (5G) requires far more devices in the public realm, and thus there is a major incentive from the 5G hardware providers and telecommunication providers to reduce costs of installation and maintenance. Sidewalk Labs has engaged in initial discussions with providers who have acknowledged this benefit and are interested in Koala for this reason. In this way, it is the roll-out of 5G globally that would be the vehicle through which the standardization offered by Koala would take place.

At the time of street construction, capital costs are expected to be on par with installing devices in the traditional way, with the cost of modifications to poles and other street furniture that incorporate Koala offset by the savings from avoidance of dedicated wiring and custom mounting brackets.

With respect to future installations, Sidewalk Labs expects significant capital cost savings derived from the fact that devices can be installed in an hour, plus another hour for approvals — down from 30 hours today, with associated costs to close down a street for hours and install new wires for power and connectivity within the pole, and possibly in a new excavated trench to the nearest point-of-service connection within the street right-of-way. See the figure on the following page for details.

Figure: Device Installation Time Savings of 92%



The proposed mount from Sidewalk Labs could dramatically reduce the amount of time it takes to install a device — down from 30 hours today to two hours. It could dramatically decrease costs, too. Assuming labour costs of $75 an hour, installing a device on a proposed mount would cost $150, compared with $1,980 for a standard traffic installation.

Sidewalk Labs believes Koala can significantly reduce ongoing operational costs over time in two ways. First, Koala allows for easy access to perform repair or replacement by reducing labour costs and the costs associated with street closure, as previously described. Secondly, because of the ease enabled by Koala, overall costs can be reduced because it can now become possible to use cheaper, consumer-grade devices that need to be replaced/maintained more regularly and rapidly than is possible today (devices today are built to a higher durability standard because of the difficulty in replacement).

Sidewalk Labs would work to quantify these costs and benefits over the next two years to provide more certainty before a final decision on their use is made.

Ownership and operator roles

There are several operating models Koala could adopt, and the deployment would be subject to further negotiations with Waterfront Toronto and the City. These models would impact the financial arrangements and costs for Koala. An important factor will be the willingness for risk and need for control taken on by each party. For example, public infrastructure managers may sometimes just be "renting" space on a Koala rather than operating Koala devices themselves.

Koala mounts could simply connect to the existing Internet Service Provider in Quayside — implementation of Koala devices is not dependent on Sidewalk Labs' other digital infrastructure proposals. However, it may be desirable for Koala devices to be on a separate Software-Defined Network to help quarantine any rogue devices and reduce potential impacts on other digital systems.

Below, a couple of models are provided as examples of how Koala could be deployed, which are similar to how the City has deployed existing products in the public realm, such as cameras from Miovision for traffic management, Axis Communications for road emergency services, and the Toronto Police Service's CCTV for public safety:

<u>Model 1: Owned and operated by the local governing entity</u>
In one model, Sidewalk Labs would provide the Koala hardware and an associated software suite to the public infrastructure manager or building manager in accordance with the data governance rules dictating processes for permitting, approvals, and monitoring of attached client devices.

In this model, the local governing entity would pay a fixed payment per Koala device at cost, where cost is defined as the cost per hardware unit. The software suite is sold at a to-be-negotiated annual fee. In this model, the public infrastructure manager or building manager would be responsible for identifying, managing, and operating the Koala devices, which includes sustaining the costs for their installation and maintenance over time. Ideally, maintenance contracts would be negotiated at the time of purchase as a reasonable percentage of cost per device. All client devices, such as 5G antennas, lights, or sensors, would negotiate directly with the public infrastructure manager or building manager for placement on Koala and any associated fees.

<u>Model 2: Owned and operated by Sidewalk Labs</u>
In an alternate model, Sidewalk Labs would pay for the initial outlay, installation, and ongoing maintenance of Koala hosts.

Client devices that wish to attach to Koala devices would still need to gain approval through the mandated data processes and any other relevant regulatory authorities. In addition, it is likely that the local infrastructure manager would still need to pay for the software suite to help manage and monitor the deployed devices.

In this model, Sidewalk Labs would be responsible for negotiating fees for client devices. In other words, Sidewalk Labs could sublease the space on the Koala to third-party devices with details to be worked out with the City. However, the fees would inherently need to be lower than a business-as-usual installation (described above) to attract clients, marking a benefit in the deployment of the various devices.

If Koala does not succeed as a product, or is not adopted as a standard, the equipment would still be maintained in Quayside, according to the agreement between the entity managing the light poles and street furniture. Alternatively, it could be replaced with current mounting techniques — a simple fixed, physical mount and permanent power and network connections.

The City would have the ability through both contractual arrangements and the formal development application process to determine the conditions upon which Koala will be deployed and any conditions related to replacement should the product not succeed.

1.4.2.4 How Koala works: technical diagrams and specifications

Koala consists of two key components: a **host connector** that is mounted to existing light poles or other infrastructure, and a **client connector** that can adapt to be compatible with various digital products, such as public environmental sensors, antennas for 5G deployments, or transponder receptors that may be part of a mobility management system.

Figure: Koala Mounts — Client Dimensions

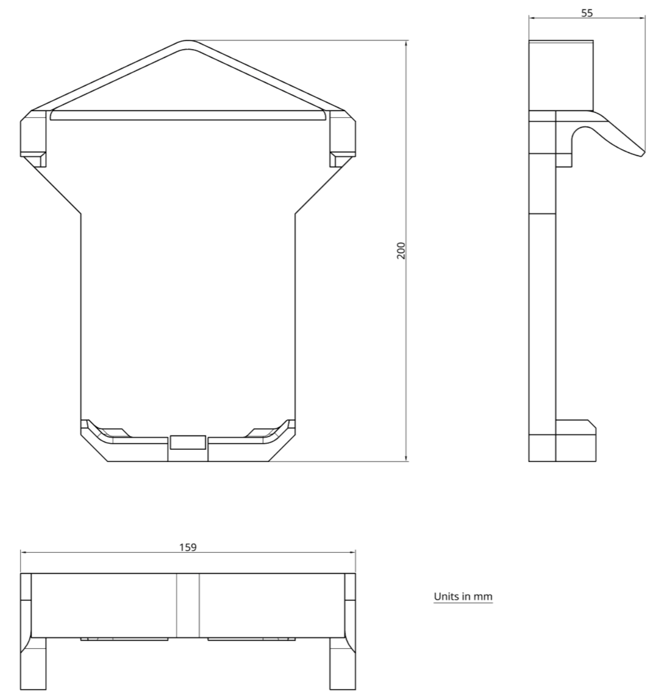


Figure: Koala — Client Isometric View

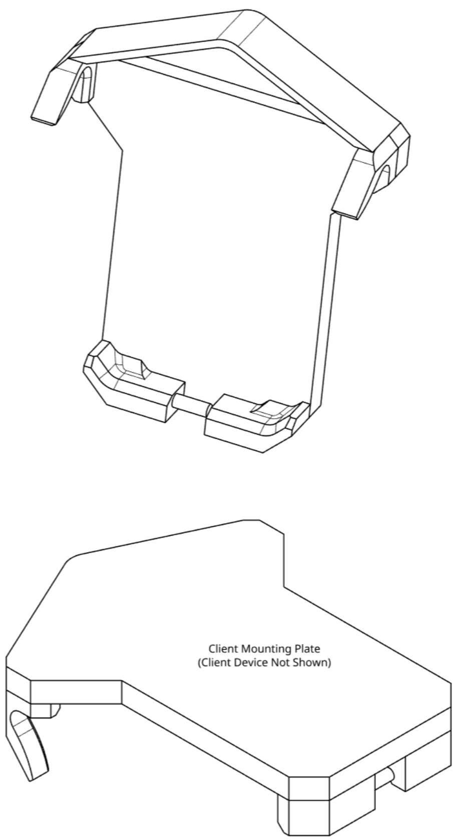
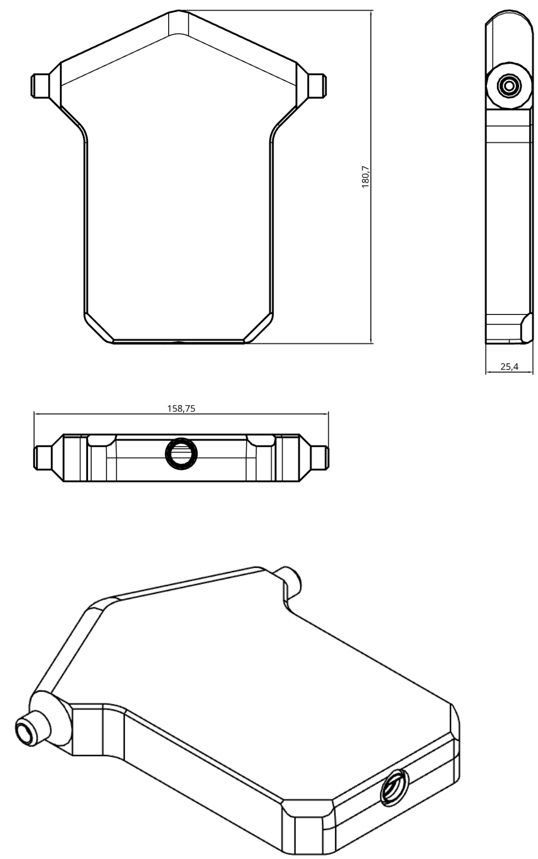


Figure: Koala — Host Dimensions



Though some devices that are installed on the mounts may be passive, such as lighting, other devices could collect or transmit data. This data collection would be subject to applicable Canadian privacy laws and the data governance policy framework for this community. The mounts themselves would be configured to monitor device health and aggregate statistics on power and bandwidth usage. Connected devices would be authenticated by the mounts to ensure they are allowed to use power and connectivity

Technical specifications

Power
Input Voltage: 19–24VDC
Output Voltage Options:
5 VDC, 12VDC , 24 VDC, 48 VDC
Power Consumption:
max. 20W, typ: 2W
Power Transfer: Wireless Induction 100kHz - 150kHz

Dimensions
See below

Weight
6.5 kg

Data Throughput
1.5Gbps with upgrade option to 6Gbps

Operating Temperature
-30°C to +70°C

Storage Temperature
-40°C to +85°C

Housing
IP67 per IEC 60529

Connectors/Interfaces
Host: 1x 10 Gbit Ethernet + screw terminal power
Client: 1 x 10 Gbit PoE

Vibration & Shock
NEMA TS-2 5-30 Hz; 0.5 g double-amplitude
IEC 60068-2-27: 5-100Hz; 0.5g rms

Host Mounting Options
Pole mounting using metal banding
Wall mounting using provided bracket

Maximum Client Weight
12 kg

Regulatory
FCC part 15 subpart C

Figure: Koala Mounts — Locking Mechanism Illustration 1 — Locking Sequence

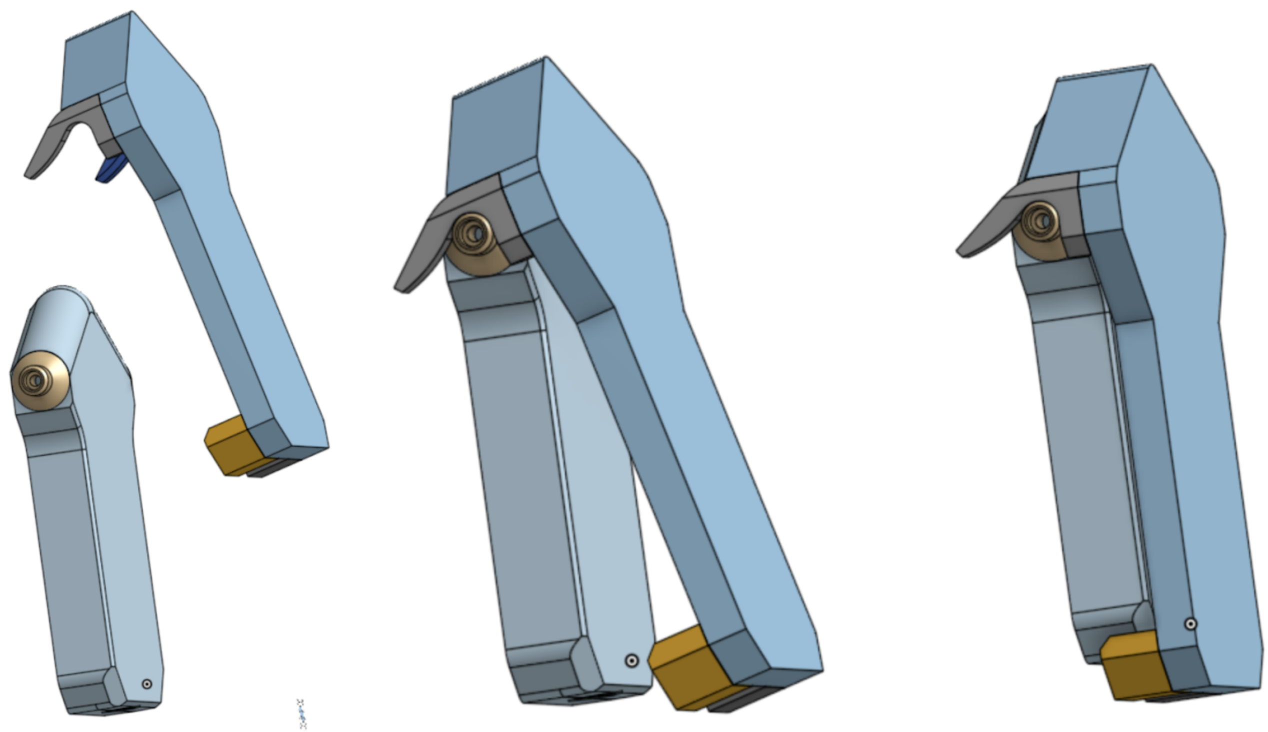


Figure: Koala Mounts — Locking Mechanism Illustration 2 — An Internal View of the Host Side Mount

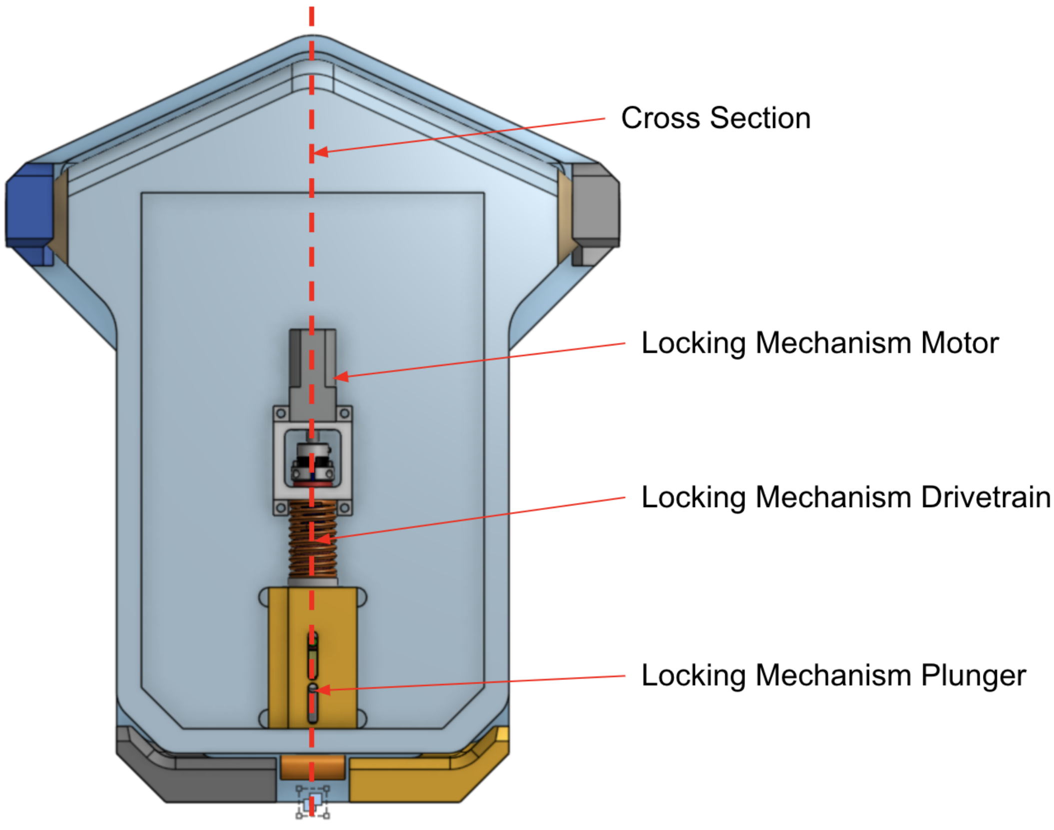
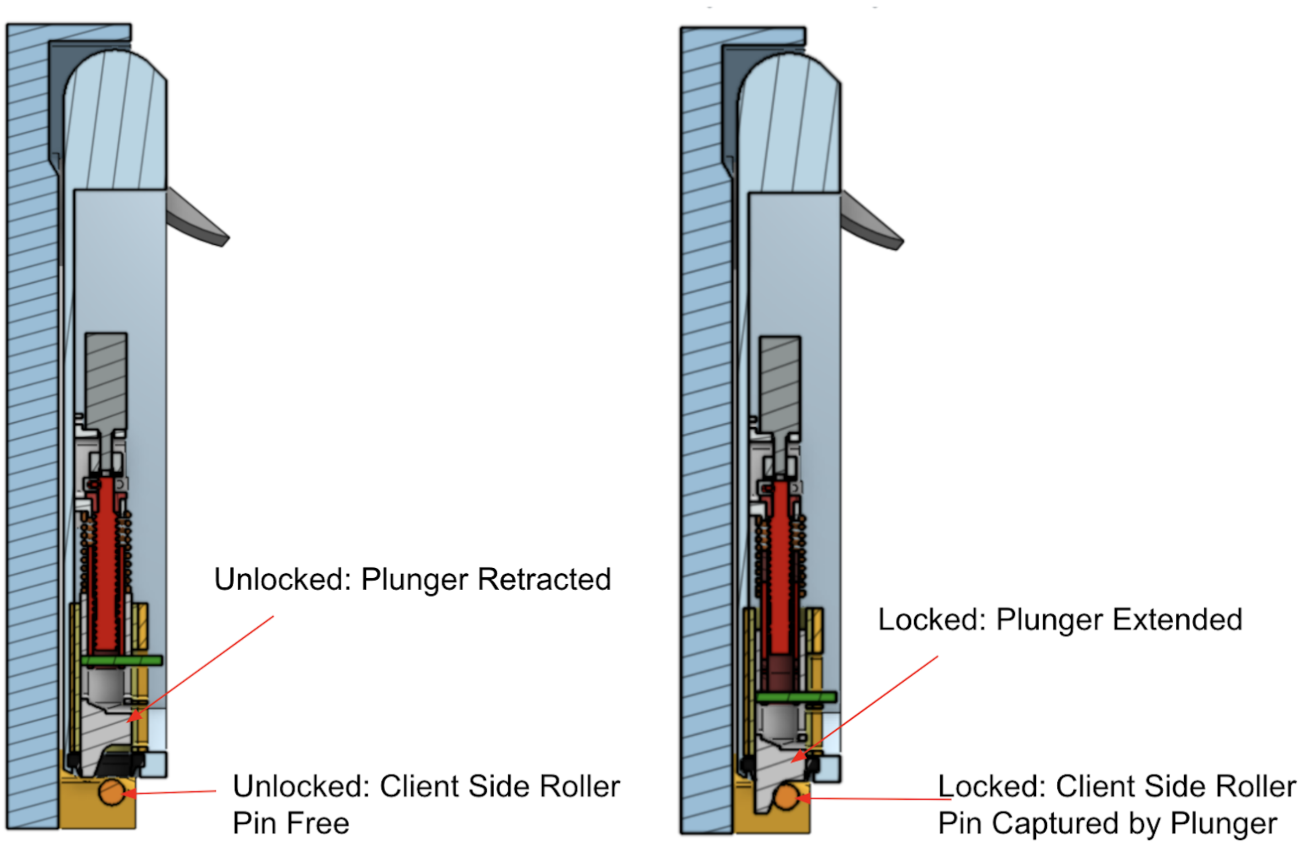


Figure: Koala Mounts — Locking Mechanism Illustration 3 — The Locking Sequence of the Koala Connector



Risk mitigation proposals

Cyber and physical security

Koala devices would face a range of threats. They would be deployed outdoors and must remain dormant and functional over long periods of time. Snow, cold, power outages, and other passive environmental conditions could pose a constant danger to the device.

Koala devices may be physically or digitally accessible to attackers with a range of motivations/targeted assets, including:

- **Vandalism:** Attacker may want to cause reputational damage by damaging or destroying sensors, the Koala itself, or upstream power or data connections.
- **Local service disruption:** An attacker may perform attacks that disable a Koala and attached sensors to disrupt associated services. For example, an attacker may tamper with the power supply on a Koala to disable security cameras attached to the device.
- **Network service disruption:** Attacks against Koala devices may aim at disrupting or degrading the performance of a sensor network as a whole. For example, an attacker may want to disrupt air-quality sensor data collection to hide pollution by tampering with sensors or adding rogue sensors to the device, or launch a Distributed Denial of Service (DDoS attack) against the Dedicated Short Range Communication network to avoid toll collection.
- **Theft of hardware:** Attacker may want to steal expensive hardware components for use or resale.
- **Theft of service:** Attackers may attempt to steal power and data services from the Koala itself, or may target services like toll collection being facilitated by the Koala. Theft of service may be facilitated by direct tampering with the Koala and attached sensors, or through the use of rogue sensors that are attached to the Koala.
- **Unauthorized access:** Koalas would be situated on a physical network shared between Koala devices and containing other internal resources. An attacker may attempt to gain access to this network to access those internal network resources or attack other devices remotely.

Risk mitigation approach

Based on these security threats, Sidewalk Labs has developed a number of design principles for Koala to protect against these concerns:

Vandalism/theft of hardware:

- Completely preventing theft may be impossible — in the extreme, an attacker can cut down and steal the entire light pole. To reduce the likelihood of theft, physical mounts should be robust, and Koalas should be placed above ground level to prevent casual access.
- Power and data should be shielded to prevent both deliberate sabotage and damage due to elements.
- Koalas should be designed to prevent casual tampering and slow down an attacker that attempts to open the

device. This may include the use of security screws and other measures that make tampering more difficult. Koalas should be placed to minimize the host access risk where possible.

- It would be rare for technicians to need access to Koala internals. Attackers can be slowed down by requiring many screws to be removed to service a device, and basic tamper resistance can be added by using tamper-resistant screws.

Local service disruption:

- Exposing ports (USB, UART) for management introduces a number of potential vulnerabilities. Excessive voltage (USB Killer) may be used to damage or destroy the device, and glitching and power analysis attacks may be used to bypass security controls or recover sensitive data like cryptographic keys from the device. If these ports need to be physically accessible outside of the device, they should be protected electronically with overcurrent devices (polymeric positive temperature coefficient devices, a kind of resettable fuse) or over voltage devices (transient-voltage-suppression diodes).

Network service disruption:

- Client devices must authenticate with the Koala so that rogue devices never have the opportunity to transmit any data upstream.
- Tamper detection sensing and anomaly detection will detect any effort to tamper with a client device and would initiate a corrective measure.
- Upstream connections will be embedded into furniture and extremely difficult to access without triggering tamper detection.

Unauthorized access:

- Management functionality would require credentials/only be accessible to authorized users.
- Remote management of Koalas should happen on a dedicated (virtual) network segment.
- Koalas should not be able to communicate between themselves, nor should they be addressable from the public internet.
- Remote management is a common site of critical vulnerabilities, so access should be limited to authorized users.
- Principle of least privilege: Access to the internal network should be enforced at the network's core, and sensors should only be given the minimum amount of access needed to deliver data relevant to the service.
- Network service disruption: Koalas and attached sensors may need to operate with intermittent upstream connectivity, making real-time monitoring and alerting difficult. Nonetheless, upstream systems can infer sensor and Koala health via the availability of data. Metrics around this data should be used to drive monitoring and alerting.

- Communication between the Koala and upstream devices should be authenticated to minimize the risk of MITM attacks.

Theft of service:

- There should be mutual mistrust between sensors and the Koala: the security of applications deployed via sensors ultimately depends on the authenticity and integrity of data as measured by the sensor. Thus, **data should be authenticated by sensors themselves** — not by the Koala.
- The Koala should report on, and possibly authenticate, any attached sensors. This should be a monitored event.
- Koala should not supply full power until a sensor is authenticated.
- The data connection provided to sensors should not be accessible unless in close proximity to the device. The technology chosen should not allow access otherwise.

1.4.2.5 Koala development roadmap: R&D and testing plans

Product development phases

Sidewalk Labs currently plans to have a fully tested system ready for wide release by the end of 2022. At a high level, the development roadmap anticipates completing Proofs of Concept (PoC) for both the connection hardware as well as the management system by the end of 2020 (System 1). By the end of 2021, Sidewalk Labs plans to have incorporated installation systems and iterated on both the connection hardware and the management System (System 2). Sidewalk Labs will then conduct additional tests and continue to refine the integrated systems until ready for release by the end of 2022.

- **System 1 — Anticipated completion 2020**
  - Connection hardware Proof of Concept
    - → Client Power Control
    - → Basic Client Authentication (no public key infrastructure)
    - → Basic Handshaking
  - Management system Proof of Concept
    - → Deployed Client Tracking and Inventory
    - → Basic Management User Interface
      - Can turn on and off individual client's power and data
      - Basic housekeeping telemetry from all units
      - Reports back universally unique identifier (UUID) of each client

- **System 2 — Anticipated completion 2021**
  - Connection Hardware/Firmware
    - → Robust and tested mechanical devices
    - → Optimized control and communications hardware
    - → Hardware secure elements embedded in electronics

        - → Foreign object detection and power optimization
    - ○ Client Installation Systems
        - → Pole and unmanned aerial vehicle (manually controlled) install systems PoC
    - ○ Management System
        - → PKI Authorization and Authentication V1
        - → Tracking for all devices
    - ○ Host Installation System
        - → PoC host installation system in testing

- **System 3 - End of 2022**
    - ○ Fully tested system ready for wide release

The first few designs of each piece of the Koala technology will be internal only, because they will be non-production prototypes. They will only be created in order to refine the design and test with partners. They will not be used for production deployments, and therefore will not make sense to standardize. Only once there is a design that is promising for real deployments, and the consortium of interested companies has been formed will it make sense to start the process of creating a formal standard.

Testing
Sidewalk Labs is still in the prototype stage and has not done ruggedized field testing, which will begin before the end of 2019. Sidewalk Labs is targeting a small-scale deployment in early 2020 (outside of Toronto) to begin testing these devices.

The following is a list of proposed tests and certifications that will be completed prior to large-scale deployment. This list is not exhaustive and is subject to change but shows the current test plan for the device.

Table: List of Proposed Tests and Certifications that are Planned for Koala Prior to Large-Scale Deployment

Testing standards for Koala	
Electromagnetic Emissions	
EMC Emissions Unintentional	FCC Part 15 Subpart B / IC ICES–003 Unintentional Radiator
EMC Emissions Intentional	FCC Part 15 Subpart C / IC RSS-Gen, RSS-210 Intentional Radiator
Electromagnetic Susceptibility	
Electrostatic Discharge Immunity	IEC 61000-4-2
Electromagnetic Field Immunity	IEC 61000-4-3
Electrical Fast Transient Immunity	IEC 61000-4-4
Electrical Surge Immunity	IEC 61000-4-5
Conducted Disturbances Immunity	IEC 61000-4-6
Environmental	
Thermal Low	MIL-STD-810 Method 502 to -30C
Thermal High	MIL-STD-810 Method 501 to 70C
Humidity	MIL-STD-810 Method 507 to 95%
Thermal Cycling	IEC 62892 or IEC 61196-1-209 or EIA/ECA-364-110
Thermal Shock	MIL-STD-810 Method 503 or EIA-364-32F
Ice/Freezing Rain	MIL-STD-810 Method 521 or EIA-364-51A
Vibration	NEMA TS-2 5-30 Hz; 0.5 g double-amplitude ASTM D4169 Assurance Level 1 Distribution Cycle 3, Acceptance Criteria 1 & 2

Shock	IEC 60068-2-27
Ingress Protection	IEC 60529 and EIA-364-50B
UV	MIL-STD-810 Method 503
Drop	IEC 60068-2-5
Safety	
UL 1977 Standard for Component Connectors for Use in Data, Signal, Control and Power Applications	UL 1977 and CSA C22.2 No. 182.3-16
UL 486D Sealed Wire Connector Systems	UL 486D and CSA C22.2 No. 198.2

Challenges for standards adoption
Koala would make it much easier and less expensive to deploy and maintain technology in the service of improving a neighbourhood. But new hardware standards require significant geographic distribution to gain the wide adoption needed for device manufacturers to incorporate the standard into their own designs; for example, a Wi-Fi antenna producer would not change its design for a small handful of cases.

Sidewalk Labs expects that Koala's offering of cost savings in device cost, repair, and replacement at scale to drive market adoption. For example, the infrastructure for 5G requires far more devices in the public realm, and thus there is a major incentive from the 5G hardware providers and telecommunication providers to reduce costs of installation and maintenance. Sidewalk Labs has engaged in preliminary conversations with providers, who have acknowledged this benefit and are interested in Koala for this reason. In this way, it is the roll-out of 5G globally that would be the vehicle through which the standardization offered by Koala would take place.

Implementation and partnerships
Over the next year, Sidewalk Labs will be looking for partners to test and co-design Koala with:

- Locations to test Koala in, with a range of weather, and in different urban design contexts.
- Manufacturers of light poles, traffic light poles, and street furniture to test the integration of the mount, power, and networking.
- Manufacturers of devices such as Wi-Fi access points, cellular access points, lights, and sensors.

Initially, Sidewalk Labs will have to partner with device manufacturers interested in exploring this idea in order to have compatible devices to use. In addition, Sidewalk Labs will build adaptors for existing devices. For example, for devices that use Power over Ethernet (PoE) and simple screws for mounting, Sidewalk Labs will create a PoE to Koala adaptor made of a material that can be screwed into. This can bootstrap the ecosystem in order to prove out the technology and the economics.

1.4.3 Neighbourhood-scale Software-Defined Networks: enabling a more secure and resilient network infrastructure

Sidewalk Labs' proposal for digital inclusion in urban innovation builds on Waterfront Toronto's track record of public Wi-Fi and affordable broadband towards a vision of ubiquitous connectivity that is highly secure and easier to use while increasing performance and reducing hardware needs. In high-density neighbourhoods, cluttered Wi-Fi bands reduce internet performance. The proliferation of end-user-managed home routers pose both security risks and operational burdens for Internet Service Providers (ISPs), and internet firewalls are typically too complicated for most to configure leaving them open to security vulnerabilities.

The Software-Defined Network (SDN) is a new approach to routing on the internet that enables better management and control over a network, as well as more security. As part of a set of digital infrastructure proposals for Quayside, SDNs support Waterfront Toronto's Urban Innovation priority outcome for Quayside, with a particular focus on inclusive communities.

SDNs support aspects of *Digital Principle #1: Everyone will have access to, and benefit equally from, digital solutions* by making it easier for residents and consumers to access secure, high-performance internet connections throughout the development and *Digital Principle #4: Strong privacy protections will be in place at all times* by providing greater control over connected devices, and by enabling greater visibility of and control over any potential security breaches.

1.4.3.1 What is a Software-Defined Network and why is it innovative?

A seamless and secure neighbourhood-wide network
When the internet was invented in the 1970s, every device could connect to every other device. Routers performed the task of getting packets of information from the transmitting device to the receiving one, usually by taking multiple hops.[22] Over time, the internet became less connected: for security purposes, some sub-networks (subnets) walled themselves off by having the router that connected them to the rest of the internet reject most incoming information packets. This was the origin of the internet "firewall" — a now-common feature of an internet router.

For this reason, it is very difficult for people to connect to a home device when they are not at home. Instead, they must engage with a home device (such as a smart thermostat or home-security camera) via a third-party website or app that this device contacts from time to time. For example, if a family wants to check on their dog while they are out, they would normally have to make sure their video camera was cloud-connected. A better approach would enable the family to access this video using data from their home internet

[22] Wikipedia, "Routing."

network, just as if they were at home, without data having to be transferred or stored at any cloud provider.

SDNs' new approach to routing on the internet enables better management and control over a network, and allows people to have their own private networks with all of their devices on it — no matter where the person or the devices are located within Quayside.

As its name suggests, a Software-Defined Network uses software to "define" the way that information travels through the network's hardware (its physical communications links and the routers that connect them). In such a system, users would not need to configure their own routers independently and have those routers reject all incoming communications using a firewall. Instead, the software-defined system would automatically configure the routers to create private networks that would remain available and secure across an entire neighbourhood — providing both greater convenience and heightened security.[23]

Implementing an SDN would mean that a single wireless service set identifier (SSID) would be accessible everywhere within the district. When a user connects and authenticates to the network, their device would join their private Virtual LAN (VLAN).

[23] Jennia Hizver, "The security benefits of software defined networking (SDN)," *AT&T Business*.

1.4.3.2 Why is a Software-Defined Network beneficial?

Software-Defined Networks are a digital infrastructure that can provide an increased level of security that benefits public agencies and other authorities who deploy digital devices, by enabling devices to communicate securely with each other without having to send data through the cloud for every transaction. SDNs can also enable people and businesses to have continuous access to their own secure Wi-Fi connection everywhere they go, without worrying about joining an insecure network.

Benefits for increased security
One key advantage of SDNs is increased security for Internet of Things (IoT) devices, whether they are public or commercial systems or personal devices. Ensuring the security of IoT devices is paramount, but challenging through a traditional network. Currently, these devices are only reachable while on the same local network, or through a third-party API that connects them to the cloud.

For example, in a resident's apartment, all the devices should behave as they do today: as if they are on a single, private local-area network (LAN). For building infrastructure equipment, like Building Management Systems (BMS) and their attached devices, those devices should be allowed to communicate with each other and with the relevant cloud-based infrastructure management system, but not third-party vendors or other, non-authorized equipment on the network.

Because the software network could be configured to monitor the aggregate stats of data each device is supposed to be transmitting, it would be able to detect if any of them have been compromised. For example, if a thermostat that normally sends a few bytes every minute starts streaming megabytes per second, the software-defined network could quickly disconnect the device from the network — putting it in a kind of quarantine.

This ability could help avoid "distributed denial of service" attacks and other exploits aimed at vulnerabilities in connected devices. Additionally, devices of the same type could be grouped into logical Virtual Local-Area Networks (VLANs), isolating them from other network devices. City and personal IoT devices would also benefit from better security and more tightly integrated management.

Benefits for consumers and organizations

<u>Ease of access:</u> These private networks would be available anywhere in the neighbourhood, including in parks and public spaces, using the ubiquitous Wi-Fi network. A neighbourhood software-defined network would enable people to connect to all of the devices on their personal network, regardless of whether they are at home, in the office, in the park, in a light rail vehicle — anywhere. And nobody else (unless authorized) would have access to those devices. These enhanced security benefits could extend to public sector agencies as well — and provide an additional level of control not currently available to manage and secure digital devices.

<u>Cost reduction</u>: Software-Defined Networks have the benefit of reducing costs to end consumers, and hopefully also to the Internet Service Provider (ISP) by requiring less hardware overall which reduces the operational and maintenance overhead for ISPs. A wireless SDN would obviate the need for ISPs to support people and organizations in the set up of their own routers and maintaining their security updates for the equipment.

<u>No more home routers:</u> Software-Defined Networks allow the management of the network to happen centrally, which means each individual home would not need its own router. Home routers that use default passwords and misconfigured firewalls can be vulnerable to hackers. Central management also relieves consumers of the burden of debugging, maintaining, and upgrading wireless equipment in their home. And that is more than just unplugging the router once in a while to fix a lost connection. Many people, even those who are technically-savvy, are not aware that router firmware has to be regularly updated as vulnerabilities are discovered — an often onerous process that involves tracking down an update on a manufacturer's website.

<u>Better connections:</u> As it stands, households in urban areas each have their own wireless access point and SSID. In high-density areas, these access points crowd the Wi-Fi

signal bands and lead to decreased performance.[24] The vision is that all access points would broadcast only the Quayside SSID, and as such would not have to compete for bandwidth. And devices could organically switch to new access points as users travel around the district.

Benefits for ISPs
Deploying fibre connections inside buildings and provisioning residential or business internet connections is expensive and laborious, as is providing support to consumers who struggle to manage their own Wi-Fi equipment. The proposed network relieves ISPs of these burdens, and reduces the risks that their network may be misused.

1.4.3.3 Implementation scenarios for Quayside

Currently, this technology has mostly been deployed for wired networks in research settings, and for industrial applications such as data centres. Additional research and development work will be needed to deploy SDNs at Quayside. Sidewalk Labs would collaborate with the research and development group for Waterfront Toronto's broadband internet provider, Beanfield Metroconnect, to advance the use of this technology. Sidewalk Labs proposes an open source standard that allows for mixing of equipment from different vendors, fostering an open marketplace that drives down equipment costs.

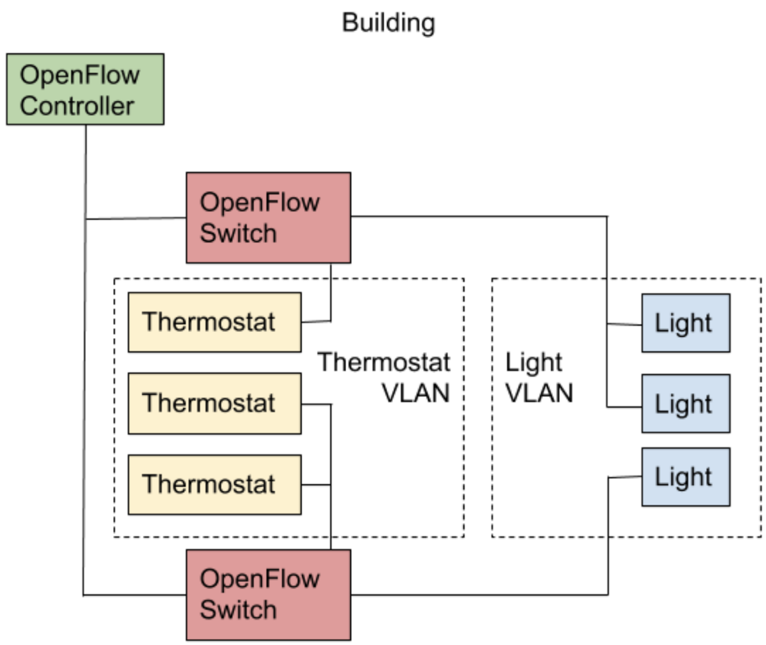
[24] Michael Horowitz, "Wi-Fi in an apartment building," *Defensive Computing*, Computer World, June 29, 2012.

As with all digital infrastructure proposed by Sidewalk Labs, residents and businesses would not be required to use this network. There are significant economies of implementing SDNs at larger scales, as SDNs allow for less networking equipment, allow for more choices in which vendor equipment is sourced from, and more rapid changes to the network when business needs change. Furthermore, in the same way that a telephone system becomes more useful when there are more subscribers — the so-called "network effect" — there are benefits that increase superlinearly with scale. For example, at larger geographies more people and organizations are covered by the SDN, and therefore will be able to take advantage of seamless access across those places.

Considerations for a Quayside wired SDN
In order to enable the use of SDNs across Quayside wired networks, the only hardware requirement is to use switches that support OpenFlow, which are available now and not significantly more expensive than other high-performance network switches. Given the large scale of the project, controllers would need to be distributed across the district to control different segments of the network.

The below diagram demonstrates this concept for a single building. An OpenFlow controller is responsible for managing all OpenFlow switches within the building. Leveraging OpenFlow, independent of what physical switch a sensor is connected to, it can be configured to be part of a specific private VLAN via the controller configuration. This allows devices of the same type, such as lights and thermostats, to be isolated to different segments of the network.

Figure: Building Network Utilizing OpenFlow



Alternative scenarios to wired SDNs include:

- Assuming there is a ubiquitous network throughout Quayside, network commissioning processes could be automated using building information modelling (BIM) to create relevant SSIDs on the wireless access points (WAPs) in physical proximity to units and systems that then associates them with their own VLAN. This would create a huge improvement over today's business as usual as people and devices would be on a specific network and the risks of people on the wrong network or a malicious network are reduced.
- Consider using third-party, commercially available network products like Dispel that use a combination of software (security certificates) and hardware (Software-Defined Wide-Area Network based routers) on top of OpenVPN to tunnel traffic in interesting ways to create secure private networks.

Alternative scenarios for wireless SDNs:

- Wireless SDNs require Openflow compatible WAPs, which are now becoming available on the market. Should they be unavailable, VPN products could be used to provide users with a manual system similar to that which SDNs automate.

1.4.3.4 How SDNs work: technical overview and current state of the technology

Software-Defined Networking defines a methodology for designing, building, and managing networks that separates the network's control and data planes.[25] The control plane, analogous to the brain of the network, sets the network policy and topology. The data plane that handles the forwarding of packets, analogous to the muscles of the

[25] Kanika, "Difference Between Control Plane & Data Plane," SDN Tutorials.

network, is directly programmable by the software running in the control plane.

The goal of Software-Defined Networking is to dynamically create ad hoc, secure networks that can physically span the entire district in order to monitor and control what classes of devices do to improve security, which is not typical of standard business practices today.

Technical advantages of SDNs

Provisioning/flexibility: When using SDNs, the physical topology becomes less important than the software configuration. Currently, the location of routers and firewalls, usually at each customer location, defines the network topology. With SDNs, new devices can be added to any port along a switch and configured/provisioned via software. Additionally, if things go wrong, a network administrator can easily rollback to a previous working configuration without physically moving any wires.

Security: SDN centralizes the definition of the network policy to the control plane. Similarly, SDN enables you to define a monitoring policy that monitors traffic that conforms to a specific ruleset. Of particular interest in monitoring is Poseidon,[26] which leverages machine learning across network activity to detect anomalies, something that is not possible with the partial knowledge that current internet routers have of device behaviour.

Performance: Google has seen large performance benefits through its use of SDN in data centres.[27] Google Data Centres use SDNs to optimally route traffic to the fastest data centre available to the client. For example, users in California are automatically connected to the West Coast data centres, while users in New York are connected to the East Coast data centre. The network topology can be dynamically rebalanced to more effectively respond to demand.

Security and resiliency benefits of SDNs

Software-Defined Networks enable more secure and resilient network infrastructures compared to business as usual because:

- They create flexible networks that can rapidly be reconfigured or customized for specific needs simply through software. Typical networks would require manually updating individual network components, which is expensive and prone to error, because at large scale there can be hundreds of devices.
- Using SDNs lowers operating expenses and reduces network downtime from errors because it allows for automated configuration and reprogramming, instead of the laborious manual process typically used.

[26] Charles Lewis, "Poseidon: A Machine Learning Approach to Network Device Role and Behavior Identification," SC18 Network Research Exhibition: Demonstration Publishable Submission.

[27] Amin Vahdat, Bikash Koley, "Espresso makes Google cloud faster, more available and cost effective by extending SDN to the public internet," *Google Cloud*, April 4, 2017.

- Sidewalk Labs proposes an open source standard that allows for mixing of equipment from different vendors, fostering an open marketplace that drives down equipment costs.

Current state of the technology
Presently, large-scale SDNs have been deployed mostly in wired networks within corporate data centres and a university, and some challenges remain before wireless SDNs will be commercially feasible. A proof of concept network has been created at Sidewalk Labs, and it is expected that commercial equipment to support SDNs at Quayside scale can continue to mature and reduce in cost. Sidewalk Labs would work with network equipment manufacturers to create products that would be capable of supporting the Quayside network.

Sidewalk Labs proposes a SDN built upon open source technologies, as it allows real-time, dynamic network configurations of devices by any manufacturer that supports OpenFlow.

Key open-source technologies for implementing SDNs include:

- **OpenFlow:** OpenFlow is the most widely used SDN standard. OpenFlow-compatible switches are controllable via the OpenFlow protocol, allowing an OpenFlow controller in the control plane to control OpenFlow-compatible switches without worrying about their specific hardware.

- **Faucet:** An open source OpenFlow controller designed for large scale production networks. Faucet runs on a controller (or set of controllers) connected via the control plane to OpenFlow compatible switches.

- **Open vSwitch:** Open vSwitch (OVS) is a software implementation of an OpenFlow compatible switch. This is useful both for simulating and creating new SDN applications.

Faucet already plays a large role in many large networks around the world. One project of particular interest is the deployment at the University of Waikato in New Zealand.[28] This network is using OpenFlow over 600 network switches and 900 Wi-Fi access points.

For wireless SDN networks, the state of the industry is much less mature and would require custom hardware. Sidewalk Labs plans to work with Wi-Fi router manufacturers to provide the required hardware in time for construction in Quayside.

[28] Brad Cowie, "Using an Open Source SDN Controller to Deploy a Multi-Terabit/s Production Network," The Linux Foundation, July 2018.

Challenges and limitations to deployment

Several challenges and limitations remain for the wider deployment of these open source technologies. Currently, using Faucet and related technologies has the following limitations:

- Ethernet-only networks work as long as the total number of network nodes is less than 2,000. This is due to the requirement that a single Faucet controller be connected to each switch in the network. Currently, the largest Faucet-compatible switch is 48 ports. Counting up the number of switch ports needed to cascade switches and to connect to the Faucet controller leaves approximately 2,000 switch ports available. This limits the number of devices that can be connected to the network and is insufficient to support the provisioning of public WiFi and the connectivity needs of other devices.

- Faucet is a set of Python scripts that have not been optimized for massive deployments. With 2,000 devices, the maximum currently possible, Faucet performance suffers.

- There are few commercially available Wi-Fi Access Points (WAPs) that support Faucet. Allied Telesis has released a series of OpenFlow- and Faucet-compatible switches and WAPs. Most are still building their own WAPs using WAPs with a modified version of OpenWRT that supports OpenFlow. This won't scale to millions of devices, which Sidewalk Labs expects to have, and requires finding a hardware manufacturer. It is expected that future WAPs will support Faucet.

- There is no registration or commissioning system that would automatically associate devices with their SDNs — it would have to be developed. For example, this would be a way for an organization to bring a new device online. Such a system is imagined to work as follows:

    - A user files a request through their resident portal to provision a new wireless device. This process includes specifying the make, model, and possibly the media access control (MAC) address of the device so that a Manufacturer Usage Description specification can be downloaded for security systems. Sidewalk Labs believes further testing and iteration will dramatically improve this process.

    - The user connects their device to the Wi-Fi network and its MAC is captured and localized to their apartment (since it is known which WAP it is connected to). Sidewalk Labs compares this to the request previously made to add a device to the network as a way to know who owns this device.

    - The device is automatically part of the user's private VLAN based on its MAC address.

1.4.3.5 SDN development roadmap

Before deployment in Quayside, Sidewalk Labs would solicit a partnership with a property owner or developer who is interested in co-developing a Software-Defined Network at a building and small-scale public-realm scale. This can demonstrate feasibility for the environment that Quayside would represent, albeit at a smaller scale. In building out this pilot, Sidewalk Labs would rely on existing examples of SDNs deployed in production environments such as Ammon, Idaho, and university campuses like the University of Waikato.

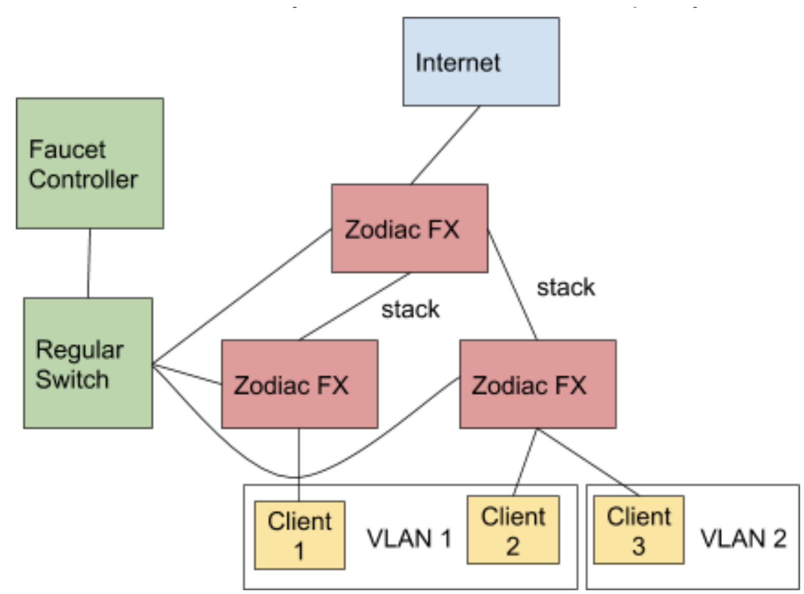
Sidewalk Labs believes that Software-Defined Networks could become a default option built into wide-area-network Wi-Fi routers. Software-Defined Networks have been used for some time in wired network outlays and are starting to gain traction in Wi-Fi corporate networks. AT&T SDN articles and Verizon SDN articles have recently been released in support of advancing the networking approach.

In-office wired SDN experimentation

Sidewalk Labs built a test network in the office using Zodiac FX OpenFlow switches to prove the viability for the firm to build a scalable SDN itself if adoption does not occur before Quayside comes online. Through this test, Sidewalk Labs was able to experiment with configuring an SDN via Faucet and observing the effect of pushing configuration changes.

In the configuration below, three Zodiac FXs were stacked into a single logical switch. Within the Faucet configuration, Client 1 and Client 2's ports were configured to be part of VLAN 1 and Client 3's port was configured as part of VLAN 2. As such, Client 1 and 2 can freely communicate with each other, while Client 3 remains isolated on VLAN 2. These clients could be moved to a different VLAN through pushing a configuration change without moving any physical wires.

Figure: Test SDN Using Zodiak FX Switches



Each time a device sends a packet, the Faucet Controller resolves what should happen based on its configuration and pushes a flow back to the switch. These flows allow the switch to decide how future similar packets should be routed without having to send them back to the controller.

Sidewalk Labs conducted this test because the use case of wirelessly connected devices that need to be rerouted dynamically is a different use case from data centres, which has seen the majority of adoption thus far. Sidewalk Labs learned that using SDNs was feasible for residential, commercial, and public applications using off-the-shelf components.

1.4.4 Super Passive Optical Network (Super-PON) - Installing a more efficient and flexible connectivity backbone

Toronto's waterfront currently incorporates world-leading internet speeds, thanks to the work of Waterfront Toronto with its telecommunications partners, such as Beanfield Metroconnect. Looking forward, Sidewalk Labs' vision of ubiquitous connectivity for Quayside builds on this foundation, proposing abundant, secure, and seamless connectivity both indoors and outdoors for people and infrastructure systems.

The network to support this must be state of the art when deployed, but also built to be future-proof and flexible so it can be upgraded both in terms of speed and adaptability to new technologies.

Sidewalk Labs has had preliminary discussions with Beanfield Metroconnect, which has expressed interest in Super-PON - a novel technology that could be used to build out the ubiquitous network at Quayside.

Super-PON multiplies the capacity of access fibres and extends the passive footprint of fibre access networks for easier construction, better reliability, and lower cost of operation. It offers the ability to build scalable networks that can meet for future smart cities with demanding communication requirements.

As part of a set of digital infrastructure proposals for Quayside, Super-PON supports Waterfront Toronto's Urban Innovation priority outcome for Quayside.

Super-PON supports aspects of *Digital Principle #1: Everyone will have access to, and benefit equally from, digital solutions* by increasing the capacity to provide secure, high performance internet connections throughout the development and *Digital Principle #2: Digital solutions will be open, ethical, and resilient* by advancing an open-source solution that provides a path for future network upgrades and capacity improvements while minimizing costs.

1.4.4.1 What is Super-PON and why is it innovative?

Super-PON reduces the amount of materials (fibre), the amount of space in buildings for equipment (communication closets), and the amount of energy (electricity) needed for large areas. It provides service on par, or better, with that already offered today by typical Internet Service Providers.

Conventional fibre-optic networks are constructed with a stranded fibre-optic cable running from the network provider's central office to the user's site, typically a single building. This type of system can reach 32 or 64 users per fibre strand, with 20 kilometres of transmission reach.[29] In contrast, Super-PON technology is capable of supporting 768 users per strand and extending the reach to 50 kilometres — meaning that a single cable could now provide connectivity to multiple buildings across a neighbourhood or district.[30] [31] Super-PON achieves this improvement by splitting light into many different colours (or wavelengths) over a single strand of fibre-optic cable, with each colour serving as its own signal. In one possible configuration, each light wavelength (such as red, yellow, or blue) would provide connectivity to a specific building.

This technology infrastructure could result in a higher-bandwidth network with a number of additional benefits. The ability to split cables among more users means the network would require less fibre material and physical infrastructure than traditional networks, enabling it to be constructed faster and at lower cost, allowing ISPs to pass cost-saving to consumers. The network would also use less electrical power because its extended reach requires fewer "stops" for a signal (a traditional network could require rooms with electric boosters every 20 kilometres).

This Super-PON specification is now being studied by the IEEE Standards Association, the world's largest technical professional organization, for possible inclusion in its 802.3 international standards for telecommunications.

Super-PON provides the path to a shared fibre plant infrastructure for converged wireline and wireless access networks. It offers massive bandwidths and a massive number of connection endpoints, which would be useful for building scalable networks for supporting connectivity in environments with demanding communication requirements.

---

[29] GPON, "How GPON Works."
[30] Stephen Hardy, "IEEE Study Group tackles Google Fiber Super-PON," *Lightwave*, August 28, 2018.
[31] Claudio DeSanti, et al, "SUPER-PON," Google.

1.4.4.2 Why is a Super-PON network beneficial?

Laying the foundation for 5G networks
Major infrastructure build-out for 5G (fifth generation) wireless networks around the world began in 2019.[32] 5G wireless networks not only bring higher bandwidth to users — potentially exceeding 10Gbps — but also allow higher density of endpoints and very low latency. These are very important for Internet of Things (IoT) operation and deployment, as well as supporting connectivity for sensors and other types of digital hardware that support municipal operations.

As 5G wireless networks will use large numbers of antennas with different frequencies, and base stations of much higher bandwidths and densities, a massive fibre backbone infrastructure is required. In fact, to prepare for the coming of 5G, major carriers started announcing tenders and requests for proposals (RFPs) to source fibre cables in 2017, causing a global shortage of optical fibre cable manufacturing capacity.[33]

The performance of wireless technologies depends on the fibre optic backbone. Although wireless access networks offer the convenience of untethered connectivity, they require directly wired fibre connections which have the advantages of offering virtually unlimited upgrade bandwidth with very low power consumption (the energy to transmit one bit of data in a fibre link is 1/1000 of that required to deliver a bit wirelessly[34]), much more stable performance that is free of interference, with higher reliability and very easy operation.

Super-PON fibre access architecture is designed to multiply the capacity of the types of access fibres that are being installed already today, and has the potential to help meet the soaring demand for fibre resources as operators begin deploying 5G wireless networks. The technology extends the passive footprint of fibre access networks, enabling easier construction, better reliability, and lower cost of operation.

1.4.4.3 Super-PON Implementation scenarios for Quayside

Sidewalk Labs proposes to apply recent advances in fibre-optic technology and new approaches to network management ay Quayside. Sidewalk Labs would provide technical guidance and requirements and work with Waterfront Toronto's broadband internet partner, Beanfield Metroconnect, to build out the required physical infrastructure and operate the network.

---

[32] Tim Fisher, "5G Availability Around the World," *Lifewire*, September 26, 2019.
[33] Dan Littman, et al, "Communications infrastructure upgrade: The need for deep fiber," Deloitte, July 2017.
[34] Jayant Baliga, et al, "Energy Consumption in Wired and Wireless Access Networks," *IEEE Communications Magazine*, June 2011.

Beginning in Quayside, Sidewalk Labs' proposed design for a fibre-optic backbone would be connected to two major Internet Points of Presence (POPs) in downtown Toronto. The proposed designs would be able to be upgraded over time without replacing much of the infrastructure. Sidewalk Labs plans to evaluate whether an additional POP is required to provide sufficient redundancy. Sidewalk Labs proposes to work with the local broadband internet partner to install fibre sufficient for Super-PON — but depending on the initial cost and availability of Super-PON terminating equipment, may opt to use Gigabit Passive Optical Network (GPON) equipment, since Super-PON's advantages are much less significant at the Quayside scale. As development expands, the GPON equipment can be upgraded to Super-PON.

In Quayside, Sidewalk Labs proposes that the conduits holding the fibre have express and local routes, as well as regular handholes (access points). Each building would serve as an aggregation point for outdoor fixtures capable of mounting digital devices, such as streetlights or poles, and would have fibre-optic runs to provide additional access if needed.

At wider scales, further enhancements could be possible, including laying out the fibre-optic backbone as a loop so that a fault at any location would not disrupt access further along the fibre.

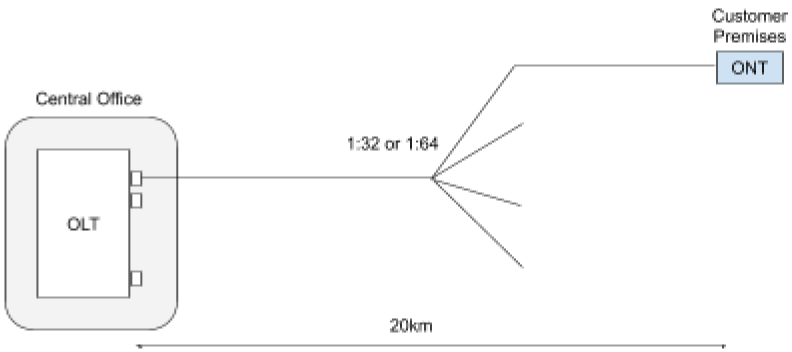
1.4.4.4 How Super-PON works: technical overview and current state of the technology[35]

Passive optical network (PON) has been widely deployed as the last-mile platform for broadband FTTH (Fibre to the Home) access networks. In fact, PON is almost used synonymously to represent FTTH. As the name implies, PON systems employ an unpowered passive fibre plant infrastructure between carriers' central offices (COs) and customer homes. The passive nature of PON makes it easy to deploy (as there is no need to coordinate with power utility companies) and more reliable to operate (active network elements are more prone to failure).

Conventional PON systems use a passive power splitter to broadcast optical signals from the optical line terminal (OLT) at an operator's CO to end users, as shown in the following figure. The signal from the CO is terminated at an optical network terminal (ONT) in the customer premises. The ONT performs the function of an optical modem, which converts the optical signal into electrical signal for in-home network consumption.

[35] This technical overview section is excerpted and adapted from a white paper written by Jeff Tarr of Sidewalk Labs and Cedrick F. Lam of Google Fiber. Available upon request.

Figure: Conventional PON System



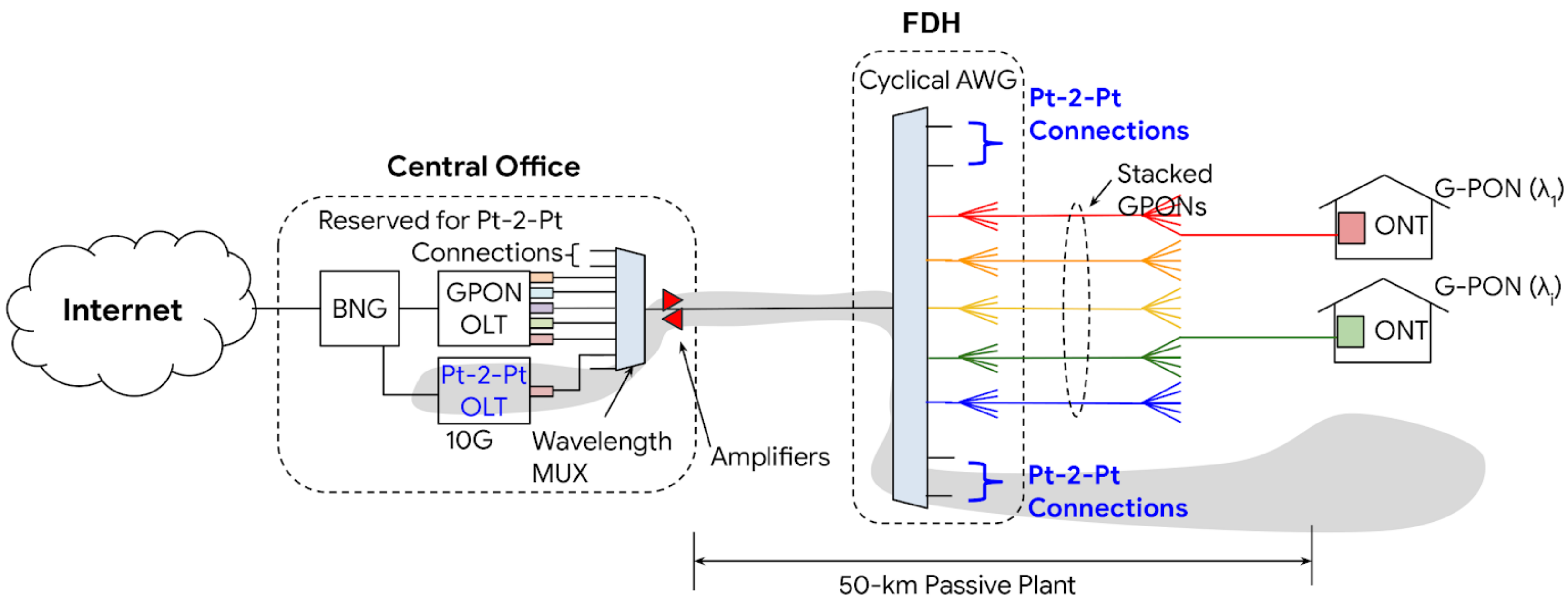
The power budget between the OLT and ONT limits the reach between the CO and customer premises and the splitting ratio. Conventional PON systems usually are limited to a 1:32 or 1:64 splitting ratio (for example, every 32 or 64 users requires a fibre terminated at the CO) and 20km of transmission reach.[36] Currently, the most commonly deployed PON systems are G-PON systems defined by the ITU-T G.984 standard.[37]

The number of users each CO can serve is limited by multiple factors, including the number of fibre terminations available at a particular CO. For example, a 288-core fibre cable with a 1:32 splitting ratio can terminate 9,216 users. The size of the fibre cable is finite. The larger the cable size in terms of number of fibre strands, the more difficult and expensive it is to construct and maintain such cables. Large metropolitan areas are usually constructed with a dozen or so COs, which are interconnected through a metro backbone. COs are active sites requiring management, hence the associated operational costs. In addition, the permitting process of COs is time consuming and cumbersome. Most cities do not like COs, as they are usually unsightly and may require backup power generators. It is therefore advisable to consolidate COs from the viewpoint of both easy construction and easy management.

Super-PON is capable of supporting 768 users per fibre strand from the CO and extended reach of 50km. The Super-PON system makes use of the Wave Division Multiplexing (WDM) techniques developed in long-haul transmissions to increase the PON capacity. In this Time Wavelength Division Multiplexing (TWDM) Super-PON implementation, individual GPON channels (on different wavelengths) are carried using lights of different colours (wavelengths), which are multiplexed onto a single strand of fibre as shown in Fig. 2. Thus, the fibre capacity is multiplied by the number of wavelengths employed.

[36] GPON, "How GPON Works."
[37] Wikipedia, "G.984."

Figure: Time Wavelength Division Multiplexing (TWDM) Super-PON Technology Illustration



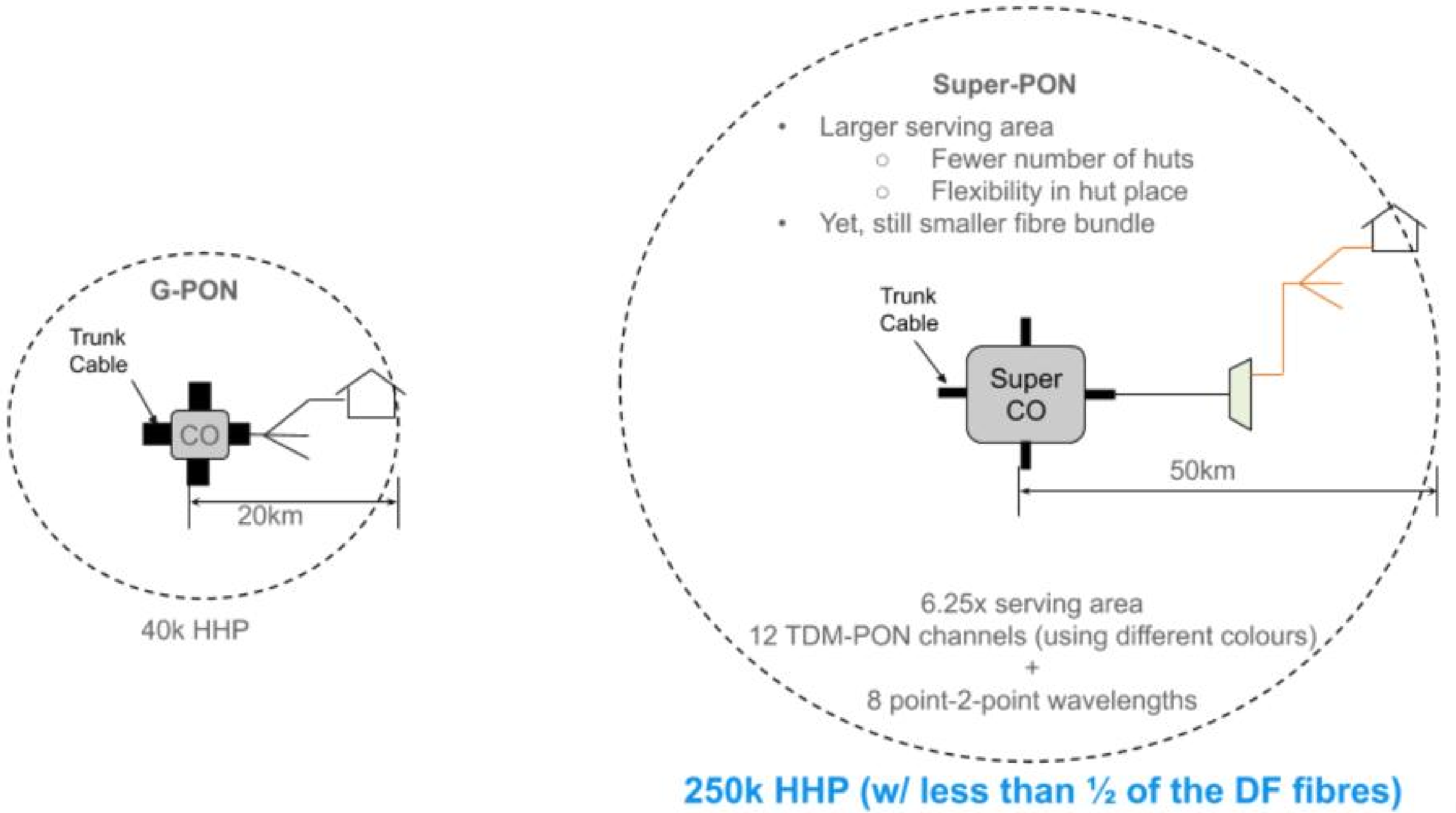
Super-PON uses 20 wavelength channels. The number of wavelength channels adopted is a balance between cost/implementation difficulty and the overall system capacity. Out of the 20 wavelengths, 12 of them are modulated with the conventional GPON signals, which are time-shared among the GPON users.

A passive wavelength routing/splitting element, in the form of a cyclical arrayed waveguide grating router (CAWG) is used in the field to separate the individual wavelengths. As indicated in the figure on the page above, each coloured GPON wavelength channel is further split with optical splitters to broadcast the optical signal to the individual users. To increase the reach of the system, an optical amplifier is used at the CO to boost up the signal level. The optical amplifier is shared across all wavelengths (and all the users served by those wavelengths), thus the amplifier cost per user is very small.

The ONTs in the Super-PON architecture use very low-cost wavelength tunable laser to establish connections with the OLT through the CAWG. Traditional tunable lasers have very stringent requirements developed for long-haul transmissions. Google Fiber has spent extra effort to dramatically reduce the cost of WDM technologies, especially those of tunable lasers, to make it accessible to use in access networks. The software in the OLT and ONT makes wavelength tuning transparent to network operators so that the installation and operation of the TWDM Super-PON is as easy as conventional G-PONs from a data networking viewpoint.

The figure on the page below shows the comparison of CO coverage using conventional PON technologies and Super-PON technologies. The thick, dark lines emanating from the CO (indicated as trunk cable in the figure) represent the size of the optical cables required to connect to the CO for the number of users supported, and they have been drawn to scale.

Figure: Comparison between Conventional G-PON and Super-PON



Convergent wireline and wireless access networks
An important feature provided by the Super-PON is the coexistence of point-to-multipoint (PtMP) time division multiplexing (TDM) connections to residential users and point-to-point (PtP) connections on the same fibre plant infrastructure.

Residential FTTH users usually have low average data rate requirements. The PtMP TDM-PONs makes efficient use of wavelengths by allowing not only statistical multiplexing but also momentary burst operation of up to the whole TDM-PON's aggregate bandwidth. Modern 4G and 5G wireless networks also require significant fibre resources for backhaul connections to traditional base stations and fronthaul applications to remote radio heads. Fronthaul is becoming more and more important for cloud radio access network (C-RAN) deployment. Such applications not only have very high bandwidth requirements but also have very strict timing and latency requirements. Wireless fronthaul is usually implemented with dedicated dark fibre connections. Demand for fibre resources is soaring as operators begin deploying 5G wireless networks.

There are eight PtP wavelengths along with the 12 PtMP wavelengths in the wavelength plan of the Super-PON (see further in the figures below). Google Fiber has developed and verified 10Gbps transceivers on these protocols and data-rate agnostic links. They can be used to support wireless fronthaul connections whose strict timing requirements would not survive on current TDM-PON systems. They can also be used for connections to other high-value services, such as enterprise connections requiring guaranteed and symmetric 10Gbps connections.

Figure: Coexistence of High-Value PtP Services and Wireless Fronthaul/Backhaul Links on the Super-PON System

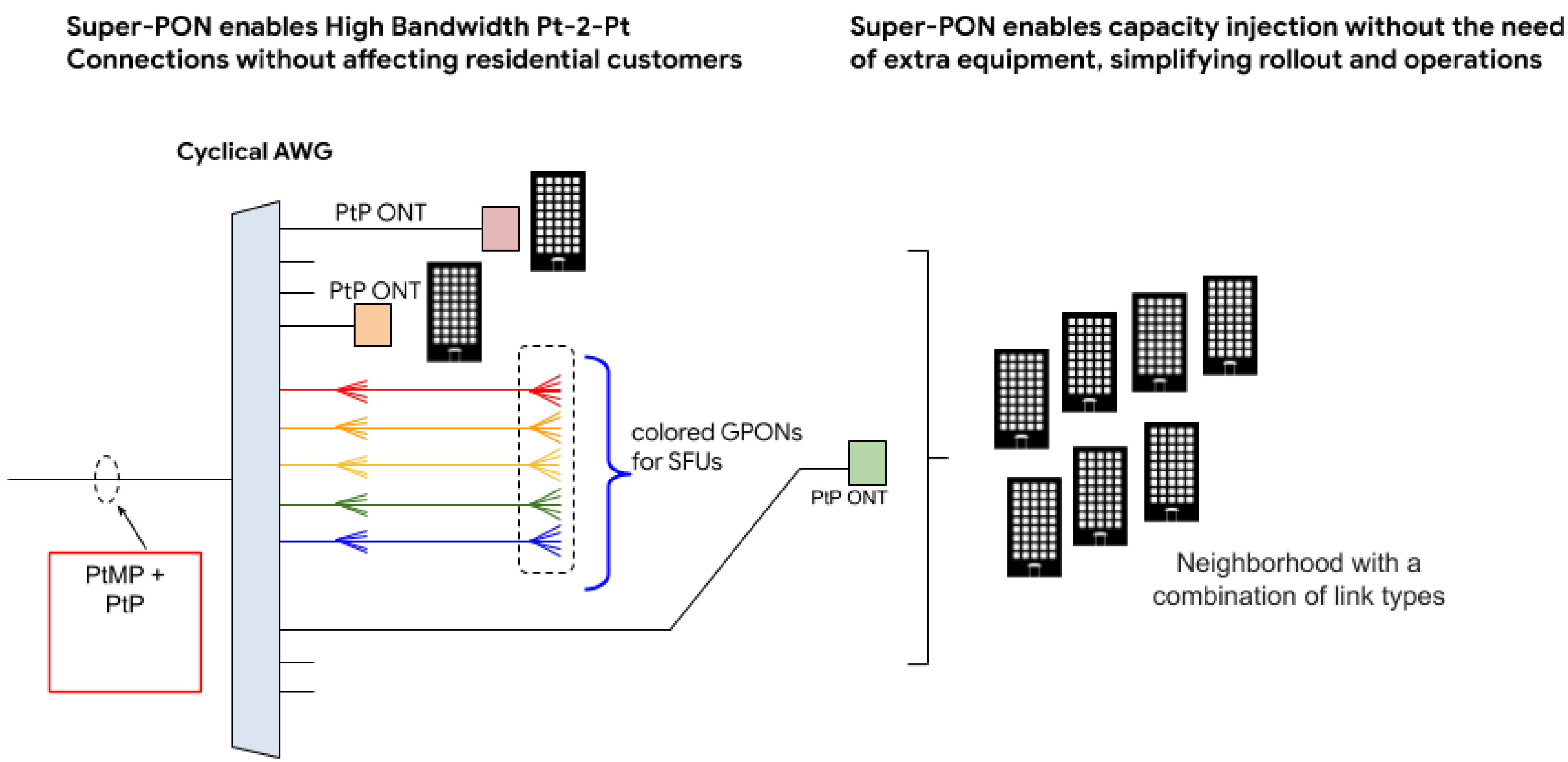
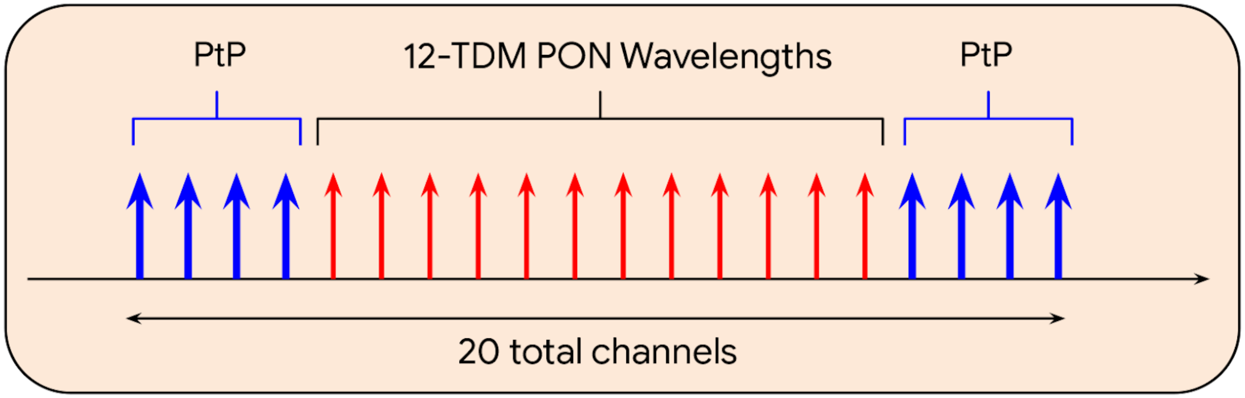


Figure: Super-PON Channel Plan

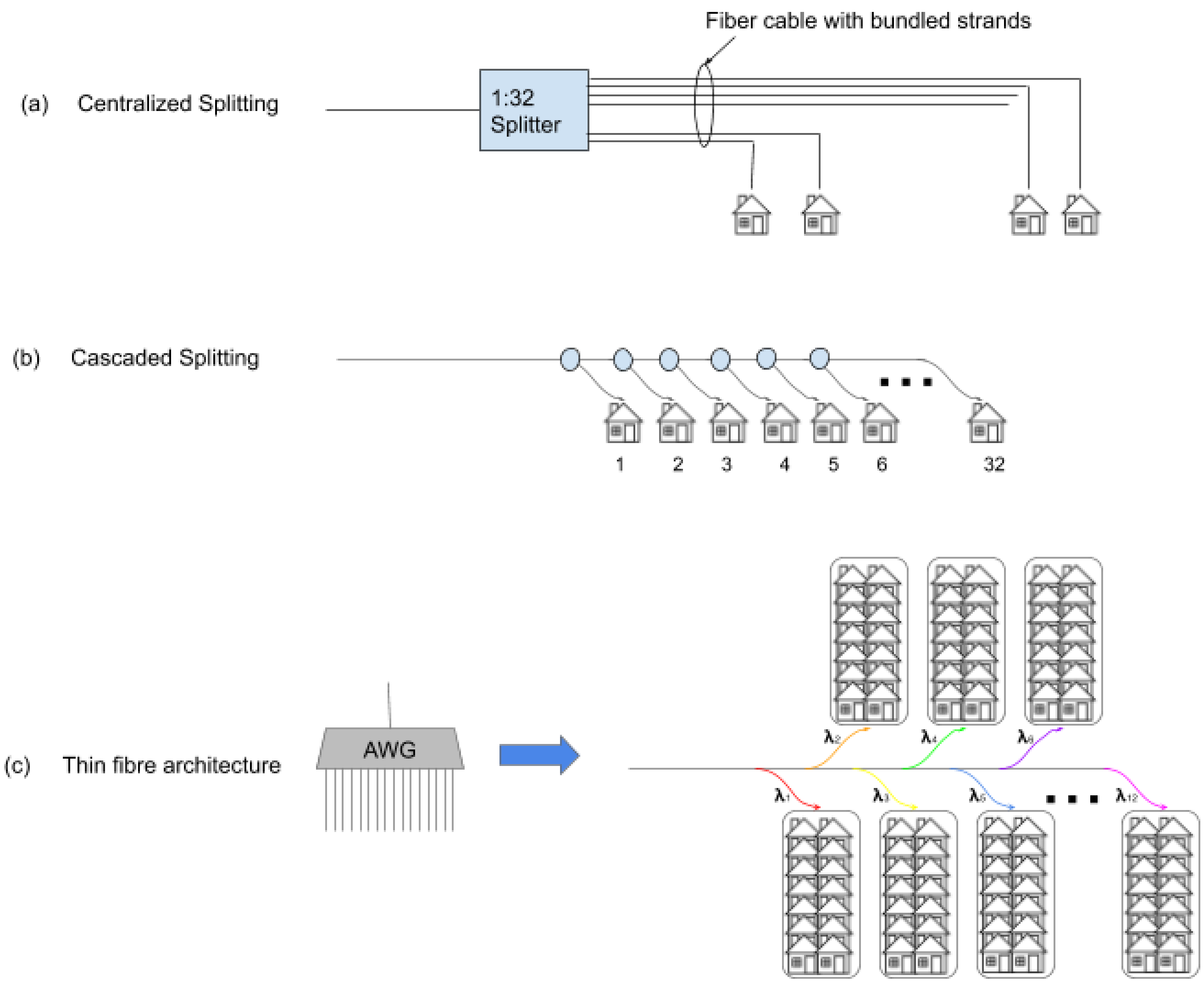


As wireless networks are becoming more and more important, the ability to carry such converged wireless and wireline services in a single managed system would reduce complexity and maintenance costs.

Thin fibre architecture

Traditional FTTH architecture adopts a star architecture. The fan-out of the splitters are connected to a fibre cable with a bundle of fibre strands that are “peeled off” one by one along the way to connect customer homes, as shown in Figure (a) below. In certain scenarios, the number of fibre strands may be limited — a splitting structure with cascaded splitters along the way may be desirable, as shown in Figure (b). This idea could be further explored with wavelength add/drops cascaded as a bus along a trunk fibre, and each wavelength branch could use the cascaded splitters as shown in Figure (b). This kind of thin fibre structure has been studied by Google Fiber to determine the savings in reduced materials and space requirements.

Figure: Thin Fibre Architecture



Summary
The Super-PON fibre access architecture is a novel technology to multiply the capacity of access fibres and extend the passive footprint of fibre access networks for easier construction, better reliability, and lower cost of operation. The Super-PON specification is now being studied by the IEEE Standards Association for possible inclusion in its 802.3 international standards for telecommunications.

It increases the speed of network construction by reducing the complexity and time of the permitting process and greatly reducing the number of active CO sites. Super-PON provides the path to a shared fibre plant infrastructure for converged wireline and wireless access networks. It offers massive bandwidths and a massive number of connection endpoints and could be useful for building scalable networks for future smart cities with demanding communication requirements.

1.4.5 Distributed Verifiable Credentials - privacy-enhancing infrastructure

Responsible data practices are the foundation of technology development at Sidewalk Labs. Distributed verifiable credentials, an emerging and promising privacy-preserving technology, provides individuals with control and transparency over the personal information they share in order to access digitally enabled products and services.

Verifiable credentials are a critical technical component on Sidewalk Labs' privacy innovation roadmap. Verifiable credentials, data minimization, and zero-knowledge proofs will be crucial components of how Sidewalk Labs will enable the protection of personal data within cities and provide people with a means of gaining secure and convenient access to services with reliable data privacy controls.

Distributed verifiable credentials enable people to prove their identity or verify other personal details with relying parties in a safe and secure way, without oversharing personal information. Conceptually, distributed verifiable credentials are similar to credentials used to authenticate websites online — when a lock icon appears in the URL bar, your browser has successfully parsed a digital credential that says you're really talking to the website you think you are.

As part of a set of digital infrastructure proposals for Quayside, distributed verifiable credentials supports Waterfront Toronto's Urban Innovation priority outcome for Quayside.

Distributed verifiable credentials also support aspects of Waterfront Toronto's *Digital Principle #3 : Everyone will be able to understand how their data is being collected and used, and how organizations can and will be held accountable for their practices* by providing people with an innovative way to control how their personal data is used and accessed by others and *Digital Principle #4: Strong privacy protections will be in place at all times* by advancing a technological infrastructure that limits the collection and use of personal information while enabling access to services.

1.4.5.1 What are distributed verifiable credentials and why are they innovative?

As the number of digitally enabled products and services in cities rise, people will need to manage an increasing number of accounts, logins, and passwords. A decade ago, city dwellers did not need an online account for such simple tasks as taking a cab, finding a dog sitter, hiring a housecleaner, or ordering a pizza. But as real world services become digitized, people are maintaining a bewildering array of digital accounts to access and pay for daily services (Uber, Rover, TaskRabbit, and Foodora, for the examples above). With each account, passwords must be created and remembered, and sensitive personal information is stored with an increasing number of organizations. As analog services continue to become digitized, this trend will only continue.

Very few credential systems today allow someone to use the same credentials online and offline to access a meaningful number of services. Presenting a physical credential like a driver's licence is the most common way in which someone proves their identity in the real world, but it is difficult to use a driver's licence to authenticate online. Furthermore, presenting a driver's licence often divulges levels of detail that are unnecessary in some contexts. For example, to simply prove one's age when entering a bar, one's full name, address, and date of birth, and many unnecessary pieces of information are also provided. A consistent user experience and data standard for transferring information between people and organizations would better enable the responsible use of technology in cities.

Distributed verifiable credentials

To meet these challenges, Sidewalk Labs has investigated distributed verifiable credentials: small pieces of data that are cryptographically "signed" by an issuing entity and can be authenticated when presented by a user to a service provider. A distributed verifiable credential can represent the same information as a physical credential such as a driver's licence, university diploma, passport, or health card. But, instead of presenting raw information, a verifiable credential can be used to perform a proof over the information, like whether the information satisfies a binary true/false, or fits within a range of acceptable values. For example, rather than providing a full date of birth, a distributed verifiable credential can simply state that a person's age is greater than 19. Or it can verify whether, for example, a person holds a government-issued Ontario driver's licence or a bachelor's degree from an accredited university, without divulging details like the specific licence ID number or where the bachelor's degree is from. This is accomplished through a complex mathematical equation.

Distributed verifiable credentials are not managed by a single authority or stored in a central repository, rather, they live on a user's device — a smartphone, smart card, or key fob, for example — and are shared with a relying party at the user's discretion. The data transaction is cryptographically secure and mirrors how identity verification is conducted in cities today: a person proves their identity directly to the relying party, peer-to-peer, without involving a third party. These cryptographic proofs of credentials allow users to make provable claims about who they are without disclosing raw information. These proofs are verifiable in that they are issued by trusted, and often regulated, counterparties such as banks or government institutions.

The associated technology can enable personalized experiences and distribution of information without compromising the privacy of residents or visitors. Distributed verifiable credentials reveal only the necessary information to authenticate to a service, with explicit user consent, in a process called selective disclosure. Users of the system are able to understand to whom, and for how long, their personal attribute data (that is, their credentials) are being transacted with and used to access a service. And the credentials are fraud-proof, given appropriate certification infrastructure for service providers.

Verifiable credentials are in many ways similar to notarized documents, in digital form. A person who wants to verify that a statement made on the document is true can check the notary's mark, as well as the signature and letterhead of the document. If they trust the issuer of the document, they can trust the statement is true.

1.4.5.2 Why are distributed verifiable credentials beneficial?

A solution to advance distributed verifiable credentials can benefit both individuals as well as businesses that have to handle personal information. For individuals, distributed verifiable credentials would provide much more control and transparency over how their personal information is used; for businesses, the same solution can lead to substantial cost savings and for some businesses new types of services (such as banks).

Benefits for individuals

Services collect too much Data – Many services that exist in cities today require a system to manage the people who want to use the service: libraries need to keep track of who has checked out books; offices need to keep track of tenant leases and visitors to the building; and some 311 systems require some knowledge of the people reporting issues with city services.

All of these services have a clear purpose for collecting some amount of data, but in many cases they do not require true personal information in order to function and create value. Using one of the examples provided above, a 311 feedback tool for a neighbourhood might only require proof that someone lives in a neighbourhood, rather than an individual's full name and address. An office building might only want to know that a visitor has been given building access by an authorized tenant, rather than needing every visitor's name and address.

Sharing your identity using traditional credentials been an all-or-nothing system. Consider the previous example of showing ID to purchase alcohol: bars need to know their patrons are of legal drinking age, but do not need an exact date of birth, name, or address. And as companies continue to disrupt the methods by which people consume and provide traditional services, the need to verify user identities will follow — as will the proliferation of personal information into more and more hands.

Users worry about data collection – Increasingly, individuals are demanding to know how services use their data. Users of digital services often do not have confidence that their privacy is protected, and are concerned with having too many accounts that require the disclosure of personal information. In addition, as more and more services collect slices of data, the risk of re-identification increases if the data streams are linkable.

Sidewalk Labs believes people should be able to directly control their data disclosure while interacting with services, and that this control should be easy and intuitive to even the least tech-savvy people. For some services, it is difficult today to control or manage what information is given to that service beyond simply choosing to opt out of the service entirely, which is an unavoidable loss for people who might otherwise benefit from innovation but are too wary of the exposure and risk they might be subject to by participating.

Use cases and examples – Sidewalk Labs has explored several use cases for distributed verifiable credentials, including housing applications, reserving a pick-up or drop-off space at a dynamic curb, and reporting anonymous household energy consumption. These use cases are illustrative of how a distributed verifiable credentials solution would be beneficial for Quayside.

- **Housing applications** are often an onerous process that require the exchange of highly sensitive financial information, like employment pay stubs and bank statements. Especially in the competitive housing markets of Tier 1 cities, people are incentivized to disclose even more personal information in order to appear as attractive tenants to a property management leasing office. User research performed by Sidewalk Labs concluded that people prefer to share less personal financial data, in fear of fraud and identity theft, and that they feel especially vulnerable if there are many disparate leasing offices holding copies of their data.

  An identity management system that leverages verifiable credentials gives people greater control over their financial privacy during the leasing process by allowing users to prove that information is true, like their ability to afford the lease, without disclosing the actual data behind it, like net worth and salary. In such a system, banks could issue a digitally signed certificate attesting to the financial solvency of the prospective tenant without sharing the dollar amount of their savings account or biweekly direct deposit — this would be instead of the prospective tenant sharing copies of their bank statements to the leasing office.

- With a **dynamic curb** that governs access to scarce curb space, people seeking to use the curb (for parking, pick-ups, or drop-offs) could be issued a reservation by the curb management entity without linking the reservation to a personal parking account. A blind curb reservation system would be just as effective at managing space without requiring users to sign up for a personal parking account (that might track the location of every reservation).

- **In the home**, people might be incentivized to report their household energy consumption in order to help optimize the demand-response profile of the grid, and could do so with minimal personal data exposure. With distributed verifiable credentials, a user could prove that their household energy consumption contributed to the net energy consumption of a particular geography (such as a block, ward, or neighbourhood) without disclosing their exact address or further information about how the energy was used.

Benefits for businesses and organizations

Identity verification and fraud protection is costly for business – Verifying a person's identity can be resource-intensive, costly, and onerous for organizations.[38] The most common way to do so is to verify against a third-party database (such as LexisNexis), but businesses may also use linked social media accounts, a scanned ID, or personal identification numbers.

Collecting and managing this information is difficult for businesses. It involves expensive engineering resources for integration, large databases of personally identifiable information, guarding against data breaches, and meeting privacy regulations related to data transparency. These steps can also make onboarding complicated and may discourage customers or providers from joining a service.

[38] John Callahan, "Know Your Customer (KYC) Will Be A Great Thing When It Works," *Forbes,* July 10, 2018.

The biggest potential benefits for businesses include time/cost savings and fraud reduction. By cutting time to sign up for new services from weeks to minutes, businesses can see cost reductions of up to 90 percent in customer onboarding; and worldwide, theft of consumers' identities cost businesses an estimated $141 per person.[39]

Relationships with trusted institutions are not leveraged – Regulated institutions like banks, governments, and telecom companies are required to store validated information about their customers. Banks, for example, have Know Your Customer (KYC) compliance programs with comprehensive processes to verify a person's identity. They demand extensive documentation and undergo rigorous checks of clients in order to estimate risk, whether it is in lending money or to avoid being used for money laundering or other illegal activities. They are stewards of data and personal information, accountable to and trusted by both service providers and individuals. However, there is presently no easy and effective way for consumers to create, manage, and use their trusted identity profiles online and in-person for services, which could be an opportunity for these trusted institutions, if a data standard and transaction format can be developed and can be widely adopted.

[39] Olivia White, Anu Madgavkar, James Manyika, Deepa Mahajan, Jacques Bughin, Michael McCarthy, and Owen Sperling, *Digital Identification: A Key to Inclusive Growth,* McKinsey Institute, January 2019.

1.4.5.3 Implementation scenarios for Quayside

Engagement and participation with Canadian industry/community – Sidewalk Labs has been closely monitoring developments in privacy-preserving technology, and following the work of researchers and policy-makers who are advancing the deployment of distributed verifiable credentials and other forms of secure digital identity. At IdentityNORTH, Canada's annual convening of industry and government experts on privacy, digital identity, and the future of the Canadian digital economy, the Information and Privacy Commissioner of Ontario talked about the importance of advancing Canadian digital identity to allow for interoperability across services and sectors, an initiative the IPC has been working on since 2000. At the KNOW Identity Conference in Las Vegas, an industry event focused on identity and trust, there was a rich discussion on digital identity, which was largely focused on risk, fraud mitigation, and on privacy regulation (such as the General Data Protection Regulation [GDPR] and The Personal Information Protection and Electronic Documents Act [PIPEDA]) and how it affects the expanding data economy.

Research and development into solutions – Presently, Sidewalk Labs' research and development has implemented an end-to-end technical prototype for distributed verifiable credentials based on the U-Prove protocol. This, in addition to engagement with many of the researchers and companies in this ecosystem, has helped Sidewalk Labs determine that distributed verifiable credentials is a viable privacy preserving technology that will likely be developed by the burgeoning ecosystem for deployment in Quayside.

Based on Sidewalk Labs' engagement with industry, and investigation of the use cases and needs for digital credentials in cities, Sidewalk Labs would not build this technology, but instead would focus on understanding the space and what a desired solution should look like. Roughly, the desired architecture is composed of **privacy-preserving verifiable credentials,** connected by an **auditable and resilient public key infrastructure,** and an **open standard for managing credential schemas** — described in further detail in section 1.4.5.4.

1.4.5.4 Technical description, data flow diagrams, and design specifications for a distributed verifiable credentials solution

In this section, Sidewalk Labs presents a high-level description of what a desired architecture could look like. There are three parties in this ecosystem: issuers, holders, and verifiers. The whole verifiable credentials system relies entirely on an ecosystem of trust across issuers, holders, and relying parties.

Issuers: Issuers are trusted institutions with important identity requirements, such as banks and governments, that can issue encrypted credentials to holders (that is, people).

For example, a bank could issue credentials that verify a person's name, age, or credit score. A provincial government could issue credentials that vouch for a person's age, address, or voting eligibility. These credentials would be transmitted directly from the issuer to the holder's device. Issuing authorities would be able to use this technology to simplify, digitize, and standardize their relationships with holders.

This distributed verifiable credentials system could allow multiple trustworthy institutions to participate and issue credentials if they wish, including the City of Toronto. No one — including Sidewalk Labs — would be a sole or centralized manager of authority.

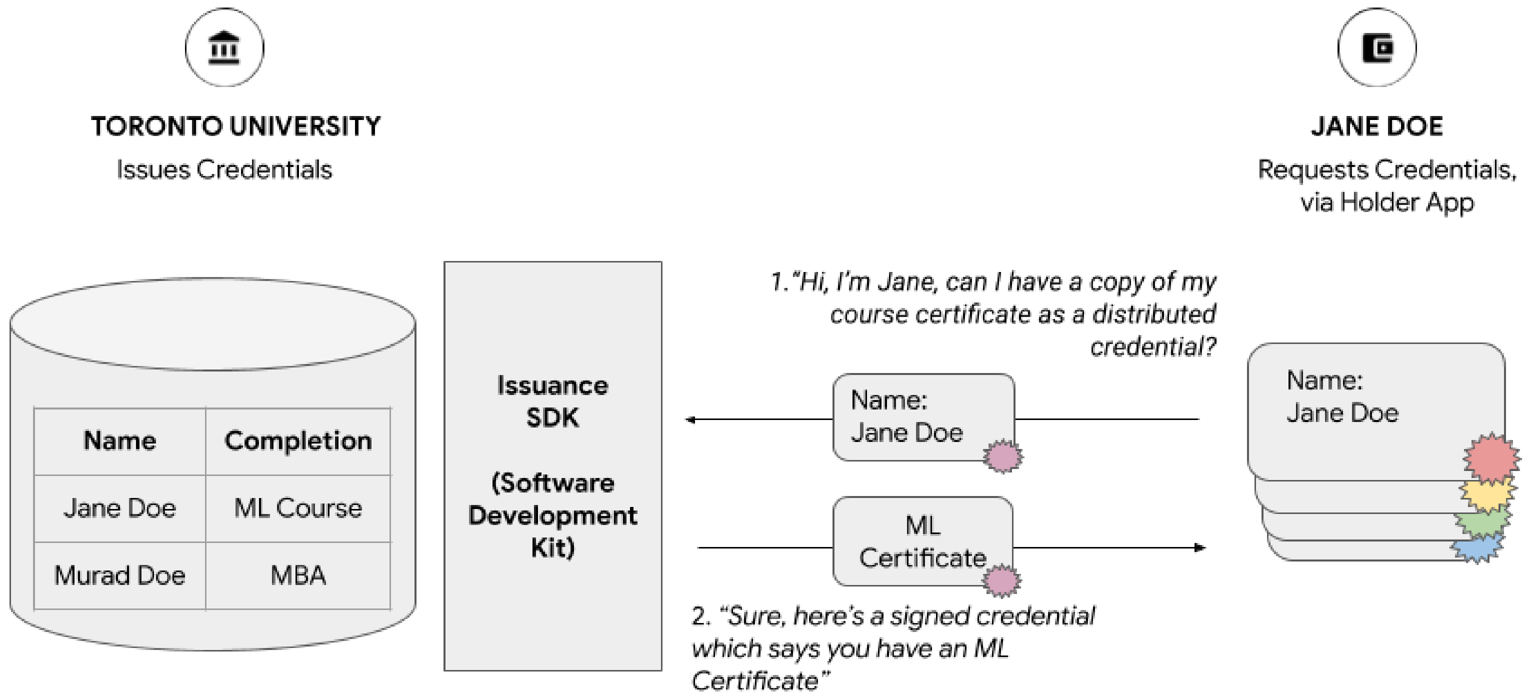
Holders: Holders are verified individuals who manage and use credentials stored locally on their device. These credentials, provided by issuers, can be used to verify the user's identity (name, birth date, address), education qualifications, and financial status, for example.
The holder can use these credentials to access digital and in-person services, in lieu of having to sign up for user accounts or carry an ID card. This provides more convenient access to services, and reduces the amount of personal information that is unnecessarily shared between parties. Data would be centrally controlled by the holder, who can choose to store a backup with their bank, government, or brands they trust.

Verifiers: Verifiers, also referred to as relying parties, are the companies and organizations that provide services to people, such as car rental services, employers, landlords, short-term housing rental hosts, and more. Instead of managing a database of accounts or collecting personal information to verify a person's identity, they can use the distributed verifiable credentials provided by the holder.

Limiting the amount of personal information collected also reduces liability and risk: you cannot suffer from a data breach if you do not store any data. That risk can impede verifiers' ability to bring their services to people who want them. With secure distributed verifiable credentials, service providers can reduce the risks related to storing personal information.

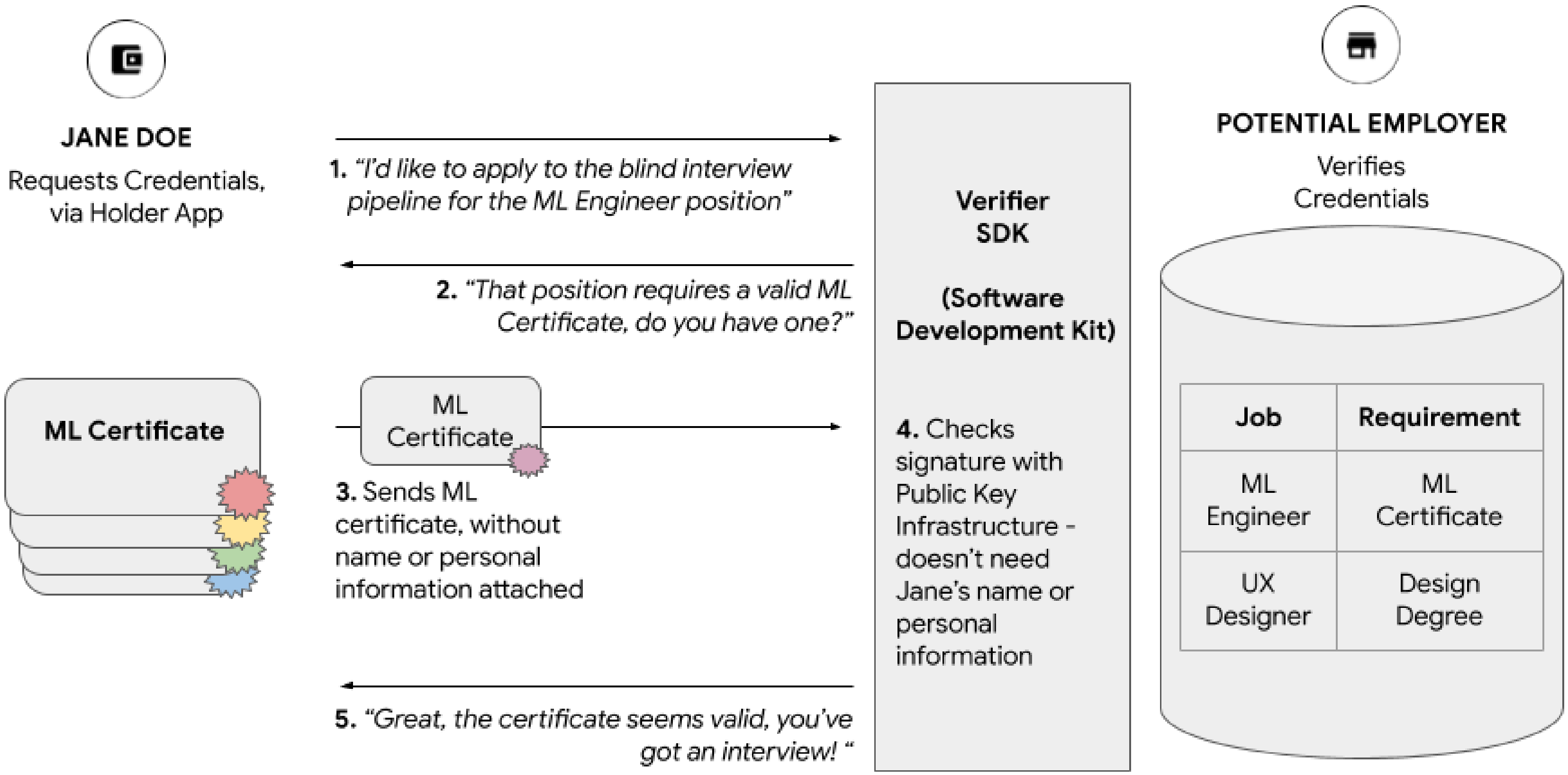
Data Flow
The following two diagrams together show what a desired architecture for distributed verifiable credentials could look like. There are two parts of the process — credentials issuance, represented below by Toronto University, and credentials verification, represented by an employer.

Figure: Distributed Credentials with Verifiable Claims — Credentials Issuance



This simple diagram illustrates how a university issues a distributed verifiable credential to a student by using a software layer ("Issuance SDK") to produce a cryptographically secure copy of the credential and transfer it to the student's device. Jane Doe completes an ML (machine learning) course and is issued a certificate of completion by Toronto University. Toronto University holds a database of certificates of completion and issues a digitally "signed" certificate in the form of a distributed verifiable credential to Jane Doe. Jane Doe can store and use this credential for job applications that require a ML course certificate.

Figure: Distributed Credentials with Verifiable Claims — Credentials Verification



Following the above example, Jane Doe pursues a blind application process (i.e., an application process that corrects for bias and discrimination by blinding all subjective attributes of the applicant and only verifying training, certification, and education requirements of the applicants) for an ML engineering job. The potential employer is the verifier that requires that all applicants submit an ML certificate in order to accept the job application. Jane Doe submits her ML certificate and is granted an interview. The verifier cryptographic software layer (SDK) enables the potential employer to view the job application that contains Jane Doe's ML certificate (in the form of a digitally-signed distributed verifiable credential) without revealing her name or other information that might bias her application and prevent her from being granted an interview.

Design principles for distributed verifiable credentials
Some types of verifiable credentials have the following properties:

Verifiable – Data can be positively identified as having been unchanged between issuance and verification of a credential, and verifiers can prove to themselves that a particular, trusted organization issued the credential, like a real bank or library, rather than a scammer.

Optionally anonymous – If a credential does not disclose personal information (only proof that you live in a particular postal code, for example), then it is difficult if not impossible for an issuer and a verifier to figure out more information about the credential, even if they are colluding.

Stored on device – Credentials do not live in the cloud, but are owned and stored by the individual. This gives individuals ultimate control over their data. The credentialing system should also be deployable on inexpensive devices and work offline in a low-power mode.

Allow selective disclosure – People can choose to disclose only a small part of a larger credential. For instance, if a credential contained the attributes of name, address, and postal code, a holder could show only the postal code attribute to a verifier, without revealing any other information.

Allow proofs over attributes – A holder can make what is called a zero-knowledge proof over the values of their credentials, rather than revealing the actual value. For instance, a job searcher can prove to a potential employer that they have a university degree, rather than revealing the name of their university, which might reduce bias in the hiring processes.

Machine-readable – Most credentials used in cities today are readable by humans, but very few are readable by computers. Verifiable credentials are machine-readable, allowing for the use of the same credentials both online and offline.

Accessible and offline – These credentials must also have failure modes that allow them to work offline. They also must be accessible to a broad and diverse swath of the population.

These properties enable an interoperable and modular system of credentialing (which log-in and account systems could be built on top of) that is resilient and auditable, and in which the owner or creator of the system does not have to know every transaction that happens using the protocol. This directly contrasts with existing digital protocols like OAuth and OpenID Connect, which, if implemented in a city that extends interoperability into public municipal services, would mean that the operator of the system sees every transaction.

Public key infrastructure (PKI) and transparency
A core requirement for distributed verifiable credential infrastructure is the ability to prove that a particular organization, entity, or person signed a particular statement, and to verify that the signature on that statement is correct. This is commonly done today with public key cryptography. Many public key cryptography schemes today are based on

the concept of a “web of trust,” in which a public key is trusted if it is signed by another person the verifier trusts. This creates several difficulties. For one, it is difficult or impossible to join the system without knowing someone who is highly trusted. Secondly, verifying a signature without being connected to an entity that has signed a large number of keys is difficult.

The critical issue is where to post public keys such that a log of all changes to the bulletin of keys is public. Many key bulletin boards exist, but if keys are compromised and changed without the consent of the real holders, it is impossible for these holders to plead their case. Conversely, the Secure Sockets Layer (SSL) infrastructure that powers web browser security has centralized this scheme into “certificate authorities” that effectively have the ultimate power to issue certificates to anyone, at any time.
Some sort of auditability is necessary in order to entrust real-world credentials to a PKI-based scheme. Instead of several highly trusted authorities managing keys, keys should be managed by publicly posting them in a single, auditable database. Innovations like Certificate Transparency (CT) in the SSL space provide guidance here; they have proved it is possible to host a public, auditable log in a single place and mirror it for resiliency. In many ways, technologies like blockchain are overkill for the problem of hosting keys: CT proves that auditable key management can be done centrally. A government, issuing authority, or consortium could host the key infrastructure for credential systems.

Further, technology like Certificate Transparency and its sibling, Key Transparency, could be used by issuers of credentials to provide transparency to holders of credentials: a holder should be able to prove that the issuer has not issued a credential with their attributes to another person. Transparency of system operations is a crucial part of future digital credential systems.

Relevant standards
A standard for distributed verifiable credentials is critical to deploying digital services more broadly, especially in cities where there is a dense set of service offerings that people use on a daily basis. There are several efforts in the space that Sidewalk Labs is closely watching and are described in further detail in section 4.5.5.

1.4.5.5 Overview of existing systems

While investigating how to enable this vision for a new type of neighbourhood and community, Sidewalk Labs explored several existing approaches to user data and identity management. Leading technology companies and governments are innovating in this space, but offer only partial solutions.

OAuth and other common systems
OAuth, short for “open authorization,” is a protocol that allows a user’s account information to be used by third-party services without exposing a user’s password. The promise

these federated systems offer is having one account, but access to many services. For the user, this means only remembering one password and log-in method. This subset includes near-ubiquitous approaches like Facebook Connect. In enterprise contexts, there has been a rise in single sign-on systems, such as Okta or OneLogin. Canadians have had a single sign-on process to use banking credentials to log in to file taxes via SecureKey for years. In general, these systems work well and relieve service developers of the need to manage a database of usernames and passwords, with its associated security and privacy risks.

However, these systems also rely on management by central authority that provides all identity verification for the ecosystem. If that authority is breached, data could be exposed. If that authority loses connectivity to the rest of the ecosystem, no one can authenticate or prove attributes about themselves. Also, every single authentication transaction in the ecosystem must involve that authority, which can make users vulnerable to breaches to that single authority. For example, in the context of a smart lock for building access, using an authentication system like this might involve alerting/logging/recording with the central management authority every time one opens your front door.

Government-level authentication systems

Few national governments have fully embraced digital IDs, but Estonia is a notable exception (see section 4.5.5.1 and section 4.6.1.2 for more details). Over the past decade, the country has issued ID cards that allow residents to authenticate to government services over the internet and in person.

Sidewalk Labs applauds Estonia's approach to ID and hopes to see many of its innovations adopted globally, notably fraud-proof transactions, ubiquitous digital service delivery, and integrations with physical experiences. However, Sidewalk Labs hopes a Toronto implementation will improve on the Estonian model in several ways, most notably by creating more open standards and extending the network of issuers such that the government is not the sole trust provider and issuer of credentials

Aadhaar is India's centralized identity system, provisioned by the government to issue unique identification numbers to citizens. Numbers are assigned and issued to individuals after taking biometrics (fingerprints, iris scans, and a facial photograph) as well as demographic information like names and addresses. Many government-subsidized services, like welfare and healthcare, are only accessible through Aadhaar, so citizens are mandated to input their personal information to claim services. The mandatory linking of mobile phone numbers and bank account information has also made it convenient for both private companies and public agencies to use e-KYC to authenticate transactions. Sidewalk Labs is supportive of the Aadhaar component that enables the expansion of service access to citizens. However, Sidewalk Labs' preferred approach is decentralized and relies on a network effect of issuers and verifiers to enable interoperability. Sidewalk Labs would support a distributed credentialing database where personal data only resides with the citizen, the individual owner of the data.

Multi-source or self-sovereign identity systems
Self-sovereign identity systems are based on the premise that people should control their data. In order to enable ecosystems, the focus is on complete independence from management authorities, like governments, and credentials are stored solely on a user's device. Many of these systems involve forms of blockchain technology in order to keep records of public keys and schema management.

The ecosystem around self-sovereign identity systems has rapidly evolved over the past two years. Systems like uPort and Hyperledger Indy have grown significantly in terms of capabilities and embody many of the properties that a good implementation of a city digital ID would have: user-centric credential management, zero-knowledge proofs of attributes, and a system for storing schemas for credentials. However, there has not been sufficient progress on tools that enable identity recovery or issuance to warrant wholesale adoption of these systems.

In the future, integration with these systems and the standards they embody may be critical for broadening the set of experiences enabled by this approach to verifiable credentials. Organizations like the Decentralized Identity Foundation are doing foundational work on infrastructure for these systems, but this infrastructure still requires further work.

1.5 Sidewalk Labs' approach to open and resilient technology design and implementation

1.5.1 The need for open and resilient approaches for technology design and implementation

In the preceding parts of this section, Sidewalk Labs has provided an overview of its approach to integrating physical planning, urban design, and digital systems as part of development planning, as well as provided more detail on the digitally enabled services and digital infrastructure aspects of the proposal.

Throughout Sidewalk Labs' engagement with Waterfront Toronto and the Digital Strategy Advisory Panel, as well as Torontonians, we have heard concerns expressed about:

- The potential for technological lock-in — the inability of the city to adapt to technologies that are put in place in this development.
- Risks related to security and resiliency of digital systems.

These concerns echo those expressed by people from around the world and have sparked a wide range of approaches and policy responses (see section 4.5.6 Agile and open-technology practices for additional detail).

Sidewalk Labs acknowledges these concerns and is aware of the best practices and approaches to address these issues that are being advanced by a wide range of stakeholders and sectors in Canada and around the world.

In this section, Sidewalk Labs confirms its commitment to applying the principles that were outlined in the Master Innovation and Development Plan (MIDP) for open architecture, published standards, modular components, resiliency, and security; to working with other organizations and institutions who are already advancing these principles; and to identifying how these commitments are responsive to Waterfront Toronto's Urban Innovation and Economic Development priority outcomes and their Digital Principles.

1.5.2 The importance of published standards and open architecture for enabling flexibility and innovation

As described in the MIDP (Volume 2, Page 400[40]), Sidewalk Labs firmly believes that published standards for digital hardware and software, and public access to data collected in the public realm, is fundamental to catalyzing a diverse multi-stakeholder innovation ecosystem to improve quality of life in cities.

A set of published standards around open-data architecture, open access to data collected in the public realm, and open source integration code would enable third parties to build upon this foundation to enable flexibility and spur innovation. For an overview of precedents and ongoing efforts for open source policies in cities, see section 4.5.6 Agile and open-technology practices.

Sidewalk Labs commits to:

- *Open architecture:* providing data in standard formats and via well-defined, public application programming interfaces. Where relevant standards do not exist, it would work with other companies, researchers, and standards bodies to create those standards.
- *Open access:* data collected in the public realm is publicly accessible by default.
- *Open source:* the software source code required for others to integrate with each of these systems would be made publicly available under a free software licence.

These approaches support aspects of Waterfront Toronto's *Digital Principle #1: Everyone will have access to, and benefit equally from, digital solutions* by enabling participation in digital activities through open digital processes and the sharing of data as appropriate. They also support *Digital Principle #2: Digital solutions will be open, ethical, and resilient* by advancing open standards, interoperability, and protocols that do not foster vendor lock-in and dependency.

[40] Sidewalk Labs, [Master Innovation and Development Plan, Volume 2](), Chapter 5, Page 400.

1.5.2.1 Open architecture: public standards

Any digital hardware and software that Sidewalk Labs creates would use published standards. This approach follows that of the World Wide Web, which as a platform for creativity and innovation is based on a collection of public, internationally recognized standards (HTTP, HTML, CSS, SSL, etc). Public standards help:

- Ensure that no single company has a monopoly on providing a critical component.
- Make it easier to replace components of systems.
- Provide a foundation for others to build new tools and services.

For data, where relevant published standards exist, Sidewalk Labs would use them. For Quayside, Sidewalk Labs commits to publishing an ongoing list of standards it uses.

1.5.2.2 Open Application Programming Interfaces (APIs)

Application programming interfaces, or APIs, are standardized programming tools that enable computer systems to communicate and provide a well-documented way for software developers to access public data.

Sidewalk Labs would make its own APIs well-documented and publicly available, and would use public standards where they exist.

Where public standards do not exist, Sidewalk Labs would work with others to define formats that could become standards in the future. As described in Section 3.2.3.4, Sidewalk Labs intends to further engage with the work underway by groups such as the CIO Strategy Council to build on their existing efforts to establish standards that value inclusiveness, open architecture public interest, and respect for individual rights and privacy. Finally, Sidewalk Labs would encourage other organizations and individual developers along the waterfront to do the same.

1.5.2.3 Open access to data

Publicly available data has enabled innovation across multiple industries. By enabling students, researchers, and entrepreneurs to easily try out new ideas, broad availability of data enables and accelerates innovation. Making data available is also crucial to enabling transparency and accountability in the operation of the digitally enabled services and the achievement of priority public outcomes.

Sidewalk Labs is committed to working collaboratively with academic and public- and private-sector partners to ensure that data is made available through appropriate organizational, legal, and technical mechanisms suited to the proposed use and sensitivity of the data. See section 3.2.3.2 for further details on how Sidewalk Labs proposes to support trusted data sharing at Quayside.

1.5.2.4 Open source code for interoperability

Data cleaning and manipulation tasks can take a lot of time and effort, even if data is made publicly available in standardized formats through APIs. Parsing and processing data or writing code that interacts with the APIs can take substantial effort and time.

Sidewalk Labs is committed to open-sourcing software code that enables the use of public APIs and data, in order to support flexible, interoperable digital systems that enable continuous improvement and create more robust and useful software through engagement with a broader technology community.

Open source code that Sidewalk Labs has released to date are available at https://github.com/sidewalklabs. Releases mentioned elsewhere in this Digital Innovation Appendix include CommonSpace, a mapping tool for public life studies, and the visual language and digital channel prototype from the Digital Transparency in the Public Realm project.

1.5.3 Using best-in-class resiliency and security

In the Master Innovation and Development Plan (MIDP) (Volume 2, Page 408[41]), Sidewalk Labs describes its approach to digital security and resiliency for the digital services and infrastructure systems proposed in the MIDP.

Sidewalk Labs' approach includes leveraging best practices as well as public and open standards to ensure that digital systems are not only secure and protected from deliberate cyber-security threats but also function reliably in the face of unusual events.

Sidewalk Labs' approach to digital reliability emphasizes three design goals:

- Prevent disruption and loss of functionality.
- Enable rapid detection of actual loss or increased risk of loss of functionality.
- Prepare to rapidly restore functionality to services that are disrupted.

Additionally, Sidewalk Labs is committed to:

- Adhering to Waterfront Toronto's draft Intelligent Communities Guidelines regarding data residency as they apply to all proponents in the Designated Waterfront Area.

[41] Sidewalk Labs, Master Innovation and Development Plan, Volume 2, Chapter 5, Page 408.

- Adherence to maintaining appropriate network and data security safeguards as required by PIPEDA, as well as following industry best practices generally to prevent breaches of digital systems.

These design goals and commitments, as applied to the digital services and infrastructure systems proposed in the MIDP, support aspects of Waterfront Toronto's *Digital Principle #4: Strong privacy protections will be available at all times* and *Digital Principle #5: Data and systems will remain under local control and be subject to local laws* by advancing data protection through best-in-class security measures; taking steps to ensure that all digital infrastructure and solutions are secure and resilient; and adhering to all applicable policies regarding data residency.

1.5.3.1 Preventing disruption and enabling resiliency through modular components

Sidewalk Labs will, wherever possible, use public standards and open source software with strong institutional and community support to collaborate with practitioners around the world to address problems as they arise. Sidewalk Labs will also use the Common Vulnerabilities and Exposures system — a widely used public catalogue of security threats — to stay abreast of potential problems.

Additionally, Sidewalk Labs will give preference to modularity of systems whenever possible, enabled by its commitments to open standards and interoperability detailed in the previous section. Modularity and reliance on open-source hardware and software makes it easier to isolate, replace, or upgrade individual components.

Given the rapid evolution of best practices as new technologies emerge, Sidewalk Labs' strategy is to follow general best practices as established by the security community for all the technologies it develops or maintains, such as the benchmark security standards, SOC 2 compliance and ISO27001 for applicable products and services.

Finally, as detailed in sections 1.4.2 and 1.4.3, Sidewalk Labs' digital infrastructure proposals for Koala and Software-Defined Networks provides a set of technical means to enhance security and resiliency at Quayside.

1.5.3.2 Ensuring integrity and reliability of digital systems through detection and auditability

Ongoing auditability is key for confirming the integrity and reliability of digital systems. Sidewalk Labs plans to use auditing systems such as Trillian to achieve this objective.

Modularity, another Sidewalk Labs' design preference for digital systems, enables a high degree of transparency, as even when data is encrypted, the amount of data being transferred between systems can be monitored to ensure that systems and devices are operating within expected parameters.

Sidewalk Labs' digital infrastructure proposals are designed to leverage the properties of modular and interoperable systems to ensure reliability and integrity of digital systems.

For example, as described in section 1.4.2, Koala can provide public infrastructure managers a means of monitoring and deactivating devices that might be malfunctioning or otherwise compromised; and, as described in section 1.4.3, Software-Defined Networks help isolate systems to reduce the potential of widespread disruption and loss of functionality affecting multiple systems.

1.5.3.3 Proactively prepare for incidents through threat modelling and ensuring response readiness

Designing plans for detection of or response to incidents requires anticipating potential issues and being prepared to respond to service disruptions.

As detailed in the MIDP in Vol 2, Page 412[42], each digital system that Sidewalk Labs implements for Quayside would use a preparedness assessment to provide clear answers to key questions on threat modelling and response readiness that would be coordinated with relevant agencies and organizations that operate or maintain related systems.

1.5.3.4 Comparison to municipal standards

Sidewalk Labs' understanding of City standards
In addition to adherence to Waterfront Toronto's policies and draft Intelligent Community Guidelines, Sidewalk Labs is committed to ensuring that the digitally enabled services it advances for Quayside meet local government standards.

The City of Toronto's security measures and standards are not currently publicly documented, but Sidewalk Labs looks forward to continuing the dialogue with Waterfront Toronto and city agencies to understand them. However, principles that cities apply generally include those that were outlined in the MIDP (Volume 2, Page 408[43]) – these include:

- **Security by design**: At the point of design or procurement of any digital systems, there should be an explicit focus on minimizing security risks, rapidly detecting any loss in functionality or increased risk of loss of functionality through real-time monitoring and regular audits, and being prepared to rapidly restore functionality to any service that experiences a disruption.

- **Access control**: Implement access controls across all networks and devices, requiring authentication for any access to non-open data or for any configuration

[42] Sidewalk Labs, Master Innovation and Development Plan, Volume 2, Chapter 5, Page 412.

[43] Sidewalk Labs, Master Innovation and Development Plan, Volume 2, Chapter 5, June 2019, Page 408

changes. Devices themselves should be required to authenticate before they gain access to the network.

- **Open, tested technology**: Use public standards, established security frameworks, and open-source software with strong institutional and community support.

- **Network access**: Limit communication between devices as much as possible to minimize the ability for those devices to cause damage or reveal information.

- **Encryption**: All data should be protected in transit and at rest.

- **Disclosure**: There should be well-defined policies that require disclosure of breaches.

Sidewalk Labs' approach relative to City standards
Sidewalk Labs will follow those same principles, using new technology to achieve them more effectively than the status quo allows. Technologies that Sidewalk Labs will pursue include:

- **Access control**
  Requiring devices to have unique cryptographic keys embedded at time of manufacture and the ability to respond to challenges to prove that they are a device that has been permitted to join the network by a trusted entity.

- **Network access**
  Leveraging Software-Defined Network (SDN) technology to constrain device connectivity. If a thermostat should only communicate with a single endpoint to communicate its measurements, then the only route that the SDN will provide it will be to that endpoint. This avoids the possibility that the thermostat can be, for example, co-opted into a botnet, because it cannot receive malicious firmware from another endpoint, nor can it communicate any data to another endpoint.

  Using Manufacturer Usage Descriptions (MUD), the SDN can detect devices that are behaving abnormally. For example, if the MUD for a thermostat specifies that it should only transmit a few bytes once a minute, and it suddenly starts transmitting megabits per second, the SDN can quarantine it by cutting off its network access. Koala also has the ability to detect, quarantine and remove from the network devices that are behaving abnormally.

- **Defining security and resiliency systems**
  Sidewalk Labs plans to leverage the excellent security processes already developed by industry-recognized security organizations, extending them in specific ways as the urban context creates new challenges and opportunities. The core of Sidewalk Labs' approach, however, will remain based on industry best practices.

- **Public resources**
  In addition to commissioning external security reviews, there are many public resources for defining security and resiliency standards, policies, and guidelines. For example, the SANS Institute provides resources and policy templates for the rapid development and implementation of information security policies. Mozilla is an example of a non-profit open-source-focused organization that maintains security policies for contributions, including those from software engineers unaffiliated with the organization. And the International Organization for Standardization (ISO) has also defined a set of standards for security and resiliency. A subset of these will help define requirements with more specificity and clarity.

1.5.4 Data residency

As we have stated in the MIDP (Volume 2, Page 412[44]), the decision on where to store data (data residency) is based on many considerations, including whether there is sufficient technical and physical architecture to store the data security, the costs of storing the data abroad versus in the organization's home country, and applicable laws.

[44] Sidewalk Labs, Master Innovation and Development Plan, Volume 2, Chapter 5, June 2019, Page 412

As agreed to in the resolution process for the Threshold Issues, with respect to the operations of digitally enabled solutions in Quayside, Sidewalk Labs agrees (i) that personal information will be stored and processed in Canada; and Sidewalk Labs agrees (ii) to use commercially reasonable efforts to store and process non-personal data in Canada. Should exceptions be required, they will be determined on a case-by-case basis through a review process.

1.5.5 Data breaches

Sidewalk Labs applies best practices to prevent network and data breaches before they occur and also recognizes its obligations under the Personal Information Protection and Electronic Documents Act (PIPEDA) to maintain appropriate safeguards that include physical, organizational, and technical measures to ensure the security of networks and data that it controls.

These measures include:

- Implementing internationally recognized information security standards, such as the ISO 27000 series of standards.
- Conducting Threat Risk Assessments/Vulnerability Assessments and penetration testing.
- Developing, implementing, and maintaining an information security program to proactively assess risks and implement safeguards.

- Rigorously updating and patching operating systems, firmware, and software.
- Continuous monitoring for unusual network activity.
- Physical measures to limit physical access to digital infrastructure.
- Administrative measures to limit system and data access.
- Security procedures and regular training.
- End-to-end encryption, as applicable.
- Contractual requirements with vendors that provide appropriate safeguards consistent with those above, and notification of network or data breaches.

Additionally, Sidewalk Labs believes in applying best practices to address any network or data breaches that may occur, including having a cyber-incident response plan in place, which includes:

- Detecting incidents and escalating to the appropriate level within the organization.
- Investigating the characteristics of an incident and its impact.
- Containing the scope and severity of incidents.
- Coordinating and managing recovery activities.
- Assessing and managing risks.
- Preserving information associated with the incident, as appropriate.
- Providing notification to insurers, affected individuals, affected third parties, and authorities, as applicable.
- Analyzing the incident after the fact to prevent future incidents.

In the event of a network or data breach, Sidewalk Labs will diligently execute requirements under PIPEDA, other applicable legislation, and contractual obligations.[45] This includes:

- Reporting breaches of security safeguards involving personal information that Sidewalk Labs controls to the Privacy Commissioner of Canada when the breach involves personal information and it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to individuals.
- Notifying affected individuals about such breaches and notifying any third parties that may be able to reduce or mitigate harm, such as other organizations or government agencies.
- Maintaining records of all breaches.

[45] Office of the Privacy Commissioner of Canada, "What you need to know about mandatory reporting of breaches of security safeguards," October 2018.

Section 2

Sidewalk Labs' Approaches to Responsible Data Use and Inclusive Design

Abstract

This section first demonstrates Sidewalk Labs' commitment to ethical and responsible data practices through a detailed explanation of how the company applies its internal Responsible Data Use Guidelines through Responsible Data Use Assessments. Second, it demonstrates how Sidewalk Labs practices inclusive and participatory planning and design.

Table of Contents

Figures

Tables

Section 2: Sidewalk Labs' Approaches to Responsible Data Use and Inclusive Design

2.1 Not having "tech for tech's sake" is about having processes that guide decision-making and actions

Cities all around the world are facing related challenges and stressors, such as sustainability, housing affordability, and congested mobility, and are increasingly looking to new technological tools and increasing amounts and types of data to better deliver and expand services. At the same time, the increasing use of digital technologies in our urban infrastructure and public service delivery has ushered in a number of political and ethical questions.[1]

Technology innovation has always been fundamental in cities. Across history, cities have been shaped by the advent of new technologies, such as the steam engine, electricity, elevators, and the private car. Today, there is incredible potential for digital innovation to improve urban living, yet an approach to ensure the responsible use of such technologies is necessary to fully realize the benefits of these digital innovations for public outcomes.

Sidewalk Labs' approach to city building is to start from the human experience, rather than the questions of what technology to use or what data is collected. One of Sidewalk Labs' Responsible Data Use Guidelines is "beneficial purpose," which ensures that each proposed data activity has a clearly demonstrable purpose and value that would benefit individuals or the community.

Sidewalk Labs believes that responsible data use and being accountable requires going beyond the letter of the law. This means considering the spirit of the law, data ethics, and human rights. It also means actively and consciously designing internal processes and tools such that the Responsible Data Use Guidelines inform Sidewalk Labs' digital planning processes, helping teams consider privacy and ethics throughout their work, from vendor selection to product design to implementation/launch.

Building this internal capacity and set of organizational reflexes to ensure privacy and data ethics by design is an ongoing process, and Sidewalk Labs is committed to having in place and continuously improving on the processes that guide decision-making and actions so as to avoid "tech for tech's sake."

[1] More information on these critical issues in smart cities and digital governance is provided in Section 4.2

2.2 Responsible Data Use

2.2.1 Why do we need Responsible Data Use?

We are surrounded today by digital technology embedded in buildings and the public realm which is often invisible or goes unnoticed. Travelling through the downtown area of a city, or on a visit to a popular public gathering space, one could encounter security cameras, traffic cameras, pedestrian or bicycle counters, Wi-Fi access points, or occupancy sensors that turn on exterior lights or open doors — to name just a few typical systems.

This digital layer has the potential to improve many aspects of our lives — it can help keep us safe, unsnarl traffic, aid in the planning of city infrastructure, provide reliable access to the internet, or make spaces more accessible. This is just as true in Toronto as in most big cities, as diagrams mapping visits to King Street and Yonge-Dundas Square, and showing typical digital building systems found today in Toronto, illustrate below.

But still, there is often a lack of transparency around these implementations. And furthermore the pace of digital technology development and implementation requires a robust approach to privacy and responsible data use beyond simply thinking about the point of collection with notice and consent. Sidewalk Labs believes in a higher standard of data governance: that government should have oversight of plans and implementation, and that the public should know how and why data is being collected and used in our streets and public spaces.

Diagrams of Existing Conditions in Toronto Today
Visits to King Street West (in the block between Spadina and Brant Street) and Yonge-Dundas Square in early October 2019 demonstrated a wide range of technology implemented into the streetscape, primarily serving transportation, security, and connectivity functions.

The first two diagrams below document each instance of technology found in these downtown Toronto locations, including a photo of each item, a brief description of the type and function of the equipment (as best understood) and relevant Digital Transparency in the Public Realm (DTPR) Purpose icon[2] (also as best understood). Notification signs were also documented. In the one King Street block, 38 instances of approximately 28 unique types of equipment were encountered. At Dundas Square, 59 instances of 23 unique items were found. All information - with the exception of the photos themselves - must be considered approximate, as with little signage providing information on the systems deployed, the function and relationships of items found can only be inferred.

[2] For more on DTPR iconography see section 2.3.2.4.

The second pair of diagrams provided below illustrate typical digitally enabled systems found in a modern mixed-use building in Toronto today. A layer of technology is used to operate every major system found in such a building, and the diagrams illustrate typical locations of equipment deployed to control fire alarm, safety, security, plumbing, elevator, ground floor, lighting, heating, ventilation and air-conditioning (HVAC) systems, and power infrastructure. Brief descriptions of the digital equipment and relevant Digital Transparency in the Public Realm (DTPR) Purpose icons are also listed (for more on DTPR see section 2.3.2.4).

Figure: Yonge-Dundas Square in Downtown Toronto —Existing Technologies (and related signage) in the Public Realm

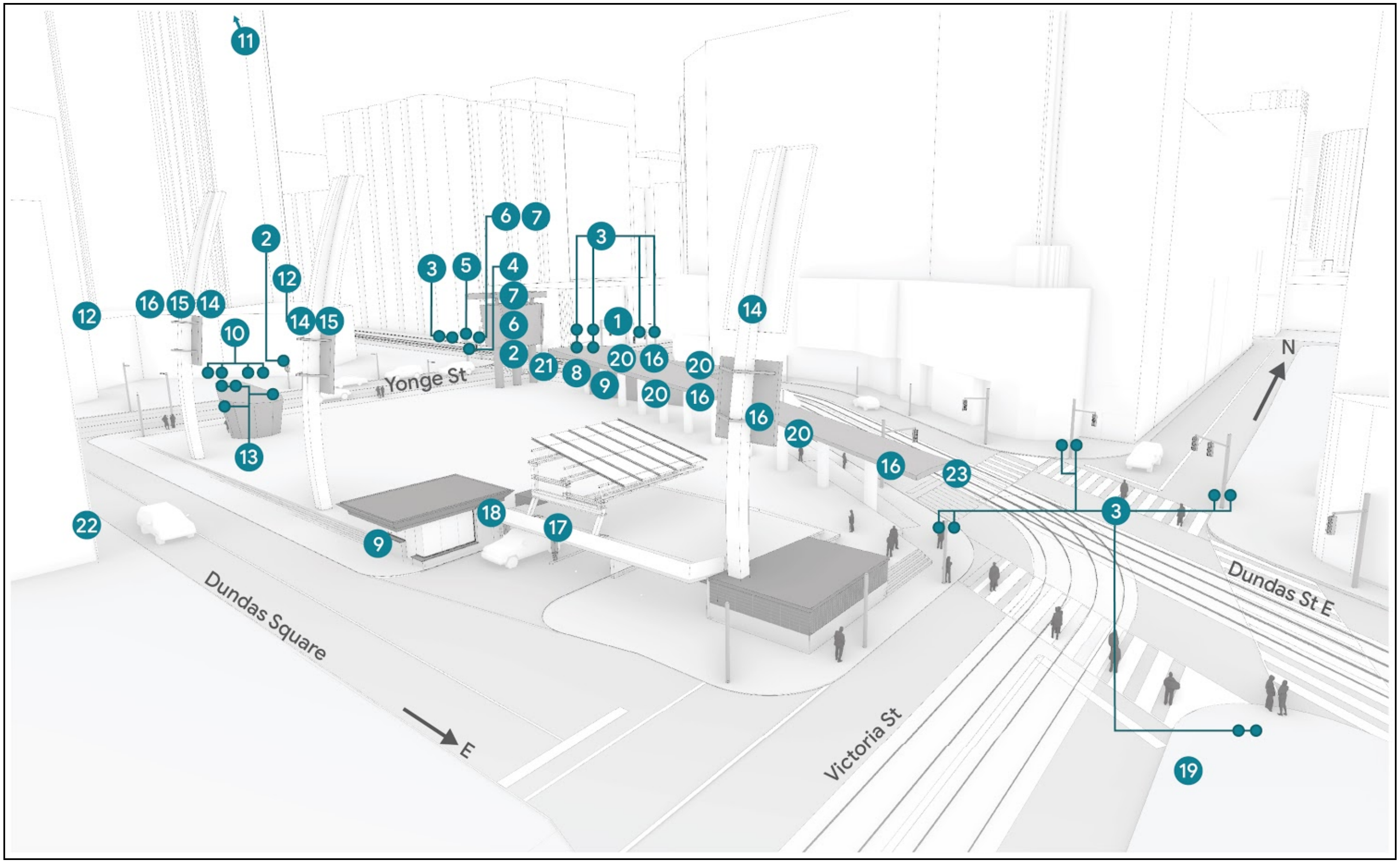


Table: Description of Existing Technologies (and related signage) in the Public Realm at Yonge-Dundas Square in Downtown Toronto

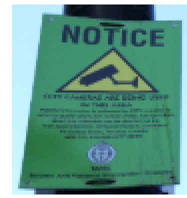
	Item	Description	Item photo	DTPR Purpose
1	Police CCTV notice	Public notice of police CCTV (Closed Circuit TV). A self-contained surveillance system comprising cameras, recorders, and displays for monitoring activities.		N/A
2	Light sensor on sign	Light sensor that is able to distinguish headlights from cars.		Unknown
3	Push button	Push button to request an audible walk signal for traffic lights.		Mobility
4	Transit signal priority receiver	Equipment that gives priority to busses and streetcars, allowing them to communicate with street lights.		Mobility

Table: Description of Existing Technologies (and related signage) in the Public Realm at Yonge-Dundas Square in Downtown Toronto

	Item	Description	Item photo	DTPR Purpose
5	Pole mounted Camera	Communication camera: network cameras use pan, tilt, and zoom to provide both wide-area coverage and detail with a single camera.		Unknown
6	Police camera	Communication camera: network cameras use pan, tilt, and zoom to provide both wide-area coverage and detail with a single camera.		Safety & Security
7	Pole mounted camera	Unknown camera type mounted to underside of black box.		Unknown
8	Box on planter	Function unknown.		Unknown

Table: Description of Existing Technologies (and related signage) in the Public Realm at Yonge-Dundas Square in Downtown Toronto

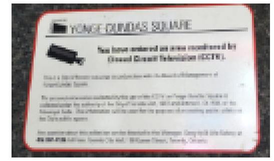
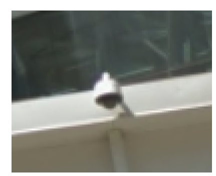
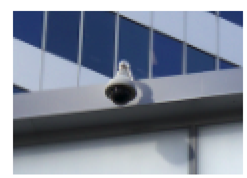
	Item	Description	Item photo	DTPR Purpose
9	Notice	Public notice of CCTV (Closed Circuit TV). A self-contained surveillance system comprising cameras, recorders, and displays for monitoring activities.		N/A
10	Notice	Notice on mall entrance doors.		N/A
11	Weather station	Ultrasonic Anemometer Measures three dimensional wind velocity and speed of sound based on the transit time of ultrasonic acoustic signals. Sonic temperature is derived from speed of sound which is corrected for crosswind effects.		Ecology
12	Camera	Communication camera: Fixed dome cameras are compact cameras with a dome casing. Private camera often used by malls, shops, or building managers.	 	Unknown

Table: Description of Existing Technologies (and related signage) in the Public Realm at Yonge-Dundas Square in Downtown Toronto

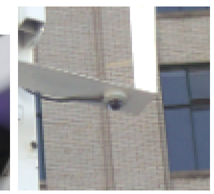
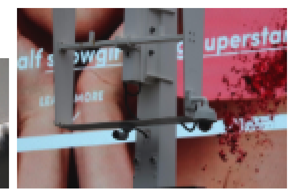
	Item	Description	Item photo	DTPR Purpose
13	4 cameras on information booth	Communication camera: Fixed dome cameras are compact cameras with a dome casing. Private camera often used by malls, shops, or building managers.		Unknown
14	Camera mounted on white sign	Communication camera - fixed dome.	 	Unknown
15	Camera mounted on white signs	Communication cameras mounted on white signs.	 	Unknown
16	Wi-fi Router mounted on multiple structures	Wi-fi Router.		Connectivity
17	Camera on parking garage entrance	Communication camera: Fixed dome cameras are compact cameras with a dome casing. Private camera often used by malls, shops, or building managers.		Unknown

Table: Description of Existing Technologies (and related signage) in the Public Realm at Yonge-Dundas Square in Downtown Toronto

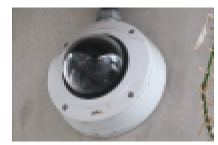
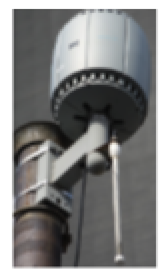
	Item	Description	Item photo	DTPR Purpose
18	Box / equipment on garage	Function unknown.		Unknown
19	DAS Antennas	A distributed antenna system, or DAS, is a network of spatially separated antenna nodes connected to a common source via a transport medium that provides wireless service within a geographic area or structure.		Connectivity
20	Cameras, mounted under the shelter	Communication camera: Fixed dome cameras are compact cameras with a dome casing. Private camera often used by malls, shops, or building managers.		Unknown
21	Cellular base station omnidirectional antenna and signal repeater	Cellular omnidirectional base station antennas consist of a linear array, encapsulated in a heavy-duty fibreglass radome with a thick-walled aluminum mounting base.		Connectivity

Table: Description of Existing Technologies (and related signage) in the Public Realm at Yonge-Dundas Square in Downtown Toronto

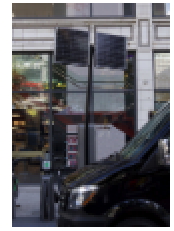
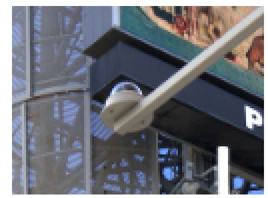
	Item	Description	Item photo	DTPR Purpose
22	Solar panels — bike share	Solar panels for bike share station energy provision.		Energy Efficiency
23	Camera attached to shelter structure facing the street	Communication camera: Fixed dome cameras are compact cameras with a dome casing. Private camera often used by malls, shops, or building managers.		Unknown

Figure: Toronto's King Street West — Existing Technologies (and related signage) on the City Streetscape

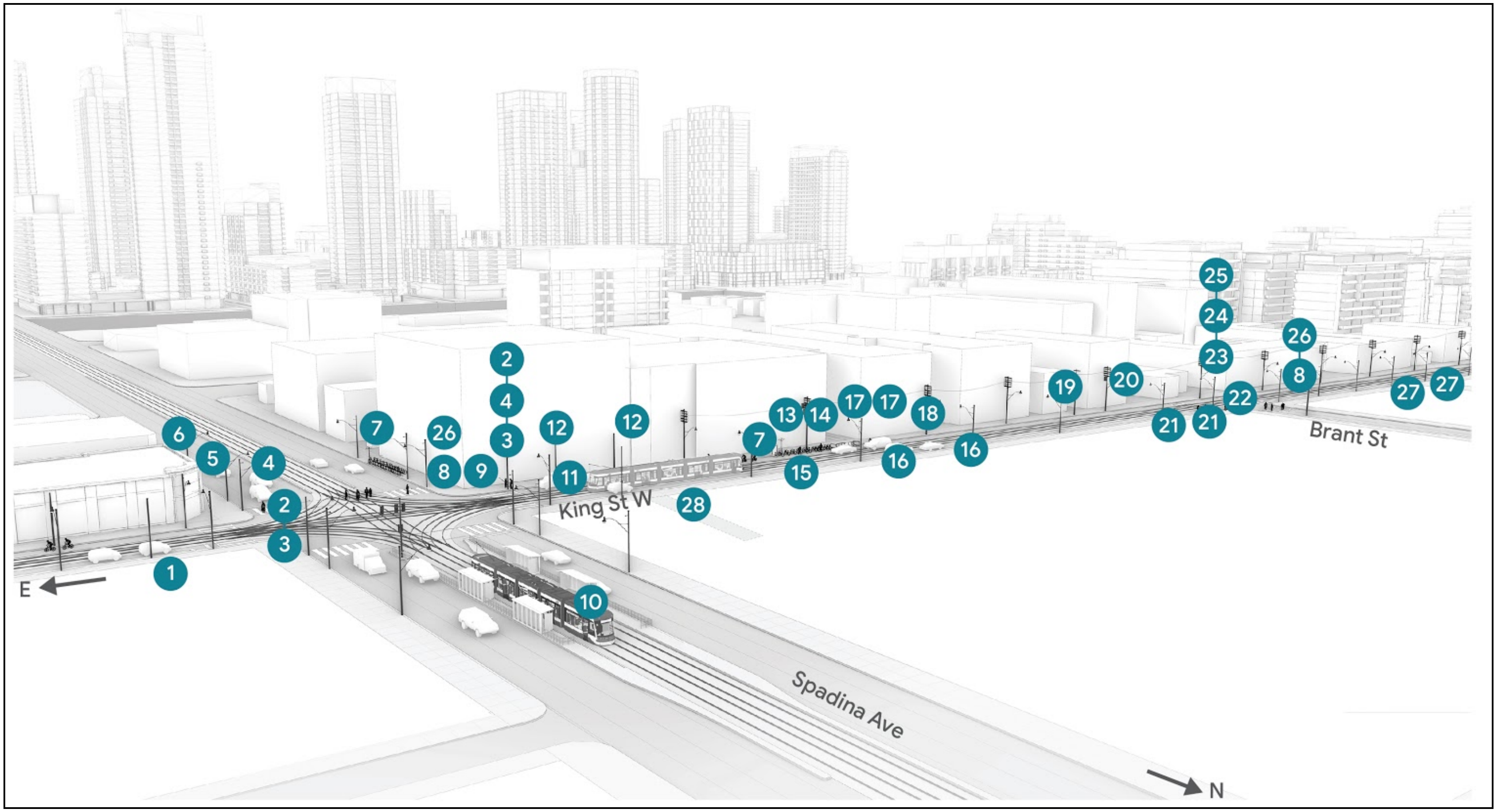


Table: Description of Existing Technologies (and related signage) on the City Streetscape at Toronto's King Street West

	Item	Description	Item photo	DTPR Purpose
1	2 cameras mounted on building fascia	Communications camera. Fixed dome, outdoor camera with infrared for night time view.	 	Unknown
2	360 degree cameras	Communications camera. 360 degree camera. Provides real time and historic video monitoring and traffic counts.	 	Mobility
3	Notice	Notice for video camera usage in posted area.	 	N/A

Table: Description of Existing Technologies (and related signage) on the City Streetscape at Toronto’s King Street West

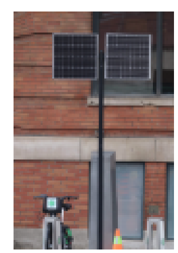
	Item	**Description**	**Item photo**	**DTPR Purpose**
4	Camera	Communication camera: Fixed dome cameras are compact cameras with a dome casing.	 	Unknown
5	Traffic camera #1	Specific function unknown. Likely either a speed control or red light camera. Located adjacent to the below traffic camera.		Mobility
6	Traffic camera #2	Specific function unknown. Likely either a speed control or red light camera.		Mobility
7	Solar panels — bike share	Solar panels for bike share station energy provision.		Energy Efficiency

Table: Description of Existing Technologies (and related signage) on the City Streetscape at Toronto's King Street West

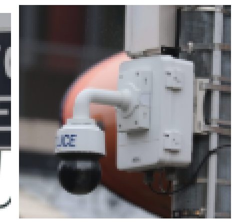
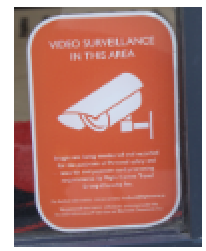
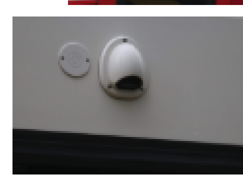
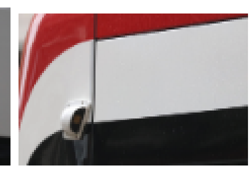
	Item	**Description**	**Item photo**	**DTPR Purpose**
8	Police camera	Communication camera: network cameras use pan, tilt, and zoom to provide both wide-area coverage and detail with a single camera.	 	Safety & Security
9	Private notice	Notice for video camera usage in posted area.		N/A
10	Video cameras on LRT door	In one car of the new LRT fleet, one security cameras on LRT front door and five other cameras on sidewalk-side exterior. Video notice sign. Eight cameras in the interior of the streetcar.	  	Mobility Safety & Security

Table: Description of Existing Technologies (and related signage) on the City Streetscape at Toronto’s King Street West

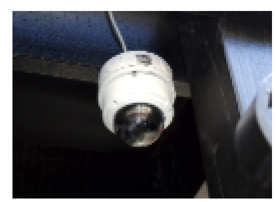
	Item	Description	Item photo	DTPR Purpose
11	Traffic camera	A vehicle presence sensor that combines a camera and a video detector in a single unit. The unit detects moving and stationary vehicles at intersections with traffic signals. Using detection outputs or IP protocol, vehicle presence information is sent to a traffic controller so that signal timing can be adjusted dynamically. Vehicle waiting time at traffic lights is reduced and traffic flows are optimized.		Mobility
12	2 Cameras mounted on building	Communication camera: Fixed dome cameras are compact cameras with a dome casing.	 	Unknown
13	Camera	Communication camera: Fixed dome cameras are compact cameras with a dome casing.		Unknown
14	Camera	Communication camera: Fixed dome cameras are compact cameras with a dome casing.		Unknown

Table: Description of Existing Technologies (and related signage) on the City Streetscape at Toronto’s King Street West

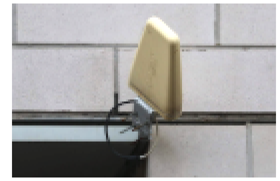
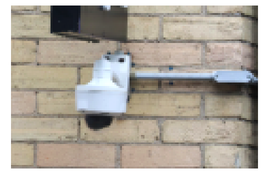
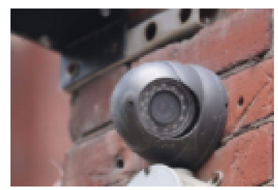
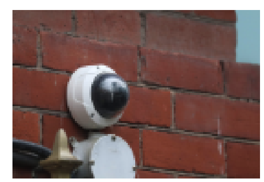
	Item	Description	Item photo	DTPR Purpose
15	Outdoor directional cell signal antenna	Cell phone signal booster for outdoor use.		Connectivity
16	2 Cameras mounted on building	Communication camera: Fixed dome cameras are compact cameras with a dome casing.	 	Unknown
17	2 Cameras mounted on building	Communication camera with night time capability.	 	Unknown
18	Camera mounted on building	Communication camera, fixed dome, with night time capability.		Unknown
19	Camera mounted on building	Communication camera: Fixed dome cameras are compact cameras with a dome casing.		Unknown

Table: Description of Existing Technologies (and related signage) on the City Streetscape at Toronto's King Street West

	Item	Description	Item photo	DTPR Purpose
20	White box	Likely a junction box for either power, phone, or coaxial cable for cable / internet.		Connectivity
21	2 Cameras mounted on building entrance	Communication camera, fixed dome, with night time capability.		Unknown
22	Camera mounted on building	Communication camera: Fixed dome cameras are compact cameras with a dome casing.		Unknown

Table: Description of Existing Technologies (and related signage) on the City Streetscape at Toronto's King Street West

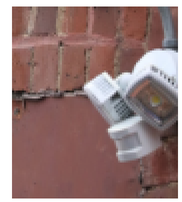
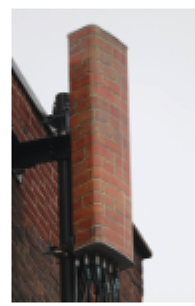
	Item	**Description**	**Item photo**	**DTPR Purpose**
23	Camera mounted on building	Heavy-duty communications camera.		Unknown
24	Motion sensor mounted on building	Motion sensor connected to light and likely to camera listed above.		Unknown
25	Microwave antenna	Microwave antenna covered in a brick wallpaper.		Unknown

Table: Description of Existing Technologies (and related signage) on the City Streetscape at Toronto's King Street West

	Item	**Description**	**Item photo**	**DTPR Purpose**
26	Cellular base station omnidirectional antenna and signal repeater	Cellular omnidirectional base station antennas consist of a linear array, encapsulated in a heavy-duty fibreglass radome with a thick-walled aluminum mounting base.		Connectivity
27	2 Cameras mounted on building	Communication camera with night time capability.	 	Unknown
28	Dish equipment	Unknown directional antenna type, mounted to exterior of building.		Unknown

Figure: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 1

Fire Alarm, Safety, Security, Plumbing, Elevator and Ground Floor Systems

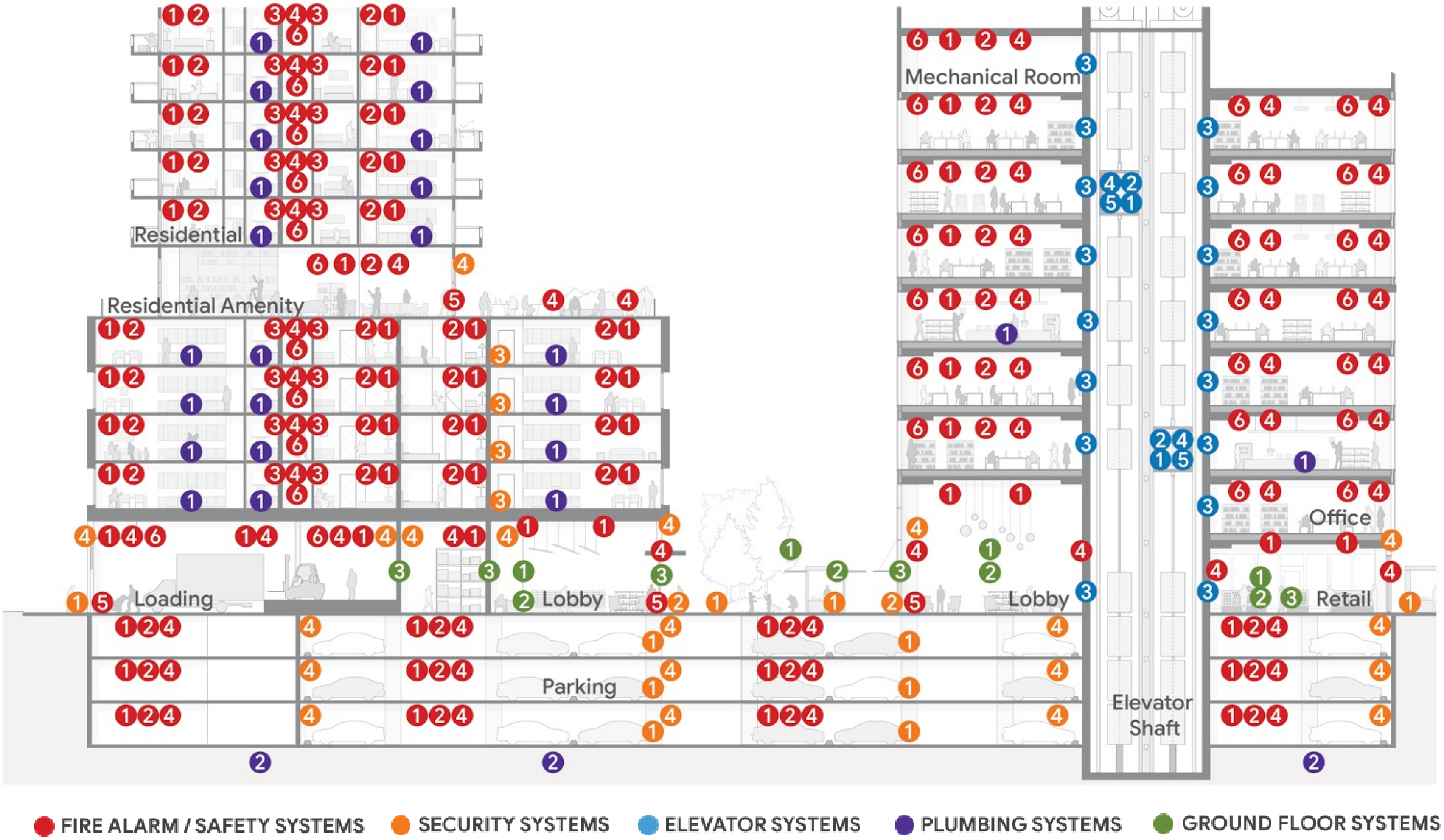


Table: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 1

Subsystem	No.	Component	Function and Types of Sensors	DTPR Purpose Icon
Fire Alarm, Safety, Security, Plumbing, Elevator and Ground Floor Systems				
Fire Alarm / Safety	1	Smoke Detector	Photoelectric or Ionization sensor, not camera, linked to the fire alarm system.	Fire & Emergency
	2	Carbon Monoxide Detector	A sensor that samples air to compute the concentration of carbon monoxide gas, linked to the fire alarm system. Three possible types: **Biomimetic sensor:** a gel changes colour when it absorbs carbon monoxide, and this colour change triggers the alarm. **Metal oxide semiconductor:** When the silica chip's circuitry detects carbon monoxide, it lowers the electrical resistance, and this change triggers the alarm. **Electrochemical sensor:** Electrodes immersed in a chemical solution sense changes in electrical currents when they come into contact with carbon monoxide, and this change triggers the alarm.	Fire & Emergency
	3	Smoke Damper	Same as a smoke detector, but located in an air duct to automatically close to prevent smoke circulation. Linked to the fire alarm system.	Fire & Emergency
	4	Fire Alarm Strobe	Strobe light triggered by fire alarm system to signal an evacuation.	Fire & Emergency
	5	Door Position	Magnetic contact closure switch connected to an alarm system that alerts when a door is open or closed.	Fire & Emergency

Table: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 1

Subsystem	No.	Component	Function and Types of Sensors	DTPR Purpose Icon
	6	Motion	Passive Infrared sensoR (PIR) motion sensor typically connected to an alarm system or to actuate a mechanical device (such as an automatic sink).	Fire & Emergency
Security Systems	1	Duress Alarm (D)	A panic button linked to the life safety system that automatically summons emergency services.	Fire & Emergency Safety & Security
	2	Door Position (dp)	Magnetic contact closure switch connected to an alarm system that alerts when a door is open or closed.	Fire & Emergency Safety & Security
	3	Door Access (DA)	An access control sensor that can read RFID badges, or similar devices, that are linked to the access control system to automatically unlock doors.	Fire & Emergency Safety & Security Entry
	4	Cameras (C)	Video cameras that record to either an on-premise digital video recorder or a cloud based digital video recorder. Typically integrated with the building security system.	Fire & Emergency

Table: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 1

Subsystem	**No.**	**Component**	**Function and Types of Sensors**	**DTPR Purpose Icon**
				Safety & Security
Elevator Systems	1	Cab Position	Typically a magnetic sensor that allows for counting of what floor the elevator is on.	Fire & Emergency
	2	Cab Velocity	Typically a hall sensor that computes how fast the elevator is moving by watching cable travel.	Fire & Emergency Safety & Security
	3	Cab Call Signals	A button that signals the elevator a passenger is waiting.	Fire & Emergency Safety & Security
	4	Cab Occupancy	Typically a weight sensor on the elevator cab cable that approximates number of people.	Fire & Emergency
	5	Cab Duress Alarm	A button in the elevator that signals an alarm system, typically linked to life safety systems.	Fire & Emergency Safety & Security

Table: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 1

Subsystem	No.	Component	Function and Types of Sensors	DTPR Purpose Icon
Plumbing Systems	1	Hot / Cold Water	Boilers and chillers that are controlled by the BMS system to decide when they should be heating or cooling liquid.	Water Efficiency
	2	Ejector / Sump Pump	Pump that is triggered by a liquid level sensor that automatically activates to pump fluid out of drains or other basins.	Water Efficiency
Ground Floor Systems	1	Mobile (Wi-Fi, beacons, location services)	A variety of tools (Wi-Fi, beacons, location services) that interact with mobile devices provide de-identified movement information within a ground floor environment.	Planning & Decision-making
	2	Camera (embedded within digital display)	A camera which captures the pedestrian footfall past an advertising display.	Planning & Decision-making
	3	Footfall sensors: infrared, lidar, thermal	An infrared sensor that tracks the volume of pedestrian footfall past a threshold or a given catchment area.	Planning & Decision-making

Figure: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 2
Power Infrastructure, Lighting Controls, Heating Ventilation Air-conditioning (HVAC) Systems

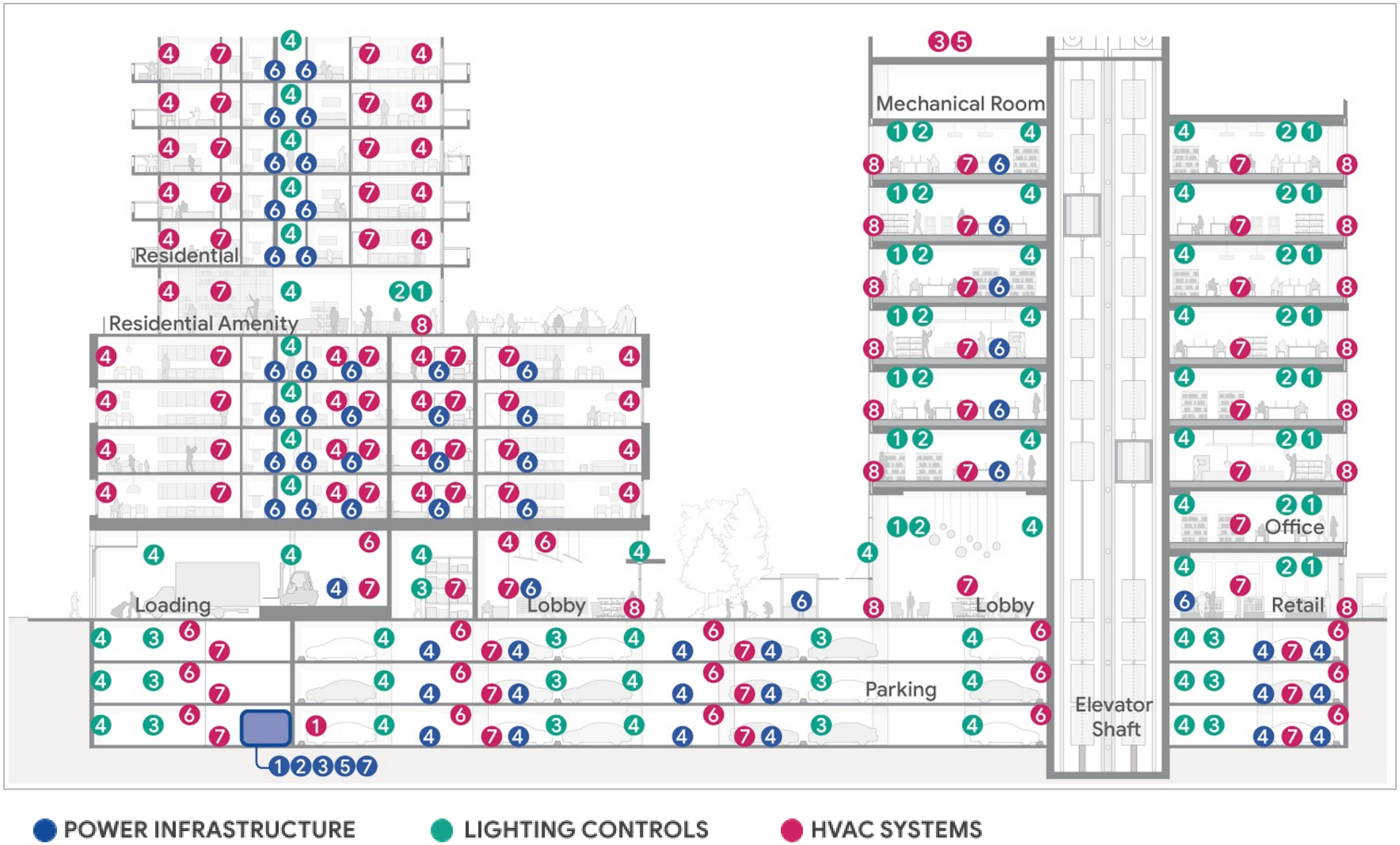


Table: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 2

Subsystem	No.	Component	Function and Types of Sensors	DTPR Purpose Icon
Power Infrastructure, Lighting Controls, Heating Ventilation Air-conditioning (HVAC) Systems				
Power Infra-Structure	1	Voltage	Electrical energy sensor used to calculate energy use.	Planning & Decision-making Energy Efficiency
	2	Current	Electrical energy sensor used to calculate energy use.	Planning & Decision-making Energy Efficiency
	3	Temperature	Temperature sensors on wires to ensure that wires are not overheating.	Energy Efficiency
	4	Plug Load	Electrical outlets that have devices plugged into them within a space, distinct from items that are hard-wired, permanently, connected to electricity.	Energy Efficiency
	5	Emergency Generator	A generator, typically gas powered, that delivers electricity in the event of a power failure. Automatically activated during utility power loss.	Fire & Emergency

Table: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 2

Subsystem	No.	Component	Function and Types of Sensors	DTPR Purpose Icon
	6	Sub Meter	An electric meter that measures a smaller space. In a building there can be a master meter that records total energy use for the building, and then sub-meters for each individual unit within the building.	Energy Efficiency
	7	Switch Gear (SG)	Mechanical switches that control the source of power and distribution. Typically automated so that in a power failure the power source is switched from the local utility to the emergency generator.	Switch
Lighting Controls	1	Daylight	A light level sensor that integrates with lighting systems, and window treatment systems, to allow for automatic dimming of lights, raising/lowering of shades.	Energy Efficiency
	2	Dimming	A light switch with dimming capabilities.	Energy Efficiency Switch
	3	Occupancy / Vacancy	Typically a motion sensor connected to the lighting and BMS systems to signal when a space is empty so that its systems can be put into a low power mode, or so they can be woken up when a space is occupied and turned on.	Energy Efficiency

Table: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 2

Subsystem	No.	Component	Function and Types of Sensors	DTPR Purpose Icon
	4	Emergency Lighting	Battery backed up light fixtures that automatically activate in the event of power failures.	Fire & Emergency
HVAC Systems	1	Pump	A mechanical device that distributes water for heating or cooling. Uses temperature sensors, pressure sensors, leak sensors and automated control sequences from the BMS.	Energy Efficiency
	2	BTU Meter	A thermal energy meter that measures the energy transfer across a point in the HVAC system. Uses temperature and flow sensors.	Energy Efficiency
	3	Chiller	A large refrigeration device that cools liquid, often to provide cooling to a building or process. Automated chiller control sequences in the BMS use temperature sensors, outdoor air temperature sensors, pressure sensors, data from Air Handling Units and Fan Coils and space temperatures and other data points..	Energy Efficiency
	4	Air Handling	A collection of fans, filters and air coils that change the temperature and humidity of air to maintain desirable conditions in a building. Air Handling control sequences in the BMS use space temperature sensors, pressure sensors, thermal energy metering and data from other HVAC equipment and the fire alarm system.	Energy Efficiency
	5	Controller	A digital component of the BMS system that gathers data from various sensors and controls HVAC mechanical systems appropriately. May use space temperature, outside air temperature, leak sensors, thermal energy metering data.	Energy Efficiency
	6	Fan Coil	A smaller piece of equipment for moving air and heating or cooling for space conditioning. Uses space temperature sensors, thermal energy metering,and automated control sequences from the BMS.	Energy Efficiency

Table: Toronto Buildings — Existing Technologies in Modern Mixed-Use Buildings in Toronto Today — 2

Subsystem	No.	Component	Function and Types of Sensors	DTPR Purpose Icon
	7	Thermostat	A space temperature sensor which reports this data to the central BMS system, a BMS controller, or a local piece of HVAC equipment.	Energy Efficiency
	8	Baseboard Heat	A heating element installed in a baseboard, controlled by the BMS system or a local space temperature sensor in the space.	Energy Efficiency

2.2.2 Sidewalk Labs' approach to responsible data use — informed by and building on best practices

2.2.2.1 Responsible Data Use Guidelines — what they are, and the best practices they were inspired by

Sidewalk Labs has created a set of Responsible Data Use Guidelines to address data ethics, access to information, and the ways that aggregate or de-identified data can impact individuals and groups of people through the use of advanced analytics such as artificial intelligence. This is in addition to the areas covered by standard tools such as a Privacy Impact Assessment.

Background on the development of the Guidelines
To help develop the Guidelines, and to receive guidance on a full range of issues relating to responsible data use, Sidewalk Labs convened a Data Governance Advisory Working Group made up of independent experts and community representatives. Sidewalk Labs' early work with these advisors, together with feedback gathered as part of the Quayside public engagement process, led to the development of an initial set of draft principles.

Sidewalk Labs was also influenced by "Privacy by Design,"a world-renowned approach to privacy, which outlines principles that should be included from the outset of any data-collecting activity, product creation, or service provision in all its aspects. Sidewalk Labs incorporated Privacy by Design elements in the Responsible Data Use Guidelines, which emphasize privacy and data ethics right from the beginning of creating a product or conceptualizing a service. The Guidelines further evolved based on consultation with experts and community feedback.

In the draft MIDP, Sidewalk Labs proposed that a government-sanctioned "Urban Data Trust" would be in the best position to create a set of Responsible Data Use Guidelines that would establish a clear, common standard for Responsible Data Use. Sidewalk Labs provided its Responsible Data Use Guidelines, used internally for pilots and projects, as an example for consideration.

Further to feedback on the data governance aspects of the proposal, Sidewalk Labs and Waterfront Toronto have agreed not to pursue establishing the Urban Data Trust as a new entity for this project, recognizing that the underlying objectives of ensuring responsible data use and supporting trusted data sharing can be achieved through supporting the strength of existing government bodies. This includes building on Waterfront Toronto's existing Draft Digital Principles to develop a set of "Intelligent Community Guidelines" that will apply to private companies deploying digitally enabled solutions in the designated waterfront area. Based on the above, Sidewalk Labs has updated its draft Responsible Data Use Guidelines.

The Guidelines
Sidewalk Labs' Responsible Data Use Guidelines apply to all data activities by Sidewalk Labs. This current set of six guidelines is used internally for assessing proposed pilots and

projects that involve data. Through the use of a Responsible Data Use Assessment tool, these Guidelines shape the design and implementation of products and pilots.

1. Beneficial purpose

All proposed uses of data must incorporate Canadian values of diversity, inclusion, and privacy as a fundamental human right. To meet this standard, there must be a clear purpose and value to any proposed use of data, as well as a clear, direct connection to the ways in which the project and proposed data-collection activity would benefit individuals or the community. A proposal or project should not be collecting data for the sake of having data.

2. Transparency and clarity

Individuals should be informed about how and why data is collected and used in a way that is proactive, clear, and easy to understand.

3. Data minimization, security, and de-identification by default

Only the minimum amount of data needed to achieve the beneficial purpose should be collected and the least invasive technology available to achieve the beneficial purpose should be used. By default, the most up-to-date de-identification techniques to reduce the amount of personal information collected should be used.

4. Publicly accessible by default

Whenever possible, properly de-identified or non-personal data should be made publicly accessible to third parties by default, formatted according to open standards. Sidewalk Labs believes that preserving individual privacy, while also enabling data and source code to be accessible by others to catalyze innovation, is the preferred approach.

5. No selling Personal Information or use for advertising

Sidewalk Labs has already committed publicly that it would not sell personal information to third parties or use it for advertising purposes. It also commits to not share personal information with third parties, including other Alphabet companies, without explicit consent.

6. Responsible AI principles required

To ensure that issues around the use of artificial intelligence systems are being considered and addressed by data collectors and developers, Sidewalk Labs has developed Responsible AI principles and is working to incorporate these principles into its development and decision-making to promote the spread of responsible technology and data use.

2.2.2.2 What is a Responsible Data Use Assessment, and how does it relate to the Responsible Data Use Guidelines?

Implementing the Guidelines through the Responsible Data Use Assessment

Corporate data governance is crucial to ensuring privacy and ethics by design. Organizational accountability is at the core of PIPEDA. The Office of the Privacy Commissioner of Canada

(OPC) states that "[a]n accountable organization must have in place appropriate policies and procedures that promote good practices, which, taken as a whole, constitute a privacy management program."[3] All organizations within Canada must implement a privacy management program, but beyond OPC guidance and best practices, there is no one standard for privacy impact assessments. Furthermore, advanced analytical systems such as machine learning require that ethical considerations be built into the design process and into the data processing architecture.

The Organisation for Economic Co-operation and Development (OECD) recommends that organizations take into account "the social and economic objectives they are pursuing. Like all forms of risk, privacy risk should not be assessed in isolation but rather in relation to the potential benefits."[4] The OECD also notes that uncertainties cannot be eliminated completely and some degree of risk has to be accepted. An acceptable level of risk is achieved by assessing the objectives and the benefits in a common reference framework. According to the OECD, the components of this framework include:

- "Establishing the objectives and the context of an activity and determining the acceptable level of risk in light of the expected benefits;"
- "Assessing risk by identifying risk factors and evaluating the likelihood and severity of risk occurrence;"
- "Treating risk, including through accepting some, reducing it to an acceptable level through appropriate measures, sharing or transferring some, or avoiding some altogether;"
- "Monitoring and reviewing on an ongoing basis the risk management cycle to adapt it to a constantly changing environment."[5]

Sidewalk Labs' RDUA includes four primary components

Purpose: The first section of the Responsible Data Use Assessment (RDUA) asks for a description of the purpose of the project, service, or product, including its objectives and goals, as well as the urban challenges it hopes to address. Examples of questions asked in this part of the RDUA include:

- Why are you collecting (or using or sharing) data?
- What is the beneficial purpose?
- What is the problem to be solved, and why will this technology solve the problem or achieve the objective(s)?

---

[3] The Office of the Privacy Commissioner of Canada, "Getting Accountability Right with a Privacy Management Program," April 2012, The Office of the Privacy Commissioner of Canada and provincial commissioners in Alberta and British Columbia adopted accountability guidance in 2012 based on the Organisation for Economic Co-operation and Development's accountability principle.

[4] Working Party on Security and Privacy in the Digital Economy, "Managing Digital Security and Privacy Risk," Organisation for Economic Co-operation and Development, June 1, 2016.

[5] Organisation for Economic Co-operation and Development's, *Going Digital: Shaping Policies, Improving Lives*, Chapter 7: Strengthening Trust, March 11, 2019.

- What are the alternatives to the proposed solution? Why will they not suffice?

Data sources: The second section of the RDUA requires a description of the technology or data collection methods, the data sources or types, and the parties who have access to the data. This section also requires a data flow diagram. Some of the questions asked in this section include:

- What are all the sources of the data, internal and external?
- Does the data activity involve personal information?

Legal compliance and data ethics: The third section of the RDUA captures conformance to applicable privacy laws and also asks questions about all data, not just personal information. Examples of questions asked in this section include:

- Personal Information: How did the individual consent to giving you their Personal Information or to the collection of their PI?
- All data: How is information about the purpose of collection and use of data being communicated to the users (for example, via a help page or as part of the process of obtaining consent)?
- Could the anticipated use of the data or technology harm, result in unforeseen consequences, or benefit certain individuals, groups of people, or communities to the detriment of others in unintended or unexpected ways? Please explain your response.
- Could it result in an individual or group being treated differently than others, such as to determine eligibility for a service or benefit? Please explain your response.
- Would anyone be surprised that this data is being collected or used in this way? Please explain your response.

Risk-benefit analysis. The fourth section of the RDUA asks the proposing entity to detail and rate the risks and benefits associated with the project and data collection activity, and how any risks have been mitigated. Example questions include:

- Consider the above-mentioned risks and mitigations with your overall objectives and stated beneficial purpose...
    - What is the anticipated impact of the benefit?
    - How likely is it to occur?

2.2.2.3 Sidewalk Labs' Responsible Data Use Assessments (RDUAs) build on an existing tool known as Privacy Impact Assessments

Sidewalk Labs has been asked how the RDUA compares to existing privacy assessment tools, such as the Privacy Impact Assessment (PIA). The section below describes what a PIA is and how the RDUA builds on this.

An overview of Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are a tool typically used by governments to identify and potentially mitigate the potential privacy risks of programs or services that will involve the handling of personal information. PIAs involve a detailed review and analysis, and are documented in a report.

A PIA is part of a process to identify and address privacy risks when a process or program that collects, uses, discloses, or retains personal information is being implemented or is substantially changed. PIAs are used to ensure that decision-makers understand the privacy implications of their decisions. PIAs are also a way to ensure that privacy legislation and standards are complied with and that public policy issues are identified in advance of any major decisions.

PIAs involve various steps, including:

- Identifying all of the personal information related to a particular program or service;
- Identifying how that personal information will be handled — usually this is supplemented by a data-flow diagram that depicts the flow of personal information across the program or activity (such as how it is collected, how it is stored, who accesses it, how it is transferred or disclosed);
- Identifying the authority for each collection, use, and disclosure of personal information;
- Assessing the need for each collection, use, and disclosure of that personal information;
- Assessing whether the need and benefit is proportional to the potential invasion of privacy;
- Applying and considering the privacy principles noted above;
- Identifying privacy risks and the likelihood and severity of those risks; and
- Identifying any mitigation measures that could reduce or remove those risks.

At the federal level, government policies require public sector institutions to conduct PIAs for new or redesigned programs and services involving personal information.[6] Similarly, at the provincial and municipal level, government institutions routinely conduct PIAs, either as a matter of policy or best practice. For the private sector, an organization is free to voluntarily adopt its own policy regarding formal privacy assessments, but there is no overarching requirement to do so.

The following chart summarizes the respective PIA-related requirements for public sector and private sector organizations.

[6] PIAs are required in certain circumstances under Ontario's health privacy legislation. That legislation applies to health care providers and their handling of personal health information.

Table: Summary of PIA-Related Requirements for Public Sector and Private Sector Organizations for the Collection and Use of Personal Information

Type of Entity	**Entity Example**	**Legal Framework**	**Regulator**	**Assessment Required**	**Assessment Reviewed by Regulator**	**Public Input Required**	**Publication Required**
Public sector: Canada	Environment Canada	Privacy Act; Treasury Board of Canada Directive on Privacy Impact Assessment	Privacy Commissioner of Canada	By government policy	By government policy	Not required	By government policy
Public sector: Ontario	Ministry of Infrastructure, Metrolinx	Freedom of Information and Protection of Privacy Act	Information and Privacy Commissioner of Ontario	By government policy	Not required	Not required	Not required
Public sector: Toronto	Toronto Transit Commission, Toronto Hydro	Municipal Freedom of Information and Protection of Privacy Act	Information and Privacy Commissioner of Ontario	By government policy	Not required	Not required	Not required
Private sector: commercial activity	Sidewalk Labs	Personal Information Protection and Electronic Documents Act	Privacy Commissioner of Canada	Not required	Not required	Not required	Not required

Sidewalk Labs' RDUA builds on the Privacy Impact Assessment to consider all types of data and data ethics

Sidewalk Labs currently triggers an RDUA process for its data collection activities, even if they do not include personal information. Sidewalk Labs' RDUAs serve the same overarching purpose (identifying and mitigating privacy concerns) as PIAs and are similar in that they involve detailed reviews and analyses, and are documented in a report.

However, as illustrated in the table below, Sidewalk Labs' RDUAs have a broader scope than PIAs, both in terms of the data under consideration but also of the implications of the collection, use, and sharing of that data beyond traditional privacy concerns. In this way, Sidewalk Labs' RDUA ensures compliance with privacy laws while also including features that make for a more comprehensive assessment beyond the existing legal requirements.

Sidewalk Labs' privacy and data governance team was inspired by existing PIAs and Data Protection Impact Assessments (DPIAs), a tool that organizations under the General Data Protection Regulation (GDPR) use to analyze, identify, and minimize privacy and data protection risks.[7] Similar to how the DPIA or the PIA supports an organization's compliance with the GDPR by enforcing data protection by design and default, Sidewalk Labs uses its RDUA to ensure legal compliance for its products and services, and the incorporation of privacy and data ethics by design.

Sidewalk Labs worked with the Information Accountability Foundation to develop a version of a data assessment tool that includes all relevant privacy obligations arising from the applicable laws and regulations, and also goes beyond them to consider the beneficial uses, the risks, and questions about data ethics. This resulted in the creation of the Responsible Data Use Assessment (RDUA) tool.

[7] "What Is a DPIA?," Information Commissioner's Office, accessed September 25, 2019.

Table: Comparison of Privacy Impact Assessments and Sidewalk Labs' Responsible Data Use Assessment

Topic	**Topic Description**	**PIA**	**RDUA**	**RDUA Section**
Project overview	A general description of the project under assessment.	Yes	Yes	1
Participants	A description of relevant participants in the assessment.	Yes	Yes	1
Stakeholders	A description of relevant stakeholders or partners in the project.	Yes	Yes	1
Purpose	A discussion of the purpose of the project, including what problems it will solve and what benefits it will provide.	Yes	Yes	2
Authority or applicable law	An assessment of the authority of the organization to handle personal information under the privacy law applicable to the project.	Yes	Yes	6
Data-flow diagram and description	A data-flow diagram, which depicts each point of collection, use, retention, transfer, and disclosure of personal information. These diagrams show how personal information and other data move between different activities or participants in the project. A description usually accompanies these diagrams, providing additional context for what is happening at each stage, including who might have access at that stage, special safeguards particular to that stage, and so on.	Yes	Yes	3

Topic	Topic Description	PIA	RDUA	RDUA Section
Data analysis: 10 privacy principles	An analysis of each step in the data-flow diagram, and of the project generally, in light of the 10 privacy principles set out in the Canadian Standards Association's Model Code for the Protection of Personal Information.[8] This code was enacted into law as part of PIPEDA, but it is also applied in public sector privacy assessments. In brief, it assesses: 1. Accountability: that the project is governed by policies and practices that ensure compliance with these principles. 2. Identifying purposes: that the organization will identify the purposes for collecting personal information to individuals at or before the time of collection. 3. Consent: that individuals will have knowledge of and give meaningful consent to the collection, use, or disclosure of personal information (except where otherwise permitted by law); that purposes will be explained in such a way that the individual will reasonably understand the use and disclosure of their personal information; that individuals will be able to withdraw consent, as appropriate. 4. Limiting collection: that personal information will only be collected to the extent necessary for the identified purposes. 5. Limiting use, disclosure, and retention: that personal information will only be used, disclosed, and retained to the extent necessary for the identified purposes (except where otherwise required by law); that personal information will be securely destroyed when no longer needed.	Yes	Yes	3, 4

[8] *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, ed. Dwayne Mathers (Etobicoke, Ontario: Canadian Standards Association, March 1996).

Data analysis: 10 privacy principles (cont'd)	6. Accuracy: that personal information will be accurate, complete, and up-to-date as necessary for the identified purposes. 7. Safeguards: that appropriate security safeguards will protect the personal information, including the location where the data is stored or from where it is accessed. 8. Openness: that individuals will be able to readily access information about privacy policies and practices related to the project. 9. Individual access: if the project will involve exceptions to the organization's normal procedures for access and correction requests by individuals regarding their personal information as part of the project. 10. Challenging compliance: if the project will involve exceptions to the organization's normal procedures under which individuals can challenge the organization's compliance with the above principles.			
Responsible AI	Unlike a typical PIA, an RDUA requires an organization to consider how analytics-driven models or insights, or algorithmic decision-making, is being used. It also requires the impact to individuals and groups be assessed.	No	Yes	4
Service providers	A consideration of the role of service providers, including whether contracts with those service providers contain appropriate privacy provisions.	Yes	Yes	4
Privacy risks and risk mitigation	An assessment of privacy compliance risks, including risks of harm to individuals, as well as risk-mitigation measures to address those risks.	Yes	Yes	4, 5

Topic	Topic Description	PIA	RDUA	RDUA Section
Data ethics risks and risk mitigation	In addition to privacy compliance risks, an RDUA involves additional assessment of potential harm or unforeseen consequences to groups or communities, including differential treatment. An RDUA also includes a specific assessment of the risk that data being collected (or inferences made using that data) could relate to any category of discrimination under the Human Rights Act or other human rights or anti-discrimination laws. An RDUA requires a discussion of possible risk-mitigation measures to address these data ethics risks.	No	Yes	4, 5

Sidewalk Labs applies its RDUA to more types of data

PIAs assess the collection, use, and disclosure of *personal information*. Per public sector and Privacy Commissioner guidance,[9] PIAs focus on the privacy of individuals — and do not require consideration of impacts to groups or to society arising out of the use of data.

The protection of privacy of individuals is a natural focus for PIAs, since they arise from privacy laws. However, Sidewalk Labs sees the importance of taking a broader view, because the collection and use of de-identified information and aggregate information can impact groups of people and communities. Accordingly, Sidewalk Labs currently triggers an RDUA process for its data collection activities, even if they do not include personal information.

Moreover, the RDUA requires additional considerations beyond those typically found in PIAs, such as:

- Whether collected data (or inferences made using that data) could relate to categories of discrimination or otherwise include biases;
- How the data activity might result in potential harms or unforeseen consequences for groups or communities, including differential treatment; and
- How individuals or groups of people might be impacted by the use of any algorithmic decision-making included in the data activity.

Sidewalk Labs proactively publishes summaries of RDUAs

Public sector PIA frameworks do not always require that summaries of PIAs be made publicly available. Only the federal government requires summary information about PIAs to be published.[10]

To increase accountability and enhance transparency, Sidewalk Labs currently publishes online summary RDUAs for product and pilot launches.[11] For example, one of these pilots further demonstrates Sidewalk Labs' commitment to radical transparency: the Digital Transparency in the Public Realm co-design project.[12]

[9] The Office of the Privacy Commissioner of Canada and the Information and Privacy Commissioner of Ontario have each developed guidance documents for how to conduct PIAs. See Office of the Privacy Commissioner of Canada, "Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada,"; and Information and Privacy Commissioner of Ontario, "Planning for Success: Privacy Impact Assessment Guide," 2015.

[10] The Treasury Board of Canada's "Directive on Privacy Impact Assessment" requires federal institutions to make a PIA summary available to the public. The summary must include a description of the program or activity, the legal authority for the program or activity, and a completed high-level risks questionnaire. See Treasury Board of Canada, "Directive," Government of Canada (website), April 2010,

[11] For the list of summary RDUAs see Sidewalk Toronto website, Documents, and filter by "Summary RDUAs".

[12] See section 2.3.2.4 for further details.

This ensures that the public can access information about the analysis conducted for a given activity, while also balancing the fact that some information included in a full RDUA cannot be made public due to legal privilege or business sensitivity.

2.2.3 Putting Responsible Data Use Guidelines into Practice

2.2.3.1 Responsible Data Use is interwoven in Sidewalk Labs' processes for design and development of inclusive and complete communities

Sidewalk Labs' responsible data use processes
The RDUA is not purely a compliance exercise with applicable laws. Sidewalk Labs believes that responsible data use and being accountable requires going beyond the letter of the law. This means considering the spirit of the law, data ethics, and human rights. Responsible data use also does not sit solely within the legal department — the RDUA is used throughout Sidewalk Labs' digital planning processes, to help teams consider privacy and ethics throughout their work, from vendor selection to product design to implementation/launch. Building this internal capacity and set of organizational reflexes to ensure privacy and data ethics by design is an ongoing process.

Sidewalk Labs uses the "three lines of defense" model for data governance. The "first line" consists of the business teams, who are accountable for the decisions made based on the RDUA, and the heads of product and of legal. Members of the privacy and data governance team also regularly attend meetings of the various business teams, which provides an early opportunity to flag potential privacy or data ethics concerns. The "second line" is the privacy and data governance team, which leads the privacy and data ethics reviews, establishes policies and guidance, provides privacy training, and serves as a first point of contact for all privacy and technology ethics matters. The "third line" is Sidewalk Labs' engagement with external stakeholders, experts, and consultants. For example, the RDUA was created through consultations with experts, such as the Information Accountability Foundation. Members of the privacy and data Governance team met also with experts at the University of Ottawa's Canadian Internet Policy and Public Interest Clinic and the Centre for Law, Technology and Society to get feedback on the RDUA and Sidewalk Labs' data governance process.

As discussed above, the RDUA implements Sidewalk Labs' Responsible Data Use Guidelines and ensures compliance with applicable privacy laws. The RDUA is a living document that lives alongside the product or pilot. The RDUA process is triggered for pilots or projects that involve data activity, including those that do not involve personal information. In practice, this means that the RDUA could be triggered at different stages of a project, depending on the product or pilot. The RDUA could be triggered at the vendor selection and contracting phase, at the idea stage in a meeting, or, for existing pilots, when there is a change in the scope of a pilot and a new RDUA is initiated or the existing RDUA is updated.

RDUAs may become dormant, but they never really "die." This means that the RDUA is continuously updated depending on the circumstances and as the applications and uses of a technology evolve. An example of this at Sidewalk Labs' office in Toronto is the Numina pilot (see the case study for this pilot in section 2.2.3.2). This pilot's RDUA was approved for data collection and use for three sensors placed in specific locations for specific uses. If the team wants to add a sensor, change the location, or change the purpose of collection, the existing RDUA will be updated to reflect these changes and the pilot as a whole is reassessed — to ensure compliance with applicable laws, but also to ensure that there is no tech for tech's sake.

Below is an overview of the typical steps in the RDUA process currently in place at Sidewalk Labs.

Stage 1: A Sidewalk Labs project team comes to the privacy and data governance team with their pilot or product ideas. If this idea includes a data activity — the collection, use, or sharing of data — then the RDUA process is triggered.

Stage 2: An RDUA is started or an existing RDUA is revised. The privacy and data governance team works with the pilot or product manager and engages stakeholders as necessary. The privacy and data ethics risks are assessed and mitigated.

Stage 3: The final section of the RDUA requires completing a summary of the main privacy and data ethics risks, the mitigation efforts and how these efforts minimize risk as much as possible, and why the beneficial purpose merits an approval of the data activity.

Stage 4: After the RDUA is complete, and if the data activity is approved, the final stage involves ongoing monitoring of the pilot or product and ongoing privacy compliance. This includes ensuring data is secure and protected from breaches and any changes in scope are recorded in a revised RDUA.

As mentioned above, Sidewalk Labs is committed to a robust responsible data use process and the process continues to evolve. Accountability is the foundation of PIPEDA, and Sidewalk Labs considers responsible data use to be an essential part of its culture and will continue to consciously weave it into Sidewalk Labs' practices.

2.2.3.2 Demonstration of the RDUA in practice

Case Study of the RDUA in practice: driving vendor selection for a public realm sensing pilot at 307

Sidewalk Labs' vision for people-centred mobility — safer and more efficient public spaces — requires a deep understanding of how people, bikes, and vehicles move through space relative to each other, as well as to events and changes that occur in the public realm. This pilot allows Sidewalk Labs to test privacy preserving technology in a small scale manner so that Sidewalk Labs can understand how this type of technology can scale to future mobility systems, and to a broader neighbourhood and public space. In the short term, this pilot will allow Sidewalk Labs to gather engagement data on exhibits and installations at Sidewalk Labs' Toronto location ("307"), which includes measuring how people interact with the outdoor weather mitigation structure (the "building raincoat") and indoor exhibits. The data will help Sidewalk Labs revise its designs to better achieve their respective goals.

Sensors using computer vision are among the most cost-effective means of identifying and understanding these flows, and in early 2018, Sidewalk Labs sought to identify privacy-preserving computer vision technologies to learn more about how they work and test their capabilities to gather insights related to mobility and design of physical spaces.

Because responsible data use is woven into Sidewalk Labs' practices, the Responsible Data Use Guidelines and Assessment process informs its research and exploration of potential technologies to procure and test. The RDUA was then used by Sidewalk Labs to evaluate the solution developed by Numina, a civic tech company, that uses a privacy-by-design approach to measure the flows of people and differentiated transportation modes through streets and open spaces for planners and transportation managers.

Numina is committed to "intelligence without surveillance," and stood out to Sidewalk Labs' team because of their development of on-device de-identification. You can read more about Numina's commitment to privacy by design on their website.

When Sidewalk Labs started initial discussions with Numina, Sidewalk Labs began the process of applying the RDUA immediately. Using the RDUA as a guide, the Sidewalk Labs staff peppered the Numina team with questions about the way their technology works, requested clarifications on their privacy policy, asked for more details on exactly how images are processed and stored, dug into details on the data streams for the operational dashboard versus Numina's QA processes, and ultimately ended up collaboratively creating the data flow diagram in the RDUA below.

The process of completing the RDUA - with team members from Sidewalk Labs' public realm and data governance teams, in addition to members of the Numina team - facilitated discussions about Numina's technology that helped build Sidewalk Labs' confidence in the privacy-centric design of Numina's system. Based on the above, the RDUA was approved and the pilot could proceed. This case study is an example of how the RDUA process drives Sidewalk Labs' decisions on the technology used and the vendors selected. The RDUA was approved for data collection and use for three sensors placed in specific locations around 307 (see section 2.2.3.2 for more details).

If the Sidewalk Labs team wants to add a sensor, change the location, or change the purpose of collection, the existing RDUA will be updated to reflect these changes and the pilot will be reassessed — not just to ensure compliance with applicable laws, but also to ensure that technology decisions in the public realm are thoughtfully considered before implementation.

In order to demonstrate how the RDUA was used to assess the public realm sensing pilot using Numina, a slightly modified version of the full RDUA has been included below. Sidewalk Labs includes this as a demonstration of its commitment to transparency. For additional information on how this template works in practice within Sidewalk Labs, please see section 2.2.3.2. Note that some details in the RDUA have been removed or brought to a more abstract level in order to preserve legal privilege and business information which could be sensitive in nature.

Figure: Digital Transparency in the Public Realm Signs Provide Information on the Numina Installation at Sidewalk Labs' 307 Lakeshore Blvd. East Office

Sample Completed RDUA for Public Realm Sensing (Numina)

1. Project Overview and Document Details	
Provide an overview and description of your proposed data activity. You should include key team members that will know all of the relevant details for this data activity.	
Project Name	Public Realm Sensing — Numina computer vision pilot
Overview of the product/pilot	Sidewalk Labs' vision for people-centred mobility — safer and more efficient public spaces — requires a deep understanding of how people, bikes, and other vehicles move through space relative to each other, as well as in response to other events and changes that occur in the public realm. Sensors using computer vision are among the most cost-effective means of identifying and understanding these flows, and Sidewalk Labs seeks to identify and test privacy-preserving technologies that strive to achieve this. Sidewalk Labs has chosen to test a solution by Numina because of Numina's development of on-device de-identification and its focus on preserving privacy. The Numina sensors process image data in real time to generate de-identified vehicle and pedestrian movement and count data through the sensors' field of view. The images are not stored in persistent memory except for occasional Quality Assurance (QA) images (i.e. they are deleted after processing). The de-identified QA images are described further in the sections that follow. Sidewalk Labs is piloting this technology (referred throughout as the "pilot") at Sidewalk Labs' Toronto headquarters at 307 Lakeshore Boulevard East ("307"), to understand flows of people throughout the space and aggregate statistics about time spent looking at exhibits, including outdoor weather mitigation structures, flexible structures, flexible pavers, and indoor exhibits. The data will help Sidewalk Labs iterate on its designs to better achieve their respective goals.

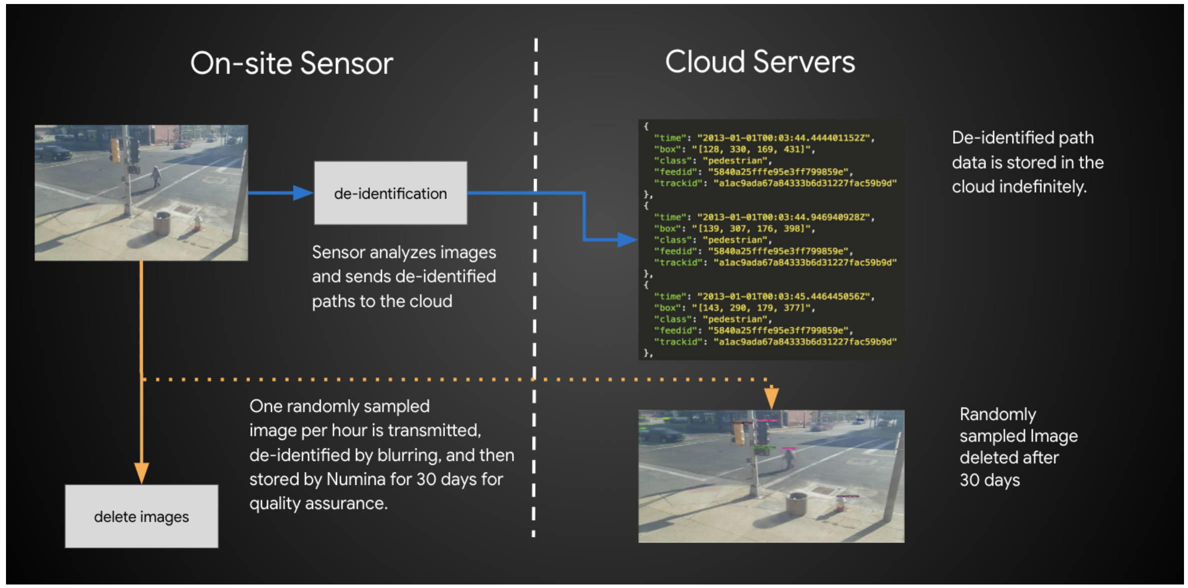
Overview of the product/pilot (Cont'd)	Cameras with on-device processing and de-identification can be among the most versatile, privacy-preserving, and cost-effective options for measuring mobility flows and the use of space. Upon scanning the market for solutions of this sort, Numina demonstrated deep consideration of the risks surrounding storage of personal information and mitigated those risks extensively by developing best practices for privacy preservation when handling visual data, which satisfied Sidewalk Labs' requirements for total de-identification and security. The pilot will allow Sidewalk Labs to test privacy-preserving computer vision technology on a small scale, at the 307 office, to understand whether this is the type of technology that can or should scale to a future mobility system and to larger scale public locations — all in furtherance of the purposes set out below (see Part 2. Beneficial Purpose).
RDUA Lead	**[Name removed]**
Project Manager **Team Members** ● Technical lead (app, website) ● External partners → Technical → Contractual	**[Names removed]**
Privacy/Data Gov Reviewers	**[Names removed]**
Product Legal Counsel Lead	**[Names removed]**

(Product Manager) RDUA Details	
RDUA creation date Anticipated Pilot/Project launch deadline Actual Pilot/Project launch date	December 1, 2018 March 2019 March 2019
RDUA Summary publication date and link	Public Realm Sensing Summary RDUA March 2019
Next anticipated review/update of this document	The next review of the RDUA is if and when the contract with the vendor is extended, or if and when there are material changes in the scope of the original data activity. Material changes include adding another sensor or substantively changing the field of view.
Is this RDUA for a new or existing data activity? If this is for an existing data activity, please also reference and link to the previous RDUA.	New data activity.
Links to relevant documents	**[Links to internal docs removed]** Contract with Numina Data flow documents Call and meeting notes with Numina

2. Initial Assessment	
Explain why you want to collect, use, or share data and why you believe that will achieve the stated beneficial purpose.	
Beneficial Purpose Why are you collecting (or using or sharing) data? What is the beneficial purpose?	Automated sensing in the public realm is essential to the Master Innovation and Development Plan ("MIDP") vision for Sidewalk Toronto's people-centred mobility system and public realm. Sensors with on-device de-identification are among the most versatile, privacy-preserving, and cost-effective options available to gather the data needed to achieve safer streets and better public spaces. Sensing of objects and activity in the public realm has a number of applications referenced in the MIDP, including: ● People-first mobility systems that start with knowing and understanding how our streets and public realm are used by people, bikes, and other vehicles, to improve safety and increase efficiency. ● Understanding how people use parks, plazas, and neighbourhood spaces enables students, researchers, communities, and governments alike to understand the impact of design and programming on public life. ● Data-driven planning for spaces, buildings, and programs. ● Traffic safety operation and evaluation. ● Maintenance of infrastructure and spaces.
What is the problem to be solved and why will this technology solve the problem or achieve the objective(s)? What are the alternatives to the proposed solution? Why will those not suffice?	Cities and private companies often require data about how public or semi-public spaces are used in order to plan programming, maintenance scheduling, and to assess for the safety of streets and sidewalks. However, traditional cameras that collect and record personally identifiable details about people can present legal and other challenges — notably, the potential for issues related to privacy. This pilot aims to solve the problem about access to reliable data while preserving the privacy and anonymity of people.

What is the problem to be solved and why will this technology solve the problem or achieve the objective(s)? (Cont'd) What are the alternatives to the proposed solution? Why will those not suffice? (Cont'd)	This pilot involves the collection of data to help assess the effectiveness of exhibits and installations at Sidewalk Labs' 307 office and workspace, including outdoor weather mitigation structures, flexible pavers, and indoor exhibits. The data will benefit Sidewalk Labs and project partners and stakeholders by helping measure how people are engaging with the exhibits at 307, which will help to revise Sidewalk Labs' designs to better achieve their respective goals. Other methods of measuring engagement include CommonSpace (a map-based data collection mobile application that makes it easier to record observations of activities in open spaces) and infrared motion sensors. Sidewalk Labs decided to not use CommonSpace for this purpose because it would require one or two dedicated personnel to gather this information over extended periods, which is not feasible for such a prolonged period of measurement. Infrared motion sensors can provide information on how many people are in a space and where they are going in a general sense. However, to effectively measure engagement with the exhibits and installation, it is helpful to know the paths of where people are going in the exhibit spaces. Additional goals of this pilot include: ● Collect data about a well-understood place using sensors and computer vision, in order to better understand the quality and reliability of the data. ● Allow Sidewalk Labs to gain familiarity with Numina's technology for future public realm sensing projects to, among other things, ensure the technology provides sufficient privacy protections. ● Develop a repeatable process for working with third-party computer vision vendors. ● Demonstrate and explain how Sidewalk Labs will apply the Responsible Data Use Guidelines to computer vision technology, and to gather user feedback from stakeholders including regulators, advisors, and members of the public.

Who are the internal (Sidewalk Labs) stakeholders? Who are the external stakeholders?	**Internal Stakeholders:** Sidewalk Labs Public Realm and Mobility teams - This pilot will help team members assess the accuracy, usefulness, and privacy-preserving features of this technology to achieve their goals, some of which depend upon having up-to-date, accurate data on how the spaces are being used. **External Stakeholders:** Privacy regulators - This pilot offers an opportunity to demonstrate the application of privacy laws to sensor-based data collection of de-identified data in a controlled environment. Numina - The company (which provides the sensor) is interested in ensuring that their product and technology meets the highest bar for privacy protection while providing consistent, accurate data derived from the sensors. Numina sensors have been deployed in 15 cities in three countries to date, and Sidewalk Labs' 307 site is one of Numina's first private-property deployments.

3. Understanding the Technology and the Data Sources	
A Data Flow Diagram and Data Table can be considered as part of the review process.	
Data Flow Diagram (link or paste in)	[Note: provided here is a high-level data flow diagram only] 

Data Table

<table>
<tr><th>Collection Source</th><th>Use(s)</th><th>Data Category</th></tr>
<tr><td>Sensor Data: Numina Device</td><td>Vehicle and pedestrian movement and count data
This data will be used to:
Assess the effectiveness of exhibits and installations at Sidewalk Labs’ 307 office and workspace, including outdoor weather mitigation structures, flexible pavers, and indoor exhibits.
Better understand the quality and reliability of the data.
Allow Sidewalk Labs to gain familiarity with Numina's technology for future public realm sensing projects to, among other things, ensure the technology provides sufficient privacy protections.
Understand whether this is the type of technology that can or should scale to a future mobility system and to the public realm, and whether the technology and data can be applied to certain applications set out in the MIDP, for example:
Understanding how our streets and public realm are used by people, bikes, and vehicles to improve safety and increase efficiency.
Understanding how people use parks, plazas, and neighbourhood spaces enables students, researchers, communities, and governments alike to understand the impact of design and programming on public life.
Data-driven planning for spaces, buildings, and programs</td><td>Vehicle and pedestrian movement and count data

De-identified Personal Information:
The Numina sensor’s cameras process images that are de-identified in real time. The sensors use cameras to capture data about movement in an area, but immediately process it on-device into a sequence of time stamped two-dimensional coordinates linked by an arbitrary path id number and a “class,” which specifies if the moving object is a person, bicycle, car, truck, or bus. The points are only connected into a path while the subject is in the camera’s field of view. The image data is processed in real time and is not stored in persistent memory (for example, the image data is deleted after processing, at the device level), except for Quality Assurance (QA) images, as noted below. The path data may be further refined into counts of people, vehicles, bicycles.

De-identified Personal Information from or about children under the age of 13:
The devices use real time de-identification, and so no Personal Information of children is transmitted by the devices, or retained or used by Numina or Sidewalk Labs (with the exception of any QA images that may depict children).</td></tr>
</table>

Sensor Data: Numina Device (Cont'd)		• In any case, Sidewalk Labs does not anticipate unaccompanied children to be present at 307. Signs are posted at the pilot site that are readily visible to adults or older children that would accompany younger children. Those signs explain the pilot, the technology being used, and the data being collected.
Sensor Data: Numina Device	**Quality Assurance (QA) images:** Numina uses the QA images for validating and training algorithms that help generate the vehicle and pedestrian movement and count data.	**QA images - De-identified Personal Information:** • A limited number of randomly sampled (one per hour), low-resolution images are transmitted to Numina and stored for 30 days by Numina for quality assurance (over 4G/LTE network, using encryption). These QA images are de-identified on Numina's servers before they are stored and before they are accessible by Numina personnel, and are only accessible by Numina agents in a secure environment. The QA images are encrypted in transit to the server where they are de-identified. • The Numina sensors will be placed such that only the 307 premises are within the field of view of the sensors. Streets, sidewalks, and entrances to buildings other than 307 will not be within the field of view of the Numina sensor.
Sensor Data: Numina Device	**Analysis and insights derived from vehicle and pedestrian movement and count data:** Same uses as vehicle and pedestrian movement and count data.	**Analysis and insights derived from vehicle and pedestrian movement and count data — Aggregate information about people:** Data from the sensors will be aggregated and used to develop analysis and insights.

4. Privacy and Data Governance	
Section 4.1 is required for projects that include the collection, use, or disclosure of *Personal Information* (as defined in PIPEDA). Check with Legal to confirm whether your data activity involves Personal Information.	
4.1 (General) Privacy and Data Governance	
Notice and Consent Personal Information: How did the individual consent to giving you their Personal Information or to the collection of their Personal Information? All data: How is information about the purpose of collection and use of data being communicated to the users (for example, via a help page or as part of the process of obtaining consent)?	**De-identified Personal Information — Communication of purpose or collection and use / Implied Consent**: The pilot at 307 will be accompanied by signage on-site notifying visitors of the data collection activity and the use of the sensors, outside the boundary of and before the visitor enters the sensor's field of view. The pilot will also be accompanied by an exhibit that will explain how privacy protection is inherent in the design of the technology and illustrate the use cases to which the data is being applied at 307, as well as potential for application at wider scales. 307 facilitators will receive training that would allow them to answer any questions that might arise. To the extent that real time de-identification is considered to be the collection or use of Personal Information, Sidewalk Labs has posted signs at the pilot site which will serve as notice for the purposes of obtaining implied consent when a visitor continues onto the pilot site.
Individual Access and Control How can users access, edit, or delete the Personal Information they have provided to you, or that has been collected, and how can they do this?	**Not applicable**: The pilot does not retain any Personal Information as all data is de-identified on-device or, with respect to the QA images, de-identified before it is stored or made available to Numina personnel.

Individual Access and Control (Cont'd) Can individuals access their data in a structured, commonly used and machine-readable format so they can transfer those data to another organization? Please explain or describe.	**Not applicable**: The pilot does not retain any Personal Information as all data is de-identified on-device or, with respect to the QA images, de-identified before it is stored or made available to Numina personnel.
Deletion Does deleting the app or service, or withdrawing from the pilot or service, delete the individual's Personal Information or is that an extra step? Describe the process and who the individual must contact to do so.	**Not applicable:** The pilot does not retain any Personal Information.
Secondary Purposes Will the collected Personal Information be used in ways other than to meet the beneficial purpose? If so, please explain your response. How can users withdraw their consent to, or delete, secondary or tertiary uses of the data?	**Not applicable**: There are no secondary purposes with respect to the data collected in this pilot.
Location of Data Where is Sidewalk Labs data stored? If applicable, list the service provider/vendor. If stored in Canada, can data be accessed from locations outside of Canada? If Personal Information is stored outside of Canada, what is the justification for storing data outside of Canada?	The vendor (Numina) will store pilot data (the vehicle and pedestrian movement and count data, the aggregate statistics and insights derived from such data, and de-identified QA images) in the United States. For redundancy reasons, the vendor stores data outside of Canada because Amazon Web Services ("AWS") has only one Canadian region. Using this region exclusively would leave the service vulnerable to outages at a single geographic region and put the pilot at risk of data loss or service outages. The risk of harm from this data is low since there is not a serious possibility of data about persons visiting 307 being rendered identifiable after it is de-identified by Numina.

Data Retention Period How long is the data to be retained? For Personal Information, you should indicate whether the Personal Information will be converted to de-identified form, and then retained as de-identified data.	Numina will retain vehicle and pedestrian movement and count data. Numina will retain de-identified QA images and securely destroy them after 30 days. Sidewalk Labs will retain pilot de-identified data for five years to fulfill the purposes of the pilot.
Destruction and Deletion After you no longer need the data, how will the data be deleted, destroyed, or made anonymous?	Numina will securely delete data from AWS. Sidewalk Labs will securely delete the de-identified data.
Accuracy How are you ensuring that data is kept accurate, complete, and up-to-date to meet the purposes for which it was collected?	The accuracy of the data is assessed on a regular QA basis by Numina as part of its services, and more closely scrutinized during the initial set-up and calibration period. Numina validates the vehicle and pedestrian movement and count data using the low-resolution QA images. The use case for the 307 pilot is the detection of pedestrians moving through the 307 space. Accuracy in detecting pedestrians and movement paths in this use case is unlikely to significantly impact individuals and groups as the data will be used to better understand how visitors to 307 interact with exhibits and prototypes and will only impact those who continue to visit 307. Accuracy in the classification of objects passing through the view of the sensor (for example, misclassifying cyclists as motorcyclists) could affect groups differently, but would not affect this pilot. If the purpose of this pilot changes, the accuracy of the data and the classification model, as assessed in the duration of this pilot, would be re-considered in a new RDUA.

Publicly Available Sidewalk Labs has committed that data that is not Personal Information or otherwise sensitive will be "publicly accessible by default." Does this data activity result in data that would be publicly accessible? If so, which data? If not, why?	Yes. This data activity may result in open data as Sidewalk Labs will retain all rights to the vehicle and pedestrian movement and count data generated by this project. Sidewalk Labs plans to make it publicly available in some format.
Responsible AI (1) How are analytical driven models or insights, or algorithmic decision-making being used? (2) How could individuals or groups of people be impacted by this use?	(1) Numina uses detection, classification, and tracking algorithms to derive the vehicle and pedestrian movement and tracking data. Numina uses low-resolution, de-identified QA images for validating and training algorithms. All generated insights will have significant review by human experts before being applied to any future designs. (2) As noted above, accuracy in the classification of objects passing through the view of the Numina sensor (for example, misclassifying cyclists as motorcyclists) could affect groups differently, but would not affect this pilot. Should the scope of this pilot change or these sensors be used in public spaces, this consideration will be reassessed.

4.1.2 (Legal) Privacy and Data Governance	
Consent — Collection, use, and disclosure of Personal Information (Canada) To the extent that Personal Information is collected, please describe how you are ensuring full compliance with the Office of the Privacy Commissioner's Meaningful Consent Guidelines? See Guidance for checklist for meaningful consent.	The pilot location (Sidewalk Labs' private office in Toronto) will be accompanied by signage on-site notifying visitors of the data collection activity and the use of the sensors, outside the boundary of and before the visitor enters the sensor's field of view. The pilot will also be accompanied by an exhibit that will explain how privacy protection is inherent in the design of the technology and illustrate the use cases to which the data is being applied at 307, as well as potential for application at wider scales. 307 facilitators will receive training that would allow them to answer any questions that might arise.

Consent — Collection, use, and disclosure of Personal Information (Canada) (Cont'd) To the extent that Personal Information is collected, please describe how you are ensuring full compliance with the Office of the Privacy Commissioner's Meaningful Consent Guidelines? See Guidance for checklist for meaningful consent. How can individuals revoke consent? What impact will withdrawing consent have on the individual?	The above information posted at the pilot site will serve as notice for the purposes of obtaining implied consent when a visitor continues onto the pilot site. The notices emphasize the key elements of the pilot technology and data and are provided at the time a visitor would be entering the pilot area (i.e. they are just in time notices). Individuals cannot revoke consent because the sensors de-identify images in real time. Even QA images are de-identified after transmission to Numina and before being stored on Numina's servers, and so are not capable of being acted upon if an individual sought to withdraw his or her consent. Individuals who do not consent to the collection of this sensor data have the option of not visiting 307 and are given notice that this technology is in use before they enter into the sensors' field of view.
What are the secondary purposes for the collection, use, or sharing of data, if any? If applicable, how did you obtain consent for secondary purposes (such as purposes other than providing the pilot or services)?	**Not applicable:** There are no secondary purposes with respect to the pilot.
Data Transfers (transfers to service providers for processing) How will third parties with whom data is transferred for processing be bound to follow relevant privacy and data security requirements?	Numina is collecting the vehicle and pedestrian movement and count data on behalf of Sidewalk Labs. Numina is subject to the following terms in its agreement with Sidewalk Labs: ● Numina shall comply with Canadian law, including applicable data protection laws, and with Sidewalk Labs' Responsible Data Use Framework, in the collection, processing, and storage of the data; ● Numina shall advise Sidewalk Labs of the name of the subcontractors/agents who will be involved in any aspect of the services, and notify Sidewalk Labs of any party changes.

Data Transfers (transfers to service providers for processing) (Cont'd) How will third parties with whom data is transferred for processing be bound to follow relevant privacy and data security requirements?	• Numina is obligated by contract to only use the data to fulfill the services for Sidewalk Labs and for quality assurance purposes. Numina shall not share any Personal Information or random still images with any third party and no effort shall be made or directed to be taken to identify such images. • Numina will securely destroy vehicle and pedestrian movement and count data after a reasonable period. In addition, in describing its security practices in the agreement, Numina represents that its hardware and software are hardened by minimizing attack surfaces, that it uses strong encryption in communications between Numina endpoints, and that its systems undergo periodic security reviews and are updated with the latest patches.
Data Disclosures (sharing with third parties) Is Personal Information or other data being shared with third parties? How is consent being obtained? For what purpose(s) is Personal Information being shared? For what purpose(s) will the receiving third party use the shared Personal Information?	**Not Applicable:** No Personal Information is disclosed in connection with the pilot.
Custody Who has custody of the data? Is the data being collected by a third party or vendor for Sidewalk Labs? If so, please explain your response.	Numina will have custody of the pilot data as it collects and processes data from the Numina sensor on Sidewalk Labs' behalf. Sidewalk Labs will store pilot data (excluding QA images) received from Numina on Google Cloud. As such, Google will have custody of pilot data and will store it on Sidewalk Labs' behalf.

Control Who has control over the data? ● Contractual ● Technical Is the data being collected by a third party or vendor for Sidewalk Labs? If so, please explain your response.	Sidewalk Labs has contractual control over the data, through its contract with Numina and its contract with Google (for data storage). Sidewalk Labs has technical control over the data that is stored on Google Cloud. Numina has technical control over the data that it collects on behalf of Sidewalk Labs via Numina sensors. Numina is contractually limited to using the pilot data solely for the purposes of internal product improvement.
Selling and Advertising Sidewalk Labs has committed publicly that it would not sell Personal Information to third parties or use it for advertising purposes. It also commits to not share Personal Information with third parties, including other Alphabet companies, without explicit consent. Confirm that your data activity conforms to this commitment.	**Not applicable**: No Personal Information is shared in the course of the pilot. Furthermore, pilot data will not be used for advertising purposes.
Relevant legal documents 1. Contracts	1. Numina (Pilot Agreement) - [**Confidential - link removed**]

4.2. Risks and Data Ethics	
Identify other risks, and concerns in respect of data ethics	
Is any of the data sensitive? Please explain your response. What kinds of biases might exist in the data? Please explain your response.	**Sensitive Data:** We do not believe pilot data to be sensitive, as it is de-identified on-device in real time. The pilot data represents vehicle and pedestrian movements and counts at the time it was collected and does not incorporate historical data. Pedestrian movements at 307 do not involve sensitive data elements (for example, movements do not reveal sensitive information about individuals). **Potential Biases in Data:** The data does not include individual or group characteristics, thus we believe there is a low risk of bias in this data. The pilot data is collected by processing images captured by the sensors into de-identified movement and count data while the images are still on the device in real time. The originally sensed images are then destroyed. A calibration period for the installed sensors helps to ensure the accuracy of the data.
Could the anticipated use of the data or technology harm, result in unforeseen consequences, or benefit certain individuals, groups of people, or communities to the detriment of others in unintended or unexpected ways? Could it result in an individual or group being treated differently than others, such as to determine eligibility for a service or benefit? Would anyone be surprised that this data is being collected or used in this way? Please explain your response.	The sensors are deployed at 307 in areas (inside and outside) to capture a wide variety of groups of people, not in places meant to single any one group out. The data is de-identified and it is not used to make decisions based on individual or group characteristics. It is used to make decisions about configuring publicly accessible spaces based on observed overall patterns of use. At the 307 pilot scale, the temporal and spatial bounds of the data collection limits the potential risks to individuals, groups, and society. By collecting this data on a pilot basis, Sidewalk Labs and other stakeholders can more concretely understand the nature of the data and its potential uses, and therefore, associated benefits and risks.

Could the anticipated use of the data or technology harm, result in unforeseen consequences, or benefit certain individuals, groups of people, or communities to the detriment of others in unintended or unexpected ways? Could it result in an individual or group being treated differently than others, such as to determine eligibility for a service or benefit? Would anyone be surprised that this data is being collected or used in this way? Please explain your response. (cont'd)	Applied at larger scales, there is a risk that this type of movement and count data can be used to treat locations that vary in scale from a site to a neighbourhood, differently. For example, the data could result in a decision to direct funding to spaces with the highest utilization, instead of trying to understand why some places are poorly utilized and directing funding towards adapting those spaces to community needs. However, these risks can be mitigated by making the data that underlies decision-making publicly accessible and available for all stakeholders to assess and analyze. Further, having comprehensive, objectively measured utilization data is more informative than not having the data, when making the same funding or other investment decisions. In any case, understanding these risks is part of the impetus for the pilot. Another type of risk is that the Numina sensors will fail to de-identify images or that the sensors will otherwise collect and transmit images to Numina or others without authorization. If this occurs, this could result in the collection of Personal Information without the proper consent of individuals, and in some cases could result in harm to individuals. Although the harm would likely be at a low level when deployed during the pilot at 307, it is possible that reputational or other harms could arise if this technology was deployed in more sensitive locations. This risk is inherent to the technology, and mitigation depends on the security and rigor of Numina's technology and practices. Finally, certain groups of individuals may perceive the sensors as ongoing surveillance. This is one reason why Sidewalk Labs is transparent about the purpose for the sensors and the de-identification techniques used. Sidewalk Labs has educated and will continue to educate people through the RDUA, a blog post, exhibits at 307 during the pilot, and relevant signs at the pilot location. Furthermore, Sidewalk Labs will ensure that the signs providing notice provide sufficient detail so that the individual will not consider the data activity to be outside of their reasonable expectations.

Does the data set include any information that relates to categories of information that are "sensitive" or relate to any category by which discrimination is prohibited under the Human Rights Act or other human rights or anti-discrimination laws? Please explain your response. Is there any reasonable likelihood that these categories of information could be inferred from the data set? Please explain your response.	Sidewalk Labs does not believe pilot data to be sensitive, as it is de-identified either: (a) on-device in real time; or, (b) on-server in near-real time. The pilot data represents vehicle and pedestrian movements and counts at the time it was collected and does not incorporate historical data. As the pilot data is not Personal Information and because the data is limited to pedestrian movement and counts at 307, the pilot data does not include any information about prohibited grounds of discrimination with respect to any individual or group. Furthermore, pilot data is not used to make decisions based on individual or group characteristics. Rather, it is used to make decisions about configuring publicly accessible spaces based on observed overall patterns of use. In addition, the Numina sensors are deployed in areas (inside and outside) to capture a wide variety of groups of people, not in places meant to single any one group out.
Consider the risks in this section... How significant are the risks? How likely are they to be realized? Please highlight your answer. Explain your reasoning.	**Significance:** **1 — Low Impact**, 2 — Moderately Low impact, 3 — Moderate impact, 4 — Moderately high Impact, 5 — High impact **Likelihood:** **1 — Low likelihood**; 2 — Moderately Low likelihood; 3 — Medium likelihood; 4 — Moderately High likelihood; 5 — High likelihood The risks relating to pilot data are low impact and low likelihood, since it is de-identified data about pedestrian movement on Sidewalk Labs' premises. The pilot data is not ripe for abuse and the decisions that the data will inform are discrete, namely design decisions about Sidewalk Labs installations and exhibits. Furthermore, as discussed in this section and below, there is substantial risk mitigation inherent in the Numina technology and the design of the pilot. A more significant risk would be the unauthorized use of Numina sensors to remotely collect images that have not been de-identified. That said, the significance of this risk in relation to Numina sensors placed at 307 remains relatively low given the sensors are not in sensitive locations. Also, because of the security measures used by Numina and the limited scale of the pilot, the likelihood of the unauthorized use of Numina sensors to remotely collect images appears low.

4.3 Mitigating Risks	
What are the risks and how are they being mitigated against?	
De-identification If the data is Personal Information, how has it been de-identified? If the data is Personal Information and is not de-identified, what is the beneficial purpose for keeping the data identifiable?	The plans and protocols for this pilot should result in no Personal Information being saved or being seen by humans. First, Numina de-identifies images on-device in real time using the following method: On-board the Numina sensor, the image is processed into a sequence of time stamped two-dimensional coordinates linked by an arbitrary path id number and a "class," which specifies if the moving object is a person, bicycle, car, truck, or bus. Numina's algorithm creates "boxes" around each moving object within the sensor's field of view, classifying into broad categories such as pedestrian, cyclist, and car without tracking any Personal Information. The vast majority of images potentially containing Personal Information are deleted and are not stored on-device or sent to the cloud. One randomly sampled image per hour is transmitted and stored in the cloud by Numina for 30 days for quality assurance (QA) purposes. The QA images are low resolution (less than 1 pixel per cm and of low image quality, JPEG Q=50). To eliminate the possibility that, despite this low resolution, Personal Information remains in the image, Numina applies an object detection and blurring algorithm to remove recognizable features from QA images before they are made available to any Numina agents or employees for validation. Sidewalk Labs never receives any QA images.
How likely is it that de-identified data could be combined with other information to identify individuals? Please highlight your answer. Explain your reasoning.	**Likelihood: 1 — Low likelihood**; 2 — Moderately Low likelihood; 3 — Medium likelihood; 4 — Moderately High likelihood; 5 — High likelihood

How likely is it that de-identified data could be combined with other information to identify individuals? (Cont'd) Please highlight your answer. Explain your reasoning. (Cont'd)	The Numina sensor could conceivably be placed in a location that also captures a doorway or entrance where someone closely associated with that location will be captured entering or leaving the location. While the information obtained by Sidewalk Labs is only a red line indicating the path of a pedestrian or vehicle, it may be possible to identify this individual when this information is used in conjunction with other information that associates the individual with the location. That said, the likelihood of the above is low with respect to the pilot at Sidewalk Labs' offices. In addition, Numina functionality makes it possible to exclude doorways from the spatial analysis on the dashboard. The pilot provides Sidewalk Labs with the opportunity to test this privacy preserving technology before deploying it in spaces where concerns such as the above are possible. This testing is part of the pilot's objective to find technology that allows the collection of important data about public spaces while respecting the privacy of individuals.
Data Minimization Is there a less data intensive way to achieve the goals of the data activity, including potential insights? Please explain your response. How has a less data intensive data activity been developed throughout the RDUA process?	The time-limited nature and small physical scale of this pilot limits the amount of potential harm. For the pilot, the data collected is to help assess the effectiveness of exhibits and installations at Sidewalk Labs' office and workspace, including outdoor weather mitigation structures, flexible pavers, and indoor exhibits. Other methods of measuring engagement include CommonSpace (a map-based data collection mobile application that makes it easier to record observations of human activities in open spaces) and infrared motion sensors. Sidewalk Labs decided to not use CommonSpace for this purpose because it would require one or two dedicated personnel to gather this information and this is not feasible for such a prolonged period of measurement. Infrared motion sensors can provide information on how many people are in a space and where they are going in a general sense. However, to effectively measure engagement, it is helpful to know the paths of where people are going in the exhibit spaces.

Data Minimization (cont'd) Is there a less data intensive way to achieve the goals of the data activity, including potential insights? Please explain your response. How has a less data intensive data activity been developed throughout the RDUA process?	The Numina sensors de-identify any Personal Information on-device when creating the vehicle and pedestrian movement and count data. As set out elsewhere in this RDUA, this data is not Personal Information and it only reveals what Sidewalk Labs is seeking to measure: engagement and activity at the exhibits and installations at 307.
Data Security and Safeguards What technical, administrative, physical, and procedural safeguards (mitigating controls) are in place to prevent and mitigate risks? What processes are in place to detect, mitigate, and report a breach of safeguards relating to Personal Information (such as. a loss of, or unauthorized access to or disclosure of, Personal Information)?	Sidewalk Labs will not store personal information through this pilot. Numina's sensors encrypt all communication with TLS1.2 using industry standard AES-256 encryption. Only authorized devices can communicate with Numina sensors, removing pathways for data interception or sensor access by unauthorized third parties. In its agreement with Sidewalk Labs, in describing its security practices in the agreement, Numina represents that its hardware and software are hardened by minimizing attack surfaces, that it uses strong encryption in communications between Numina endpoints, and that its systems undergo periodic security reviews and are updated with the latest patches.
Logging and Monitoring Describe how actions related to the collection, use, disclosure, retention, correction, copying or disposal of personal information are logged. Will those logs be subject to auditing and monitoring? Please explain your response.	Sidewalk Labs will not store Personal Information through this pilot. Only Sidewalk Labs staff with the log-in credentials to the Numina dashboard are able to view the de-identified data.

5. Project Net Benefits	
What is the net benefit?	
Consider the above mentioned risks and mitigations with your overall objectives and stated beneficial purpose... What is the anticipated impact of the benefit? How likely is it to occur? Please highlight your answer. Explain your reasoning.	**Benefit:** 1 — Low Impact; 2 — Moderately Low impact; 3 — Moderate impact; 4 — Moderately high Impact; **5 — High impact** **Likelihood:** 1 — Low likelihood; 2 — Moderately Low likelihood; 3 — Medium likelihood; 2 — Moderately High likelihood; **5 — High likelihood** With on-device processing of images into de-identified movement and count data, and short-term storage of low-resolution de-identified images, the risks to privacy are very limited compared to the potential uses and benefits of the data. The risks are further limited by the scope of the pilot at the 307 location. The collection of pilot data will help assess the effectiveness of exhibits and installations at 307, including outdoor weather mitigation structures, flexible pavers, and indoor exhibits. The data will benefit Sidewalk Labs and its project partners by helping measure utilization at 307, and helping revise designs to better achieve their respective goals. At larger scales, managers of publicly accessible spaces, from municipalities to private land owners alike, make decisions on a routine basis that impact the users of those spaces. Examples of these decisions include determining the frequency of routine maintenance tasks, or making changes to the physical infrastructure and amenities available in those spaces, or managing transportation networks. When available comprehensively across a portfolio of locations, objectively gathered utilization data can support resource allocation and investment decisions. The pilot will help determine whether and how the pilot technology can be deployed on a larger scale.

6. Summary and Approval	
What are the applicable laws? (such as, PIPEDA, FIPPA, MFIPPA, Privacy Act) Does the data activity comply with all laws, cross-border, policy, contractual, industry or other obligations, and organizational policies and self-regulatory commitments? Please explain your response.	**PIPEDA:** To the extent that real time de-identification is considered a collection or use of Personal Information, this pilot would be subject to PIPEDA as it would involve the collection and use of Personal Information in the course of a commercial activity by Sidewalk Labs. The Numina sensors process and de-identify still images on-device and Sidewalk Labs receives no Personal Information. The Numina sensors also transmit encrypted low-resolution QA images to Numina that are de-identified real-time on Numina servers. Only one randomly sampled, low-resolution QA image each hour is transmitted and stored in the cloud for 30 days for QA purposes. Numina applies a face blurring algorithm to the low resolution images to remove identifiable features from QA images before they are made available to employees or services. To the extent that real time de-identification is considered a collection or use of Personal Information, any such Personal Information would be transitory, de-minimis, and not sensitive (images de-identified and deleted in real time or random samples image de-identified on-server and encrypted in transit). As such, if the pilot is considered to collect or use Personal Information, it is reasonable for Sidewalk Labs to rely on implied consent. Sidewalk Labs will place signage to provide notice of the sensors. The notices will emphasize the key elements of the pilot technology and data and are provided at the time a visitor would be entering the pilot area (i.e. they are just in time notices). The pilot will also be accompanied by an exhibit that will explain how privacy protection is inherent in the design of the technology and illustrate the use cases to which the data is being applied at 307 as well as potential for application at wider scales. Visitors to 307 will be provided with details on what data is being collected, for what purpose, and who has access to the data.

What are the applicable laws? (such as, PIPEDA, FIPPA, MFIPPA, Privacy Act) (Cont'd) Does the data activity comply with all laws, cross-border, policy, contractual, industry or other obligations, and organizational policies and self-regulatory commitments? Please explain your response. (Cont'd)	To the extent that Personal Information is collected or used in connection with the pilot, information posted at the pilot site will serve as notice for the purpose of obtaining implied consent when a visitor continues onto the pilot site.
After considering all the above factors, is the activity a "go," "no go," or should some aspect of the activity be recalibrated to reduce the residual risk of the activity? Please explain your response.	Yes. This pilot should proceed. Sidewalk Labs approved this pilot because it meets the beneficial purpose of testing the pilot technology, which is intended to be a tool to improve mobility and enhance a people-first public realm. The RDUA allowed Sidewalk Labs to assess the risks and benefits of this data activity. The vendor's (Numina) use of privacy-preserving technology result in a low risk. There are many benefits to this pilot and the risk of harm to individuals and society is very low. A new RDUA will be completed if the parameters of the pilot change. For example, if a new sensor is added that collects data in a location other than Sidewalk Labs' private property.
Key privacy or data governance issues	The key privacy and data governance issues are: ● On-device and on-server de-identification of Personal Information. ● Security of the Numina sensors. This pilot will take place at Sidewalk Labs' office, which is often accessible to the public. The Numina sensor's cameras will process low resolution images that are de-identified in real time. The sensors use cameras to capture data about movement in an area, but immediately process it on-device into a sequence of time stamped two-dimensional coordinates linked by an arbitrary path id number and a "class," which specifies if the moving object is a person, bicycle, car, truck, or bus.

Key privacy or data governance issues (Cont'd)	The image data is processed in real time and is not stored in persistent memory (i.e. the image data is deleted after processing), except for QA images, as noted below. This processing results in vehicle and pedestrian movement and count data. Sidewalk Labs receives this data in the form of aggregate statistics and insights, and may receive the actual movement and count data collected by the Numina sensors. In addition, the sensors send one low-resolution QA image at a random time, once per hour, to Numina for calibration and data validation purposes (24 images per day, from among more than 172,000 that are processed on-device to create the de-identified movement and count data which never leaves the Numina device). These QA images are encrypted in transit and de-identified automatically (through computer blurring) on receipt by the Numina servers, and may only be accessed by authorized Numina personnel (and not Sidewalk Labs personnel). These QA images are retained for 30 days by Numina and are only used to calibrate and validate the pedestrian and vehicle movement and count data. (For example, the QA images are used to confirm that the algorithm is correctly classifying pedestrians and vehicles.)
Mitigation measures	**De-identification** Numina de-identifies the vast majority of images on-device in real time using the following method: On-board the Numina sensor, the image is processed into a sequence of time stamped two-dimensional coordinates linked by an arbitrary path id number and a "class," which specifies if the moving object is a person, bicycle, car, truck, or bus. Numina's algorithm creates "boxes" around each moving object within the sensor's field of view, classifying into broad categories such as pedestrian, cyclist, and car without tracking any Personal Information.

Mitigation measures (cont'd)	One randomly sampled image per hour is transmitted and stored in the cloud by Numina for 30 days for quality assurance (QA) purposes. The QA images are low resolution (less than 1 pixel per cm and of low image quality (JPEG Q=50). To eliminate the possibility that, despite this low resolution, Personal Information is captured in the image, Numina immediately applies an object detection and a blurring algorithm to remove recognizable features from QA images before they are made available to any Numina agents or employees for validation. Sidewalk Labs never receives any sample images. **Minimization** The Numina sensors de-identify any Personal Information on-device when creating the vehicle and pedestrian movement and count data. Furthermore, QA Images are low resolution and subject to further de-identification to ensure that only the minimum amount of data is collected and used to achieve the purposes of the pilot. **Security** Sidewalk Labs will not receive Personal Information from Numina and Numina will only store de-identified Personal Information. Numina's cloud service provider is AWS. Sidewalk Labs may access pilot data (excluding QA images) in a number of ways, including: ● viewing it directly from Numina's dashboard ● copying the data to Sidewalk Labs' Google Cloud instances ● downloading data onto employee devices for the purposes of data analysis Numina's sensors encrypt all communication with TLS1.2 using industry standard AES-256 encryption. Only authorized devices can communicate with Numina sensors, removing pathways for data interception or sensor access by unauthorized third parties.
Summary of Outstanding Issues	**N/A**

Recommendations	Sidewalk Labs approves this pilot because it meets the beneficial purpose of improving mobility and enhancing a people-first public realm, while mitigating against the potential privacy concerns with a robust de-identification process. A new RDUA will be completed if the parameters of the pilot change, including the placement of any Numina Sensors in the public realm, or if the purpose for data collection or use changes.

2.2.3.3 RDUA Guidance and Reference

The Responsible Data Use Assessment (RDUA) is a tool to ensure compliance with applicable laws, as well as the application of the Responsible Data Use Guidelines and Privacy by Design principles. The RDUA process can involve an in-depth review and analysis of a project, service, product, or pilot undertaken when there is a proposal to collect, use, or disclose data about people (including personal information) or data that has the potential to impact people (referred to simply as “data” throughout this document).

Completing the RDUA is a team effort. In addition to the privacy and product counsel, team members who are technical experts are required to fill out the RDUA. To assist team members in completing the RDUA, Sidewalk Labs’ data governance team has created a living resource, known as the RDUA guidance and reference, to assist those filling out the RDUA who may have questions. The guidance and reference resource is not meant to be an exhaustive resource and does not replace ongoing conversations between multiple team members. Similarly to how each pilot or product has a product or project manager, a member of the privacy and data governance team is assigned, so that real time guidance can be provided.

Responsible Data Use Assessment - Guidance and Reference	
Canada - *Personal Information Protection and Electronic Documents Act* (PIPEDA) (in brief)	
What is personal information?	Under PIPEDA, personal information means any information about an identifiable individual. This includes information in any form, such as: ● age, name, ID numbers, income, ethnic origin, or blood type; ● opinions, evaluations, comments, social status, or disciplinary actions; and ● employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs). Information will be about an “identifiable individual” where there is a possibility that an individual could be identified through the use of that information, alone or in combination with other information. PIPEDA applies to Personal Information collected, used, or disclosed by an organization in the course of commercial activities.
What is not covered by PIPEDA?	● Personal information handled by federal government organizations that are subject to the *Privacy Act*, and their agents. ● Personal information handled by provincial or territorial government organizations that are subject to any public sector privacy law (such as the Freedom of Information and Protection of Privacy Act in Ontario), and Personal information handled by municipal government organizations that are subject to any public sector privacy law (such as the Municipal Freedom of Information and Protection of Privacy Act in Ontario), and their agents. ● Business contact information, such as an employee’s name, title, business address, telephone number or email addresses, that is collected, used or disclosed solely for the purpose of communicating with that person in relation to their employment or profession.

What is not covered by PIPEDA? (Cont'd)	• An individual's collection, use, or disclosure of personal information strictly for personal or domestic purposes (such as a personal greeting card list). • An organization's collection, use, or disclosure of personal information solely for journalistic, artistic, or literary purposes. Unless they are engaging in commercial activities that are not central to their mandate and involve personal information, PIPEDA does not generally apply to not-for-profit organizations or voluntary associations. Although municipalities, universities, schools, and hospitals are generally subject to provincial public sector laws, PIPEDA may apply in certain situations. The collection, use, and disclosure of personal information by organizations within the provinces of Alberta, British Columbia, and Quebec is subject to the applicable province's private sector privacy laws.
In general, organizations must follow the 10 fair information principles included as Schedule 1 to PIPEDA	The principles are: 1. Accountability 2. Identifying Purposes 3. Consent 4. Limiting Collection 5. Limiting Use, Disclosure, and Retention 6. Accuracy 7. Safeguards 8. Openness 9. Individual Access 10. Challenging Compliance

Responsible Data Use Assessment - Guidance and Reference Sidewalk Labs' Responsible Data Use Guidelines	
Beneficial purpose	All proposed uses of data must incorporate Canadian values of diversity, inclusion, and privacy as a fundamental human right. To meet this standard, there must be a clear purpose and value to any proposed use of data, as well as a clear, direct connection to the ways in which the project and proposed data-collection activity would benefit individuals or the community. A proposal or project should not be collecting data for the sake of having data.
Transparency and clarity	Individuals should be informed about how and why data is collected and used in a way that is proactive, clear, and easy to understand.
Data minimization, security, and de-identification by default	Only the minimum amount of data needed to achieve the beneficial purpose should be collected and the least invasive technology available to achieve the beneficial purpose should be used. By default, the most up-to-date de-identification techniques to reduce the amount of personal information collected should be used.
Publicly accessible by default	Whenever possible, properly de-identified or non-personal data should be made publicly accessible to third parties by default, formatted according to open standards. Sidewalk Labs believes that preserving individual privacy, while also enabling data and source code to be accessible by others to catalyze innovation, is the preferred approach.
No selling personal information or use for advertising	Sidewalk Labs has already committed publicly that it would not sell personal information to third parties or use it for advertising purposes. It also commits to not share personal information with third parties, including other Alphabet companies, without explicit consent.
Responsible AI principles required	To ensure that issues around the use of artificial intelligence systems are being considered and addressed by data collectors and developers, Sidewalk Labs has developed Responsible AI principles and is working to incorporate these principles into its development and decision-making to promote the spread of responsible technology and data use.

Responsible Data Use Assessment - Guidance and Reference **Privacy By Design Principles** (source: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf)	
Principle	**Text**
Proactive not reactive; preventative not remedial	The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.
Privacy as the default setting so that if the individual does nothing, their privacy is preserved (ex. Opt-in rather than opt-out)	We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.
Privacy embedded into the design	Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
Full functionality and win-win objectives (for example, so that the individual does not need to give up privacy for security)	Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.
End-to-end security and full lifecycle protection	Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

Visibility and transparency	Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is, in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
Respect for privacy, and keep it user-centric	Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Responsible Data Use Assessment - Guidance and Reference **Section 2: Initial Assessment Questions**	
Explain why you want to collect, use, or share data and why you believe that will achieve the stated beneficial purpose.	Briefly describe the problems that are being solved by the project, service, product, or pilot (“Initiative”) (in one or two sentences). This requires a clear connection to a beneficial purpose. Organizations should not collect data if collecting less data will achieve the same objectives. Explain why the Initiative (as described) is better than alternatives that may collect or use less data (particularly if less personal information is involved in those alternatives).
Who are all the possible stakeholders and parties involved or related to the Initiative? What are their interests and potential concerns?	Stakeholders are very broad and apply to anyone impacted by the data and data uses under the Initiative. For example, a stakeholder for a framework could be a regulator or advocacy organization. Stakeholders for data and data collection and uses include data partners. However, stakeholders can also include those interested in the success of a data use. For example, people who live in Quayside, people who visit 307, or users of an app could be stakeholders depending on the nature of the Initiative. List the individuals, groups, communities, society who are stakeholders.

Responsible Data Use Assessment - Guidance and Reference **Section 3: Understanding the Technology and the Data Sources**	
A Data Flow Diagram and Data Table can be considered as part of the review process.	
Data Flow Diagram	● Provide a flow diagram of all data collected, used, or disclosed in connection with the Initiative. ● The diagram should clearly depict each stage of the data flow (including instances of collection, storage, use, transfer, or disclosure). ● *(link to examples of diagrams)*

<table>
<tr><th colspan="3">Responsible Data Use Assessment - Guidance and Reference
Data Table</th></tr>
<tr><th>Collection Source</th><th>Use(s)</th><th>Data Categories</th></tr>
<tr><td>Select the applicable source of the data:
Sensor data (video, audio, location, environmental, consumption, pressure, etc)
User-submitted or user-generated data (filling out an online or paper form, interactions on a website, etc)
Third-party data (historical records, purchased data, open data portals, etc)
Metadata or API data
Internal data (data collected and stored from other purposes)</td><td>For each source, set out the use of the data. Note whether each use is a primary use of or secondary use of data.</td><td>Identify what data categories are applicable to this source/use, and (below) comment on the reliability of the data:
Personal Information: See the definition of personal information at the introduction of this guidance.
Personal Information from or about children under the age of 13: The OPC’s position is that “in all but exceptional circumstances” children under 13 cannot provide consent on their own behalf.
Non-personal data: Data about an individual that is not identifiable to an individual.
De-identified Personal Information: Information about an individual that was identifiable when collected but has subsequently been made non-identifiable.
Aggregate information about people: Information that is about people in aggregate and not about a particular individual.
Online behaviour data: such as IP addresses, cookies, logs, analytics, crash reports, location.
How are we maintaining attribution of the data source through the data lifecycle?
If one source of data is combined with others, how will we keep track of where each data element came from?</td></tr>
</table>

Responsible Data Use Assessment - Guidance and Reference		
Section 4.1: Privacy and Data Governance		**PIPEDA Reference (Canada)**
Necessity of Collection	Each item of personal information must only be collected if it is necessary for an identified purpose of the Initiative. For each item of personal information (or groups of items) explain why that personal information is necessary, and why less personal information would not achieve the purposes of the Initiative.	Clause 4.4 of Schedule 1: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Clause 4.4.1 of Schedule 1: Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.
Notice and Consent **Personal Information: Consent — Collection, use, and disclosure of Personal Information (Canada)** To the extent personal information is collected, is there full compliance with the Office of the Privacy Commissioner's ("OPC") Meaningful Consent Guidelines?	**Meaningful Consent Guidelines — Guiding Principles:** 1. **Emphasize key elements:** ○ 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 2. **Allow individuals to control the level of detail they get and when** 3. **Provide individuals with clear options to say 'yes' or 'no'**	Clause 4.3 of Schedule 1: Consent is required for the collection of personal information and its subsequent use or disclosure. Clause 4.3.2 of Schedule 1: To be meaningful, consent must be stated in a way an individual can reasonably understand. Clause 4.2 of Schedule 1: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Notice and Consent **Personal Information: Consent — Collection, use, and disclosure of Personal Information (Canada) (Cont'd)** To the extent personal information is collected, is there full compliance with the Office of the Privacy Commissioner's ("OPC") Meaningful Consent Guidelines?	4. **Be innovative and creative in how consent is obtained — relying on lengthy static text is often an ineffective means of obtaining consent** 5. **Consider the consumer's perspective** 6. **Make consent a dynamic and ongoing process** 7. **Be accountable: Stand ready to demonstrate compliance**	Section 5(3): An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. Section 6.1: The consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequences of the collection, use, or disclosure of the personal information to which they are consenting.
Personal Information: Consent — Collection, use, and disclosure of Personal Information (Canada) (Cont'd) How did the individual consent to giving you their data? If applicable, did you obtain consent for secondary purposes? How can they revoke consent? What impact will withdrawing consent have on the individual?	**In addition to addressing the above principles:** If the Initiative uses mobile, web, or other applications, is there a consent flow in your app? If so, provide links to or embed your mock-ups and your consent wording. Does the Initiative use consent forms? If so, provide links to the form. Does the Initiative rely on implied consent (opt-out consent)? If so, describe the mechanism. For an example of implied consent, a sign is placed at the entrance of the building with all of the information detailing the data activity. The individual provides implied consent when they read the notice and continue to walk into the building.	See above. Clause 4.3.4 of Schedule 1: In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Clause 4.3.5. of Schedule 1: In obtaining consent, the reasonable expectations of the individual are also relevant. Clause 4.3.6 of Schedule 1: An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive.

Personal Information: Consent — Collection, use, and disclosure of Personal Information (Canada) (Cont'd) How did the individual consent to giving you their data? If applicable, did you obtain consent for secondary purposes? How can they revoke consent? What impact will withdrawing consent have on the individual?	What type of control do individuals have with respect to their personal information? If individuals can withdraw consent to secondary uses, how can they do so?	Clause 4.3.3 of Schedule 1: An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes. Clause 4.3.8 of Schedule 1: An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.
All Data: Notice How is information about this process being communicated to the users (for example, help page or part of the consent flow?)		N/A. PIPEDA's obligations only apply to data that is personal information.
Access and Individual Control How can users access, edit, or delete the data they have provided you and how can they do this?	If the Initiative has mobile or web app or other interface, can individuals access their personal information from the interface? Can they edit or delete their personal information through the interface? If so, describe how individuals may access, edit, and delete their personal information and what personal information they may access, edit, and delete.	Clause 4.9 of Schedule 1: An individual shall be informed of the existence, and shall be given access to, their personal information on request. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Access and Individual Control (cont'd) How can users access, edit, or delete the data they have provided you and how can they do this?	If not, or if the Initiative does not have a website, app, or other interface, is there a contact for individuals to reach in order to request access to their personal information? Describe the process for individuals to request access to their personal information.	Clause 4.3.8 of Schedule 1: An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal. Section 8(1): Individual requests under clause 4.9 of Schedule 1 must be made in writing. Section 8(3): Organizations shall respond to requests with due diligence and in any case within 30 days, subject to extensions pursuant to section 8(4). Section 9(4): Access may be refused only in certain cases.
Deletion Does deleting the app or service delete the data or is that an extra step? Describe the process and who the individual must contact. Can users delete individual line items or can they delete all the data associated with the Initiative at once?	If applicable, describe the process required for users to delete their information. If deleting an app or service does not delete the personal information of an individual, state the purpose for which that personal information is being retained.	Clause 4.5 of Schedule 1: Personal information shall be retained only as long as necessary for the fulfilment of the purposes for which it was collected. Clause 4.3.8 of Schedule 1: An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

Secondary Purposes Can users withdraw consent regarding secondary or tertiary uses of the data?	If users cannot withdraw consent to secondary uses of data, explain why. **Canada** For personal information, if users cannot withdraw consent consider whether such uses are truly secondary uses. If after further consideration they are still considered secondary uses of personal information and users cannot withdraw consent, these uses must be removed from the Initiative until users can withdraw their consent. The OPC refers to mandatory collections, uses, or disclosures of personal information as conditions of service. Mirroring the wording of PIPEDA, the OPC notes that a condition of service "must be integral to the provision of that product or service such that it is required to fulfill its explicitly specified and legitimate purpose." A secondary use would be any use that is not a condition of service.	Clause 4.3.3 of Schedule 1: An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes. Clause 4.3.8 of Schedule 1: An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.
Location of Data Where is data stored (primary, disaster recovery, via service provider)? Can data be accessed from locations outside of Canada?	This encompasses primary storage, backup/DR storage, and third party provider storage. It should cover all places where the data can be stored or from where the data can be accessed.	Clause 4.1 of Schedule 1: An organization is responsible for personal information under its control. Clause 4.7 of Schedule 1: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Location of Data (cont'd) Where is data stored (primary, disaster recovery, via service provider)? Can data be accessed from locations outside of Canada?		Clause 4.1.3 of Schedule 1: An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
Data Retention Period How long is the data to be retained? For personal information, you should indicate whether the personal information will be converted to de-identified form, and then retained as de-identified data.	Set out the minimum and maximum retention periods for data. If there is no uniform minimum and maximum retention period for all data, set out the minimum and maximum retention period for each type of data in the Data Table. Set out whether personal information will be de-identified or deleted. **Canada** OPC Personal Information Retention and Disposal: Principles and Best Practices PIPEDA mandates that "personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous.	Clause 4.5 of Schedule 1: Personal information shall be retained only as long as necessary for the fulfilment of the purposes for which it was collected. Clause 4.5.2 of Schedule 1: Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. Clause 4.5.3 of Schedule 1: Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

Data Retention Period (cont'd) How long is the data to be retained? For personal information, you should indicate whether the personal information will be converted to de-identified form, and then retained as de-identified data.	Personal Information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made. Personal Information that is subject to an access request must be retained as long as necessary for the individual to exhaust any recourse under PIPEDA.	Section 8(8): Personal information that is subject to an access request must be retained as long as is necessary to allow the individual to exhaust any recourse under PIPEDA.
Destruction and Deletion After you no longer need the data, how will the data be deleted, destroyed, or made anonymous?	Explain how data will be destroyed based on the medium on which it is stored (for example, on-device, on portable storage media, in the cloud). Agreements with third party processors should include clauses regarding the return and deletion of data. Where possible, refer to commonly accepted or industry standards. **Canada** OPC guidance refers to "commonly accepted ways for organizations to properly dispose of personal information" and notes that "[t]he goal is to irreversibly destroy the media which stores personal information so that personal information cannot be reconstructed or recovered in any way. When going through the process of disposal, an organization should also destroy all associated copies and backup files."	Clause 4.5.3. of Schedule 1: Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. Clause 4.7.5. of Schedule 1: Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Data Transfer (transfers for processing) **Legal:** How will third parties be bound to follow relevant privacy and data security requirements?	Sidewalk Labs needs to retain control of all data transferred for processing. The third-party processor should only be able to use the data as instructed by Sidewalk Labs in writing, and only to provide Sidewalk Labs with services. At the end of the relationship, the third-party processor should return all data to Sidewalk Labs and destroy all Sidewalk Labs data. Sidewalk Labs' agreements with third-party processors should require that they maintain all safeguards set out in the "Mitigating Risks" section of the RDUA that are applicable to the third-party processor. **Canada** OPC Guidance for processing personal data across borders "Transfer" is a use by the organization. It is not to be confused with a disclosure. When an organization transfers personal information for processing, it can only be used for the purposes for which the information was originally collected and if so, additional consent is not needed. A simple example is the transferring of personal information for the purpose of processing payments to customers. Or to use another example, an internet service provider may transfer personal information to a third party to ensure that technical support is available on a 24/7 basis.	Clause 4.1 of Schedule 1: An organization is responsible for personal information under its control. Clause 4.1.3 of Schedule 1: An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Clause 4.7 of Schedule 1: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Data Transfer (transfers for processing) (cont'd) **Legal:** How will third parties be bound to follow relevant privacy and data security requirements?	"Processing" is interpreted to include any use of the information by the third party processor for a purpose for which the transferring organization can use it. "Comparable level of protection" means that the third party processor must provide protection that can be compared to the level of protection the personal information would receive if it had not been transferred. It does not mean that the protections must be the same across the board, but it does mean that they should be generally equivalent.	
Data Disclosures	A disclosure is a separate act from a "use." The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).	Clause 4.3 of Schedule 1: Consent is required for the collection of personal information and its subsequent use or disclosure. Clause 4.3.2 of Schedule 1: To be meaningful, consent must be stated in a way an individual can reasonably understand. Clause 4.3.3 of Schedule 1: An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes.

Data Disclosures (cont'd)	Sidewalk Labs has already committed that it would not sell personal information to third parties or use it for advertising purposes. It has also committed to not share personal information with third parties, including other Alphabet companies, without explicit consent. Some of the questions that should be considered here: 1. Who is sharing the data with whom, and on whose behalf? 2. How will the shared data be matched, combined, or augmented with other data? 3. How is secure data transfer done? 4. Length of the data transfer arrangement 5. Link to Data Sharing Agreement: (if unavailable flag privacy@sidewalklabs.com) 6. Link to Vendor Security Agreement: (if unavailable flag privacy@sidewalklabs.com) 7. What mechanisms, controls, and safeguards exist to ensure parties receiving Personal Information adhere to data obligations? 8. How effective are those mechanisms is mitigating risks?	
Custody and Control (Canada)	Sidewalk Labs retains control of the personal information it transfers to third-party processors for processing on Sidewalk Labs' behalf (the OPC has noted that "a company does not relinquish control of the information" by transferring it to a third-party processor).	Clause 4.1 of Schedule 1: An organization is responsible for personal information under its control. Clause 4.1.3 of Schedule 1: An organization is responsible for personal information in its possession or custody.

Custody and Control (Canada) (cont'd)	In contrast, where Sidewalk Labs discloses personal information to another organization, that other organization may then have control of the personal information that was disclosed. Third-party processors will have "possession or custody" of personal information or data that Sidewalk Labs transfers for processing.	
Responsible AI (1) How are analytical driven models or insights, or algorithmic decision making being used? (2) How could individuals or groups of people be impacted by this use?	Set up a time to chat with your privacy and data governance contact person.	Section 5(3): An organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. Clause 4.3.5. of Schedule 1: In obtaining consent, the reasonable expectations of the individual are also relevant.
Publicly Available Sidewalk Labs has committed that data (excluding personal information) will be "publicly accessible by default." Does this data activity result in open data? If not, why?	Personal information will not be made available by default.	N/A. PIPEDA's obligations only apply to data that is personal information.

Responsible Data Use Assessment - Guidance and Reference		
Section 4.2. Risks and Data Ethics		**PIPEDA Reference (Canada)**
Is the data sensitive? What kinds of biases might exist in the data?	Sensitive categories of data or use include information that is used to analyze or make decisions based on race, ethnic origin, religion or philosophical belief, gender, sexual orientation, physical or mental health, and information or data that could be used to facilitate identity theft. If the data activity involves participatory data (for example, data that is generated by individuals choosing to participate in the project or activity), does everyone have the opportunity to participate or are there barriers to participation for some groups? Are participants adding their own biases? If the data activity involves historical data, has the data been assessed for historical biases? Are some communities over- or under-represented in the data set, or is data for some communities less accurate? How can these be accounted for to ensure that the biases are not perpetuated?	Clause 4.3.4 of Schedule 1: Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.
Could the anticipated use of technology harm or benefit, result in unforeseen consequences, or benefit certain individuals, groups of people, or communities in unintended or unexpected ways?		Section 5(3): An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

Could the data be used in a way that may result in one individual or group being treated differently than others? For example, to determine if someone's eligibility for a service or benefit.		
Would anyone be surprised that this data is being collected or used in this way?		Section 5(3): An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.
Data Accuracy What measures are in place to make sure personal information is not used, unless it is accurate, complete, and up-to-date? Provide details of measures.	Is the accuracy and quality of the data appropriate for the data activity? Is it more accurate than necessary? What happens when data is inaccurate?	Clause 4.6 of Schedule 1: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
How could the data activity be perceived as not fitting within the demonstrated values of society?	Evaluate whether the activities of the project are consistent with the demonstrated values of society where they take place (for example, broad principles such as freedom of expression or the protection of human rights, social policies, or policies or objectives of community organizations).	N/A.

Responsible Data Use Assessment - Guidance and Reference		
4.3 Mitigating Risks		**PIPEDA Reference (Canada)**
De-identification: If the data is Personal Information, has it been de-identified? If so, how has it been de-identified? If the data is Personal Information and is not de-identified, what is the beneficial purpose for keeping the data identifiable?	**Responsible Data Use Guideline:** Sidewalk Labs has committed to de-identification by default. If the data is de-identified, provide details on how and when it is de-identified as part of the data flow (such as. on device or in the cloud). De-identification should be included in the above data flow diagram.	Clause 4.5.3 of Schedule 1 – Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.
How likely is it that de-identified data could be combined with other information to identify individuals?	**Canada** Information will be about an "identifiable individual" where there is a possibility that an individual could be identified through the use of that information, alone or in combination with other information.	
Data Minimization: 1. Is there a less data intensive way to achieve the goals of the data activity (including potential insights)? 2. How has a less data intensive data activity been developed throughout the RDUA process?		Clause 4.4 of Schedule 1: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Clause 4.4.1 of Schedule 1: Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.

Data Minimization: (cont'd) 1. Is there a less data intensive way to achieve the goals of the data activity (including potential insights)? 2. How has a less data intensive data activity been developed throughout the RDUA process?		Clause 4.5 of Schedule 1: Personal information shall be retained only as long as necessary for the fulfilment of the purposes for which it was collected.
Data Security and Safeguards: What are the technical and procedural safeguards (mitigating controls) in place to prevent and mitigate risks should they occur (such as. encryption and delinking of data or increased transparency)? What processes are in place to detect, mitigate, and report a breach to the storage of personal information (such as a loss of, or unauthorized access to or disclosure of, personal information)?	Where does your project store the data described above, and who has internal access to it? Please specify all forms of storage (such as logs, client-side and server-side storage, storage subsystems, backups). Please also explain who gets access, who grants access, and what technical enforcement is in place? What auditing is in place? Is the data encrypted, anonymized or otherwise maintained on protected systems? What, if any, customer support teams or customer support tools have access to this data? List the physical, organizational, and technical protection measures used to protect data. Agreements with third-party processors should include provisions requiring the processor to use appropriate protection measures and to notify Sidewalk Labs of any breach in connection with Sidewalk Labs data. Set out any processes in place to detect, mitigate, and report any security breaches.	Clause 4.7 of Schedule 1: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Clause 4.7.2 of Schedule 1: The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection Clause 4.7.3 of Schedule 1: The methods of protection should include physical measures, organizational measures (ex., limiting access), and technological measures.

Data Security and Safeguards: (cont'd) What are the technical and procedural safeguards (mitigating controls) in place to prevent and mitigate risks should they occur (such as. encryption and delinking of data or increased transparency)? What processes are in place to detect, mitigate, and report a breach to the storage of personal information (such as a loss of, or unauthorized access to or disclosure of, personal information)?	**Canada** PIPEDA's mandatory breach reporting requirements arise where a breach of security safeguards (as defined in PIPEDA) creates a real risk of significant harm to individuals. Relevant factors in evaluating whether there is a real risk of significant harm include the sensitivity of the personal information and the probability that it will be misused.	<u>Section 10.1(1):</u> An organization shall report to the OPC any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. <u>Section 10.1(3):</u> Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. "Breach of security safeguards" means the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards.
Logging and Monitoring / Employee Access: 1. Describe how you log actions relating to the collection, use, disclosure, retention, correction, copying or disposal of data? 2. Will those logs be subject to auditing and monitoring?	Access to sensitive personal information should be appropriately logged and monitored, for example by logging time, date, and user information for any access, modification, or transmission of data. Agreements with third-party processors should address monitoring and auditing of the third-party processors.	<u>Clause 4.7.3 of Schedule 1:</u> The methods of protection should include physical measures, organizational measures (ex., limiting access), and technological measures. <u>Clause 4.7.4 of Schedule 1:</u> Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

Responsible Data Use Assessment - Guidance and Reference **Section 5: Project Net Benefits**	
Consider the above mentioned risks and mitigations with your overall objectives and stated beneficial purpose. What is the anticipated impact of the benefit? How likely is it to occur? Please highlight your answer. Explain your reasoning.	Does an appropriate balance of benefits and mitigated risks support the data processing activity? Consider whether the risks are necessary and proportional to the benefits. Have the risks been mitigated to the greatest extent possible? Are the mitigated risks sufficiently balanced by the benefits?

Responsible Data Use Assessment - Guidance and Reference **Section 6: Summary and Approval**	
What are the applicable laws? (such as, PIPEDA, FIPPA, MFIPPA, *Privacy Act*) Does the data activity comply with all laws, cross-border, policy, contractual, industry or other obligations, and organizational policies and self-regulatory commitments?	PIPEDA applies to the collection, use, and disclosure of personal information by Sidewalk Labs in the course of commercial activity (excluding the personal information of Sidewalk Labs own employees for employment purposes, as Sidewalk Labs is not a federal work, undertaking, or business). FIPPA and MFIPPA apply to certain Ontario public sector entities and bodies, while the *Privacy Act* applies to certain federal public sector entities. These public sector privacy laws do not apply to Sidewalk Labs directly and will only be relevant if either (1) Sidewalk Labs is processing personal information on behalf of a public sector entity; or (2) Sidewalk Labs is partnering with a public sector on the Initiative (in which case the public sector entity may require the Initiative, as a whole, to comply with a public sector law).

Summary of outstanding issues	List any risks/issues identified that have not been resolved, either because they were accepted, or because it is too early in the project to address When is the next review/update of this document? For example, next release, upon securing a partnership, during procurement, or other similar events.

2.2.3.4 Sidewalk Labs' next steps for responsible AI

Artificial intelligence and algorithmic systems are found in all areas of modern life. Some applications are as benign as email spam filters; others carry more significant impacts, such as the approval of loan applications[13] or rating a defendant's risk of future crime.[14] In many ways, datasets and algorithms can mirror social biases and blind spots, yet are often considered more objective, efficient, and trustworthy than human decision-makers — a phenomenon known as automation bias.[15] The development and use of AI systems are increasing, which raises digital governance challenges that go beyond privacy. Yet, the field of AI and data ethics is new; there is no established and comprehensive governance approach.

Over the last several years, and certainly in recent years, there has been a proliferation of AI principles.[16] The OECD Principles on AI and the Declaration on Ethics and Data Protection in Artificial Intelligence[17] are likely precursors to legislation and regulations. OECD's recommendations are not legally binding, but they are highly influential in helping governments draft national legislation.[18]

What Is "Responsible AI"?

Sidewalk Labs believes that responsible technology includes a framework of responsible data use and a commitment to responsible AI underpinned by the principles of beneficial purpose, transparency and clarity, accountability, and a

---

[13] Anupam Datta, "Did Artificial Intelligence Deny You Credit?," The Conversation, March 13, 2017.

[14] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, "Machine Bias," *ProPublica*, May 23, 2016.

[15] Information Commissioner's Office, "Automated Decision Making: the role of meaningful human reviews," April 12, 2019. See also, Nizan Geslevich Packin, "Algorithmic Decision-Making: The Death of Second Opinions?," March 28, 2019.
Also known as "data fundamentalism". Paul Roberts, "At MIT Conference, Warnings of Big Data Fundamentalism," *SecurityLedger*, October 9, 2013.

[16] See section 4.5.2 for more details , plus "AI Ethics Guidelines Global Inventory," Algorithm Watch, accessed September 25, 2019 ; "Principles on AI," Organisation for Economic Co-operation and Development, accessed September 25, 2019.

[17] Commission nationale de l'informatique et des libertés (France), European Data Protection Supervisor (European Union), and Garante per la protezione dei dati personali (Italy), "Declaration on Ethics and Data Protection in Artificial Intelligence," adopted at the 40th International Conference of Data Protection and Privacy Commissioners, Brussels, October 23, 2018.

[18] An example of a law that tries to bridge the gap between data protection and AI is the Algorithmic Accountability Act of 2019. Proposed last spring by US lawmakers, this law would require certain organizations to conduct an "automated decision system impact assessment" and a "data protection impact assessment" under the authority of the Federal Trade Commission. See Algorithmic Accountability Act of 2019, H.R.2231, 114th Cong. (2019); and Adi Robertson, "A New Bill Would Force Companies to Check Their Algorithms for Bias," *Verge*, April 10, 2019. Canada is leading in ethical and responsible AI, with the creation of an open source Algorithmic Impact Assessment. See also section 4.5.2.2 of the Digital Innovation Appendix

respect for human dignity. AI systems should be used responsibly and ethically, and this extends to the procurement, development, and deployment of AI systems, as well as to the investment in AI systems.

Sidewalk Labs' responsible AI framework is guided by six overarching principles that are contextual, progressive, and technology neutral.[19]

1. **Fairness and equity:** All projects involving AI systems should be designed and developed responsibly from the start and should consider an individual's reasonable expectations and the original purposes of data collection.
2. **Accountability:** Sidewalk Labs commits to completing RDUAs for all projects and products that involve AI and compiling an archive of all automated decision systems.
3. **Transparency and explainability:** Individuals should be informed when they are interacting directly with an automated system and when their personal data is being used to make consequential decisions about them. AI systems should be designed with the ability to explain and debug their output in terms people can understand.
4. **Relevance:** Sidewalk Labs commits to high standards of scientific excellence and a multidisciplinary approach that includes sharing research and best practices with regard to AI.
5. **Value alignment:** AI systems should be designed, developed, and used in line with international human rights and local community values.
6. **Respect for human dignity and safety:** Individual autonomy and agency should be upheld through a diverse and multidisciplinary design process. AI systems should be used to empower individuals and communities and enhance public engagement.

Sidewalk Labs' approach to responsible AI

Sidewalk Labs' next steps include convening an internal multidisciplinary team and incorporating the responsible AI assessment into its practices, while continuing to keep abreast of the research and policy landscape, and engaging with external experts and consultants on best practices.[20] The next sections briefly summarize these next steps.

[19] Contextual means that the backdrop of a situation is important to consider, as the norms of a particular context often change the considerations. Progressive means that the principles should be flexible and amenable to new developments and changes. Technology neutral means that the principles should apply broadly and not aim to favour or discriminate against any particular technology. These overarching principles allow the Responsible AI framework to be flexible and evolve as new technological capabilities emerge, norms evolve, and new harms become known.

[20] The responsible AI principles are inspired by leading international standards, such as the Declaration on Ethics and Data Protection in Artificial Intelligence, which has been signed by Canada's federal privacy commissioner. Sidewalk Labs' responsible AI principles also align with the OECD's principles for responsible stewardship of trustworthy AI in its "Recommendation of the Council on Artificial Intelligence," OECD Legal Instruments, 2019.

Convening a multidisciplinary team

Because AI systems are technologies with potentially wide-ranging policy, social, and ethical challenges, the effective implementation of responsible AI within an organization requires a multidisciplinary approach. This requires, among other things, a common language and understanding, which has been referred to as translating principles into practice. The Institute of Electrical and Electronics Engineers (IEEE), for example, recommends that principles be translated into norms and guidelines that are accessible to technicians.[21] Sidewalk Labs will convene an internal multidisciplinary team to put these principles into practice and regularly engage with experts and other relevant stakeholders.

Building upon existing AI assessment tools

In terms of existing assessment tools, Canada led the development of AI guiding principles and was the first country to release a national AI strategy.[22] In early 2018, people working for the Treasury Board of Canada Secretariat began publicly blogging about the need for public agencies to use algorithmic-impact assessments for automated systems to measure the system's potential impact.[23] In March 2019, the Treasury Board of Canada Secretariat launched its Directive on Automated Decision-Making to advise government departments on using AI in transparent and accountable ways.[24] The government's Algorithmic Impact Assessment (AIA) is meant to support the Directive on Automated Decision-Making. The AIA is a dynamic, electronic questionnaire, rather than a text-heavy form. Each answer is coded with scoring categories that add or remove risk to the proposed data activity. After the user fills out the questionnaire, they are provided with an impact level (1–4) and with instructions on which requirements apply to the data activities they have listed.[25] The AIA is being built in the open and is available online, via the project repository on GitHub,

[21] Global Initiative on Ethics of Autonomous and Intelligent Systems, "Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems," Institute of Electrical and Electronics Engineers, 2016.

[22] Tim Dutton, "An Overview of National AI Strategies," Medium, June 28, 2018. See also, "CIFAR Pan-Canadian Artificial Intelligence Strategy," Canadian Institute for Advanced Research.

[23] See Michael Karlin, "Towards Rules for Automation in Government," Medium, February 2, 2018; Karlin, "A Canadian Algorithmic Impact Assessment," March 18, 2018; and Karlin and Noel Corriveau, "The Government of Canada's Algorithmic Impact Assessment: Take Two," Medium, August 7, 2018. See also, Alex Campolo, Madelyn Sanfilippo, Meredith Whittaker, and Kate Crawford, "AI Now 2017 Report," AI Now, 2017; and Dillon Reisman, Jason Schultz, Crawford, and Whittaker, "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability," AI Now, April 2018.

[24] Treasury Board of Canada Secretariat, "Ensuring Responsible Use of Artificial Intelligence to Improve Government Services for Canadians," Government of Canada, March 4, 2019.

[25] Karlin and Corriveau, "The Government of Canada's Algorithmic Impact Assessment: Take Two," Medium, August 7, 2018.

for anyone to try out[26] and customize for their own use.[27] The AIA is also part of the OECD's Toolkit Navigator for Open Government.[28]

In addition to other publicly available toolkits and guides,[29] Sidewalk Labs will incorporate the AIA version available online into its data governance practices. Sidewalk Labs' privacy and data governance team has a lawyer who is a fellow in the Montreal AI Ethics Institute's inaugural fellowship program. Operationalizing the Responsible AI principles and exploring applied AI ethics is some of the work included in this fellowship.

Staying Current and Engaging with Experts

Artificial intelligence and machine learning are rapidly advancing technologies, bringing evergreen challenges and opportunities for policy, security, and responsible data use. Sidewalk Labs endeavours to keep abreast of the latest research and learnings in multiple ways. Sidewalk Labs stays current in AI ethics standard-setting initiatives and stays up-to-date with evolving and new research by engaging with researchers in the community, attending conferences and workshops, and reading academic papers.[30]

2.2.4 A note on data collection and minors

As PIPEDA does not distinguish between adults and children, Sidewalk Labs follows the OPC's recommendations provided in the tip sheet "Collecting from Kids? Ten Tips for Services Aimed at Children and Youth." The OPC views personal information relating to youth and children as particular sensitivity (especially the younger they are) and cautions that there may be unforeseen effects of surveillance technologies and children.[31] The OPC's "Guidelines for Obtaining Meaningful Consent" states that for children under the age of 13, consent must be obtained from a parent or guardian in most circumstances. Otherwise, consent can only be considered meaningful "if organizations have reasonably

[26] "Algorithmic Impact Assessment," Government of Canada (website), modified March 29, 2019.
[27] Algorithmic Impact Assessment project repository on GitHub.
[28] Observatory of Public Sector Innovation, OECD.
[29] See Section 4.5.2, Digital Rights, Ethics, and Tools for additional details.

[30] For example, some notable developments in responsible and ethical AI include: The IEEE's *Ethically Aligned Design;* research and publications by the AI Now Institute; working groups, research, and publications from the Future of Privacy Forum, such as "Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Models";publications by the Information Accountability Foundation, such as "Artificial Intelligence, Ethics and Enhanced Data Stewardship"; and various publications from the European Commission, such as "Building Trust in Human-Centric Artificial Intelligence."
[31] Research Group of the Office of the Privacy Commissioner, *Surveillance Technologies and Children*, October 2012.

taken into account [the child's] level of maturity in developing their consent processes and adapted them accordingly."[32] In addition, the OPC's "Collecting from Kids?" stresses the importance of designing services to avoid (to the extent possible) collecting personal information from minors (particularly younger children) and to avoid inadvertent collection.[33]

In the U.S., the Children's Online Privacy Protection Act ("COPPA") similarly restricts the collection of personal information from websites and online services that are directed to children under 13 or where the operator has actual knowledge that the user is under 13. The law generally requires companies to provide parents with notice and obtain their verifiable consent prior to collecting data in these cases.

Regardless of the jurisdiction, Sidewalk Labs recognizes that personal information from or about children deserves additional thought and care before it is collected and prior to any use or disclosure. Sidewalk Labs' RDUA specifically asks whether personal information from or about children under the age of 13 is being collected, used, or disclosed.[34]

---

[32] Office of the Privacy Commissioner, "Guidelines for Obtaining Meaningful Consent."
[33] Office of the Privacy Commissioner, "Collecting from Kids? Ten Tips for Services Aimed at Children and Youth."
[34] See section 2.2.2.3 for more details.

2.3 Inclusive and participatory planning and design

Sidewalk Labs has incorporated inclusive and participatory planning and design into its work in Toronto from the beginning. This section provides more information on these approaches, addressing questions raised by Waterfront Toronto, their Digital Strategy Advisory Panel, and the public. For more context on issues of ethics and inclusion more broadly in smart cities, as well as emerging practices in Canada and internationally, see Section 4 — Overview of Existing Policies and Approaches for Smart Cities and Digital Governance. Sidewalk Labs has taken inspiration from many of these approaches.

2.3.1 Why Inclusive and participatory planning and design approaches are needed

Sidewalk Labs believes that communities thrive when they are engaged and everyone has the equitable opportunity to participate in shaping the places, technologies, and policies around them.

The long-term success of a neighbourhood is predicated on its community members feeling a sense of ownership and belonging — of tangibly working together as stewards of their community. Sidewalk Labs is committed to planning for a future where community members can easily influence the decisions, spaces, and technologies that impact them, and where decision-making entities can be even more responsive to community input. Sidewalk Labs hopes that through appropriate use of digital tools, greater community dialogue, dedicated social infrastructure spaces, and supporting additional technology and design capacity in government, Sidewalk Labs can advance a virtuous cycle of participation and responsiveness where processes to create new systems, places, and digital tools will be not only consultatory, but also participatory and transparent.

2.3.2 Overview of Sidewalk Labs' processes

A co-creative, participatory design process must start with identifying problems, not solutions. It is insufficient to have already developed a solution and then solicit feedback from diverse groups on that solution. Design must be "with" and not "for"[35] the eventual users and stakeholders of a solution. Sidewalk Labs uses a range of methodologies to achieve a more inclusive and participatory approach to planning and design. Sidewalk Labs is not prescriptive in only using one process, but rather combines methods, such as design research and digital prototyping, to understand people's needs and co-develop solutions. This section describes a mix of approaches, principles, capacity building, and new tools that Sidewalk Labs has used to help make planning and design more inclusive.

[35] Laurenellen McCann, "The Myth of Everybody," *Organizer Sandbox*, July 31, 2014.

By using a participatory and planning design process upfront, the groundwork is set for a neighbourhood that will continue to adapt to the people who inhabit it. Sidewalk Labs is committed to continuing to work with local partners and community members to further these approaches should the next phases proceed, and also help foster the conditions for a place that is participatory with strong social capital.

Sidewalk Labs has built a team with deep expertise in civic technology and tech ethics, including former public servants who have built capacity for service design, data analytics, and digital product development in government, and designers who embed human-centred methods and accessibility into their practice.

Together, Sidewalk Labs' team is committed to working with community members, organizations, companies, and government to create inclusive places, technologies, and policies. This philosophy of inclusive, participatory co-creation — both in the planning and design phase and, importantly, as an ongoing way of working — has informed Sidewalk Labs' work to date and is further described in this section.

2.3.2.1 Prototyping

Prototyping is a critical tool for participatory design processes. Ideas for prototypes can come from many angles, such as directly from a community expressing a need, or experts evaluating an opportunity or governments prompting an area of inquiry. One of the most effective ways to collaboratively and quickly explore a solution is to make something tangible. Tangible could mean something made out of cardboard or a few lines of code. It could come about in an afternoon or in a couple of weeks or months. The key is that it is something more than words — something that allows people to meaningfully respond to an evolving concept in order to ground design in real human experiences and input.

Since its inception, Sidewalk Labs has had dedicated resources for prototyping, recognizing the critical importance of this method. Since beginning to work in Toronto, Sidewalk Labs has embarked on multiple prototyping projects with the local community, addressing questions from how to have increased agency over technologies surrounding us to ways to improve accessibility for all people. In all of these instances, Sidewalk Labs came with a problem definition but did not bring a specific solution. The prototype solutions emerged through the co-design process and are continuing to evolve. Sidewalk Labs is committed to continuing to use prototyping as a way to build with communities and stakeholders as the ideas for Quayside advance.

Sidewalk Labs uses its central office and experimental workspace in Toronto, 307 Lakeshore Blvd East, as a place for prototyping, which allows us to try ideas and receive ongoing feedback. Some highlights of projects initiated at the 307 site include the dynamic street, which started as indoor wooden pavers and has moved outdoors with higher fidelity materials, as well as a full-scale mock-up of an apartment unit made out of lightweight materials that allowed people to experience the space, imagine what living there would feel like, and give feedback.

Figure: Rumble Pavement Prototype During Co-designing Inclusive Cities Hackathon (Creative Commons License[36])

[36] Inclusive Design Research Centre. "Hackathon." Cities.Inclusive Design (blog). October 5, 2018. Accessed October 9, 2019. It is distributed under the Creative Commons Attribution 4.0 International license.

2.3.2.2 Inclusive usability testing through GRIT Toronto

To promote more equitable access and opportunity, ensuring inclusive design and addressing biases are critically important for new products and experiences that are part of urban environments. Sidewalk Labs is committed to intentionally reaching out to a truly diverse group of residents to participate and engage in the public planning processes. Historically, far too often, only a small non-representative group has shown up to formal public meetings.

For new civic technologies, this issue can be magnified, as the barriers to influence and participate in technology design are often greater. And to date, the technology industry itself has not been as diverse as the populations it serves.[37] As a result of these barriers, biases that directly impact people's everyday lives risk being baked into new technologies. For example, voice assistants struggle to successfully identify female voices and reinforce gender stereotypes[38] because the training data is heavily skewed towards male biases.

[37]S.M. West, M. Whittaker, K. Crawford, "Discriminating Systems: Gender, Race and Power in AI," AI Now Institute, 2019.

[38] UNESCO, EQUALS Skills Coalition, "I'd blush if I could: closing gender divides in digital skills through education," 2019.

In addition, traditionally, usability testing has taken the form of market research focus groups: a small group of people is recruited to come to an office during working hours to give feedback on a new technology. This method can result in narrow or even biased feedback.

Emerging from the civic tech community, there is an encouraging new approach for diverse groups to participate in technology design and mitigate bias, known as "Civic User Testing Groups." One of the earliest and most successful of these is the CUTgroup in Chicago. Blue Ridge Labs at the Robin Hood Foundation in New York City has also adapted this model to create Design Insight Group (DIG).

When Sidewalk Labs first began working in Toronto, some of its earliest meetings were with leaders in the local civic tech community. A key question Sidewalk Labs asked was, "If we could help support the growth of this community and its capacity to address key challenges, what might we do?" One of the first things mentioned was that the local community had long been looking to establish an initiative similar to CUTgroup in Chicago. Sidewalk Labs agreed that building local capacity for an additional group focused on inclusive usability testing would be impactful and was aligned with a shared interest in seeing enhanced capacity in Toronto to support equitable technology development.

To address this challenge, Code for Canada came forward with a vision for GRIT Toronto (Gathering Residents to Improve Technology), which Sidewalk Labs agreed to support with funding.

The GRIT program meets people of all digital skill levels, cultures, ages, and backgrounds where they are — in community spaces outside of working hours, for example — and incorporates their input into the creation of new digital services and products, helping to ensure these tools reflect the needs of the populations they are intended to support.

Launched in late 2018, the GRIT Toronto pilot has recruited over 350 residents from Toronto's 25 wards, representing a diversity of backgrounds, lived experiences, and technical skill levels. What unites participants is a desire to shape the digital products and services that could impact their lives and their city.

By seeding this program long before Quayside, it is already starting to benefit the Toronto tech ecosystem with six usability tests completed with GRIT testers to-date. It has been used by organizations from all sectors, including the City of Toronto, Transport Canada, Connected and Ample Labs. Sidewalk Labs also worked with GRIT to get feedback on prototypes for Collab and the Digital Transparency in the Public Realm system (see more in sections 2.3.3.1 and 2.3.2.4). In the long run, this initiative could help software developers across Toronto, including those in Quayside, collaborate with a broad range of community members and ensure that new digital solutions are built with neighbourhood needs in mind, becoming a business-as-usual way of working, rather than the exception.

Figure: DTPR User Testing Session with GRIT Toronto (Code for Canada)

2.3.2.3 Co-designing for accessibility from the start

To date, Sidewalk Labs has spent over 75 hours co-designing public amenities with over 200 members of the disability and accessibility communities in Toronto, including professional designers, advocates, and especially people who self-identify as having lived experience of disability. As a result of these sessions, Sidewalk Labs has drafted 22 accessibility principles and incorporated over 100 recommendations for improvement in their ideas.

One of the very first partnerships Sidewalk Labs established in Toronto was with OCAD University's Inclusive Design Research Centre (IDRC), to lead a series of co-design workshops with accessibility community members to inform the Master Innovation and Development Plan (MIDP). Each co-design session had a specific theme, such as "feedback and engagement," "dynamic streets," and "threshold moments." In each session, participants shared their urban experiences, identified barriers in the community, brainstormed, and prototyped ideas to address those issues. The IDRC team processed the collected notes, documents, drawings, and prototypes and built an openly shared collection of ideas generated in each of these sessions. IDRC and the Sidewalk Labs team[39] worked together to select eight ideas from the three sessions to be tested and mocked up during a hackathon, including developing a detailed project description for each.

Selection of the final ideas was based on how feasible it would be to implement a prototype within a day, how much support there was in the co-design sessions, and whether the idea was aligned with the concepts envisioned for the MIDP. The final eight ideas selected for the hackathon included:

- *Audible or haptic incoming traffic warnings at intersections* that let people know about someone approaching on a bicycle or car if they are preparing to cross the street or are currently in the street;
- *A tranquil refuge* in public settings with information screens for transit, food, health, and emergency services;
- *Construction advisory beacon messages* to inform people of construction impediments in their path;
- *Self-driving cars for sub-emergency medical visits* that act as an alternative to ambulances for non-emergency medical transport;
- *An augmented reality park feedback experience* to provide an easy way to give feedback to responsible parties;
- *Rumble pavement* to indicate where the sidewalk ends and bike/vehicular traffic starts;
- *A tactile sidewalk wayfinding strip* with geolocation for adjusting crossing times; and

[39] IRDC participants were Sepideh Shahi, Simon Bates, Colin Clark, Lisa Liskovoi, Gillian Szeto, and Syeda Hassany, with consultation from Jutta Treviranus. Sidewalk Labs team members were Samara Trilling and Logan MacDonald.

- *An AI floor describer* that describes and provides navigation assistance for the internal space of a building.

Using these ideas, teams of engineers, product designers, and community members worked together to build prototypes at the hackathon. The final products were tested and presented to the larger group, and the prize-winning ideas were shared with the public at Sidewalk Labs' Open Access event at the 307 offices.

Embedded co-design workshops

To ensure that the voices of people who could not travel or take time off work for a co-design session were not left out, the IDRC team ran a second stream of co-design workshops within the community. The team invited different organizations, including Plant a Home, Houselink, the Dream Team, the Canadian Helen Keller Centre, Parkdale Activity-Recreation Centre, Community Living Ontario, and Deaf Culture Centre, as well as elementary school classes with grade 3, 5, and 6 students, to run their own co-design activities with their members and provided them with support to facilitate those workshops.

This stream of work enabled the IDRC team to reach out to the broader community in Toronto and meet people who have lived experience of disability and marginalization (including members of the deaf and deafblind community and people with lived experience of homelessness and developmental disabilities) where they are. The notes and results from these co-design sessions were posted online at the Inclusive Design Institute blog; the Sidewalk Labs team took direct feedback from these notes and incorporated it into the Accessibility Principles.

Contribution to the Sidewalk Labs' Accessibility Principles

Sidewalk Labs has developed a core set of Accessibility Principles grouped into three main areas — General Accessibility, Physical Accessibility, and Digital Accessibility — to guide the work as Sidewalk Labs plans Quayside. Sidewalk Labs wrote a first draft of the principles, shown in the table on the following page, informed by conversations with experts and those with lived experience with disability. In the co-design workshops and hackathon, participants provided feedback and direct edits to the draft principles. Rooted in co-creation, the Accessibility Principles will continue to adapt and expand to incorporate input and additions from the community. Anyone is welcome to email accessibility@sidewalklabs.com with proposed additions. All suggestions are noted and the next time Sidewalk Labs publishes a more specific version of the principles (anticipated in January 2020), new ideas will be incorporated. When the next phase of master planning commences, following approval of the MIDP, Sidewalk Labs anticipates creating a working group consisting of people with disabilities who has stewardship of these principles and direct input into the design process.

Sidewalk Labs' Draft Accessibility Principles

General Accessibility

1. Enable experiences that were not possible before.
2. Do "nothing about us without us."
3. Make infrastructure simple, durable, reliable, and easily maintainable.
4. Design predictable, intuitive experiences. For example, place amenities like public washrooms, elevators, and reception desks in consistent places across buildings.
5. Futureproof by default.
6. Make the accessible path the most convenient, delightful path.

Physical Accessibility

1. Build for wheels.
2. Enable wayfinding in multiple formats. For example, plan for visual signage to have an audio or tactile counterpart.
3. Eliminate barriers and friction.
4. Promote relaxation and recovery.
5. Enable personal assistive technology, with a focus on easy to access, low-cost technologies.
6. Go beyond legal requirements.
7. Enable flexibility and customization. For example, provide multiple options for height of fixtures by default and design street furniture that's easy for people to move or alter to suit their needs.

Digital Accessibility

1. Provide information in multiple, easily accessible formats and languages.
2. Support multiple input modalities to all digital experiences.
3. Preserve privacy and support fairness in machine learning.
4. Allow an easy way to give feedback on digital tools.
5. Use common standards for messages in audio wayfinding features.
6. Provide a recommended, free option that is also open to third-party alternatives wherever technology is necessary to interact with a key service.
7. Use the best digital accessibility standards available and set new, higher standards wherever possible.

Influence on the Quayside proposal

Below is a series of concrete ways that the principles, created through the co-design process, influenced the proposed plan for Quayside. This list includes both ideas that first surfaced in the co-design sessions, as well as features of concepts Sidewalk Labs proposed that evolved based on feedback. This list is not meant to be exhaustive of all ideas expressed in the co-design sessions.

- **Wayfinding beacons:** Beacons are small objects, about the size of Post-it Notes, that emit signals that can be picked up by smartphones or other Bluetooth-enabled devices. Beacons can broadcast navigational information about the environment that is especially useful to people who are blind or partially sighted — for example, that an accessible ramp is located to the right of the steps. It was noted that this technology would be particularly useful during construction or any other temporary changes on the streets. In Quayside, beacons would enable the use of BlindSquare and other wayfinding apps as part of the default street-level experience.

- **Sidewalk width:** All thoroughfares in Quayside are planned to have at least enough room for two people using mobility devices (wheelchairs, scooters, white canes) to ride or travel side by side in each direction or for two people to sign while walking. Even more room would be provided wherever possible.

- **Curbless streets:** In Quayside, instead of a vertical step separating the vehicle right of way from pedestrian paths, tactile indicators would indicate the line between pedestrian-only areas and spaces shared between pedestrians, bikes, and low-speed vehicles. In addition to tactile indications, participants also requested audio and visual cues to be warned about approaching streets.

- **Accessible self-driving rides:** One of the proposals that participants in co-design sessions were most excited about was an accessible fleet of self-driving vehicles to help people get around the neighbourhood safely and independently. Ideas included the ability to hail a self-driving vehicle using a voice assistant or soft-touch button according to personal preference, as well as visual or audio cues that could guide people to their vehicles (imagine an augmented-reality thick green line on the ground to follow, paired with a unique audio identifier for a vehicle). The potential for self-driving vehicles to expand mobility and become part of a personal support network speaks to the essence of what accessibility is all about: making people feel at home in their city. Sidewalk Labs commits to working with self-driving vehicle fleets to make calling, riding, and getting picked up and dropped off easy and accessible. All streets — even pedestrian laneways — would be designed to allow accessible self-driving vehicles.

- **Seamless building thresholds:** Getting through a door with an armful of packages can be difficult for anyone — and harder still for people who are using a wheelchair, partially sighted, or experiencing reduced dexterity. A co-design session focused on improving these "threshold" moments: transitioning through a door into a home, between floors in an office building, or past a badged access point.

  The difficulty of these threshold moments can be eased or eliminated by applying simple technologies, like automatic doors. Where access control is necessary, doors can have a contactless scanner for a card, fob, or phone. Participants in the co-design session highlighted these as useful innovations, particularly when they are all knit together, such that a single access device can open doors, call elevators, negotiate access controls, and request street crossings.

Sidewalk Labs commits to a design principle that "fewer doors are better," which is captured under Accessibility Principles #3 (eliminate barriers and friction). When doors are necessary, designs should preference sliding automatic doors over button-controlled doors.

- **Infrastructure that reports back:** What causes a frustrating delay for some commuters can create an arduous ordeal for others — the wheelchair user faced with a broken elevator at their transit station; the youth with cognitive disabilities whose bus route unexpectedly changes; the visually impaired senior whose daily walk is interrupted by roadwork.

  But imagine if people could be alerted immediately when station infrastructure breaks down, when transit service gets delayed or detoured, or when street maintenance occurs, and be instantly re-routed via a smartphone or wearable device. Participants at a Sidewalk Labs accessibility hackathon prototyped just such a technology, which would allow visually impaired pedestrians using the BlindSquare app to be safely guided around construction sites.

  Sidewalk Labs commits to exploring infrastructure capable of reporting itself as broken and to working with existing navigation tools to ensure every journey in Quayside is accessible, safe, and convenient for all.

Inclusive cities co-design toolkit

Importantly, the work from this prototyping in public was not only principles specific to the Sidewalk Labs proposal, but also a resource to further build capacity in the smart-city design community more broadly. IDRC has developed an open source co-design toolkit to serve as a guide in planning and facilitating any group or community who aims to practice co-design in a city context.[40] The toolkit contains perspectives on co-design, reflections from experiences in planning and facilitating co-design sessions, and tools that can be used for planning and self-evaluating performance and outcomes. This is an open resource that the community can contribute to and adapt to match their needs.

Another result of this partnership was the launch of the "Co-designing Inclusive Cities" website, which includes an open platform for community members to share their insights, experiences, and research about inclusive and smart cities. It also incorporates open and active resources for executing co-design that will continue to be developed by the community based on their emerging needs.

[40] Please see the IDRC's co-design process resources page for more details.

Accessibility at the forefront

By no means is Sidewalk Labs' work in the accessibility sector done. Sidewalk Labs has hired an accessibility consultant in Toronto and has consulted with the Canadian National Institute for the Blind (CNIB) Foundation on designing Sidewalk Labs' wayfinding and publicly available technology systems to be open to all. Sidewalk Labs has made the [Master Innovation and Development Plan]() for Toronto accessible, as well as this Digital Innovation Appendix. Sidewalk Labs hopes to see the breakdown of systemic barriers that often make it harder than it should be for members of the community to easily enjoy all aspects of life in Toronto.

2.3.2.4 Prototyping Digital Transparency in the Public Realm (DTPR)

It is no mystery that data collection and privacy have been significant topics of discussion surrounding the Quayside project. Sidewalk Labs believes these are some of the most important social and ethical discussions of our time, and welcomes and encourages the dialogue. For this reason, Sidewalk Labs embarked on a public prototyping project, [Digital Transparency in the Public Realm]() (DTPR), to help move forward co-created solutions that have the goal of providing communities with greater agency over data collection in the public realm.

The digital technology embedded around us today is often invisible. On any one urban excursion (your commute, perhaps), you could encounter security cameras, traffic cameras, transit card readers, bike lane counters, Wi-Fi access points, occupancy sensors that open doors — potentially all on the same block.

Many of these new innovations are exciting. After all, they can make public spaces more comfortable, responsive, and efficient. But there is little transparency about what data these technologies are collecting, by whom, and for what purposes. Signage that does appear in the public realm often contains either small snippets, which give no indication of how to follow up or ask more questions, or multiple paragraphs of dense text. And in many instances, putting up devices that collect data without notice has become normalized.

In response, Sidewalk Labs began to prompt, "What could a more transparent system look like?" "How might there be a more democratic process to determine whether or not a new digital system ought to be implemented?" "How would people receive notice?" "How would people inform the solution and implementation?" In an initial landscape scan for informing on digital technology, Sidewalk Labs found that a movement towards digital transparency can help by providing easy-to-understand language that clearly explains data and privacy implications of digital technologies.

Design languages already help generate understanding around complex issues every day. Nutrition labels help demystify the content of foods people consume; Creative Commons logos quickly convey key elements of their copyright licenses; and universal symbols help us effectively navigate through transportation hubs anywhere in the world. Digital transparency can empower users to meaningfully engage in what is fast-becoming a critical conversation of our time. And, equally important, as shown through research, transparency can nudge both users and data collectors towards best practices.

With initiatives such as Boston's Beta Blocks and Transport for London's phone tracking pilot, cities have already taken important first steps by posting clear signage whenever they employ digital technologies in the public realm. Similarly, European Union parliamentary directive on personal data privacy and U.S regulatory guidance on telecommunication and privacy have called for the development of icons to communicate key terms and concepts around online privacy in a clear and digestible manner. Researchers have also noted the importance of transparency in data practices "beyond the data protection law framework: data practices that are not visible in some manner are not regulable."[41]

Sidewalk Labs believes that people should know how and why data is being collected and used in the public realm, and that design and technology can meaningfully facilitate this understanding. For these reasons, Sidewalk Labs embarked on a collaborative project to imagine what digital transparency in the public realm could be; a summary of the co-design process and outcomes is described below, and you can find additional documentation and outcomes on the Designing for Digital Transparency in the Public Realm website.

The Digital Transparency in the Public Realm Co-Design Process

Together with more than 100 participants from several cities, Sidewalk Labs sketched, debated, iterated, and prototyped a visual language that offers a quick way to understand the technology around us — and a means to easily learn more.

Step 1: Define a problem, not a solution

Sidewalk Labs initially created a problem statement, which did not have a pre-determined solution: ***How might we make digital technologies in the city more transparent and increase community agency?***

Step 2: Create a framework

To guide our process, Sidewalk Labs chose the following design principles:

- **Provide transparency:** Help people increase their awareness of how digital technology in the public realm works and give them avenues to learn more or follow up.
- **Focus on outcomes, not outputs:** More signs are often not the answer. As visual noise increases, it becomes harder for meaningful information to break through. Sidewalk Labs

[41] Lisa M. Austin and David Lie, University of Toronto, Department of Electrical and Computer Engineering 94 N.Y.U. L. Rev. (forthcoming 2019).

wants to develop a way to know whether signage or channels are working for people; that feedback is needed to improve designs over time.

- **Offer communication and utility:** Beyond wanting to understand what data is being collected around them, people also might want to know how to make better use of their environments. Signage should also be a starting point to help people better navigate and utilize their surroundings.
- **Blend digital and physical:** Sidewalk Labs is in a unique position to consider how people move from a digital to a physical space and back. This transition should feel useful and coherent.
- **Design for adaptation:** Sidewalk Labs knows this is just a first take, and intends for others to build on this work.

Step 3: Reach out

To create something successful, something that would be adopted by others and evolve over time, Sidewalk Labs needed the input and participation of a broad range of people: a cross-cutting set of experts from design, data privacy, and the public realm were brought together in a series of three co-design sessions.

A week later a session was held in London as part of The GovLab's Data Stewards Camp, followed by a half day co-design session in San Francisco at the World Economic Forum's Centre for the Fourth Industrial Revolution.

Step 4: Ask a question

Within the co-design process, Sidewalk Labs asked participants to consider the questions and concerns they have with existing digital technologies in the public realm, and note them on cards. Many people wanted to know if a technology could identify them. Others were concerned about where the data was stored and for how long. These questions informed the second half of the session: identifying patterns and themes.

Step 5: Find the patterns

With hundreds of questions and concerns to address, it is hard to know what takes priority. By grouping themes together, common questions emerge. Out of these sessions five themes arose:

- Purpose & Benefit
- Technology & Privacy
- Data & Processing
- Access & Storage
- Feedback & Follow-up

While research synthesis can inform design, it is closer to an art than a science. Because of this, Sidewalk Labs has made all materials from the workshops publicly accessible, and encourages others to find more useful patterns from the questions people surfaced.

Step 6: Tell a story

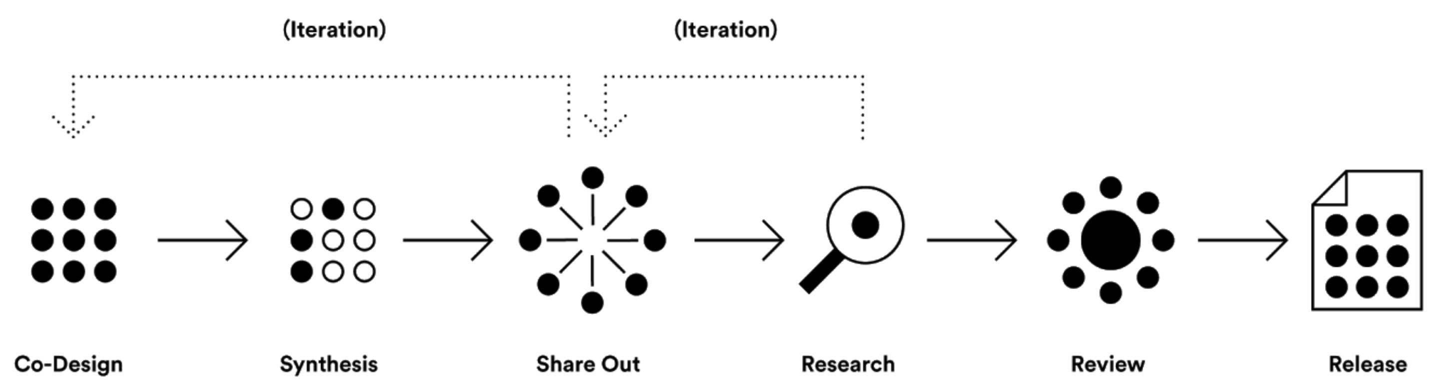
After themes were identified, participants were prompted to tell a compelling story to answer the question: How can someone see a sign, get information, or participate with a technology? This activity generated a wide variety of ideas; people drew big totems and tiny stickers; they envisioned colour-changing walls and imagined sounds that correspond to different areas.

Step 7: See the signs

The teams then turned to the question of signs. Like a traffic sign, a digital technology sign needs to be legible and unambiguous. Like the sign for baggage, it needs to be simple and understandable by people all around the world. Like the Creative Commons symbols, it needs to convey complex concepts.

Participants drew lots of icons; each group pared them down to a final set. Many of the icons were taken as is and cleaned up. Other icons became part of a series that tell a story about a type of technology.

Figure: The Co-Design Process Approach



Step 8: Open the digital door

Finally, participants imagined how they might extend the sign into the digital world. There is so much to uncover about digital technology — what data it collects, what sensors it uses, what its governance structure is — but this cannot all be said on a sign. Moreover, these workshops clearly demonstrated that different people want to know different kinds of information.

QR codes, URLs, and augmented reality played prominently in many people's stories. These digital tools allow people to move from the physical world to an online channel, ask a question, file a complaint, or search out additional information.

Step 9: Share and listen

After a number of co-design sessions, a strong set of icons emerged. Sidewalk Labs then arranged a usability testing session with GRIT Toronto, a program by Code for Canada for inclusive usability testing described in section 2.3.2.2, where the concepts were shared with a group of 12 diverse Torontonians.

Participants urged us to simplify the signage and offload complexities to the digital channel. Specifically, people wanted to see the logo of the accountable organization and the purpose of the sensor, and to know if they personally were identifiable from the technology. They also needed a way to learn more and give feedback about the technology.

The co-design sessions and usability research were not the only ways Sidewalk Labs reached out to a broader community. Input was also solicited during co-design activities at civic tech events, such as CivicTech Toronto meetups and BetaNYC's School of Data conference. Sidewalk Labs also hosted four live video share outs, where all previous participants were invited to join a video chat to see how the project had evolved and provide feedback (you can see the past share-out sessions here).

Figure: Digital Transparency in the Public Realm Co-Design Session

The first co-design session was held at Sidewalk Labs' 307 workspace in Toronto. Projects By IF helped facilitate, along with Puncture Design and other members of the Toronto design community.

The result

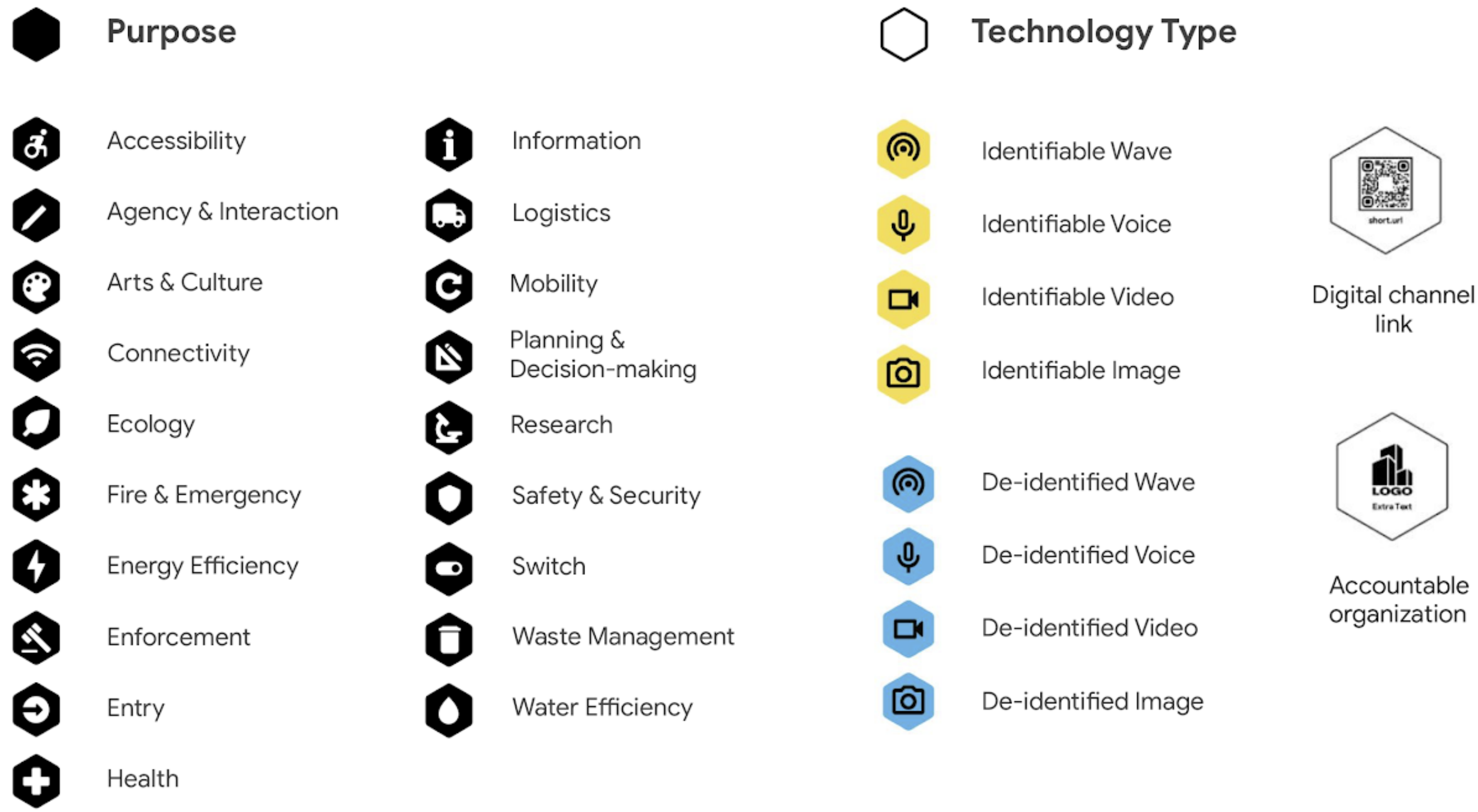
The DTPR project combined creativity from co-design sessions, considerations of legal requirements for the collection of personal information, and user-centric research sessions to design a visual language and digital channel. Sidewalk Labs released the prototype on March 17, 2019, including all workshop activities and materials, publicly and freely available for others to adopt, use and build upon, in order to advance digital literacy and help people understand digital infrastructure in the public realm.

There were four major outputs of the project: icons, a signage system, and a digital channel for communication that, together, help visualize and convey a taxonomy of key concepts.

The signage system for the public realm answers the most important questions identified through the co-design and user research process: the purpose, the accountable entity, and whether the technology collects identifiable information. As shown in the figure on the page above, in the final visual language one hexagon conveys the purpose of the technology; another, the logo of the entity responsible for the technology; and a third contains a QR code that takes people to a digital channel where they can learn more. In situations where identifying information is collected, a privacy-related coloured hexagon would also be displayed.

The visual system for DTPR, see figure on the following page, includes icons denoting purpose (in black), technology type (blue for de-identified, yellow for identifiable), the accountable organization, and a link to a digital channel to learn more.

Figure: DTPR Icons and Digital Tool (Creative Commons License[42])



[42] Digital Transparency in the Public Realm project contributors. "Digital Transparency in the Public Realm: Icon Definitions." Accessed October 9, 2019. https://github.com/sidewalklabs/dtpr. The Digital Transparency in the Public Realm Icons and Taxonomy are licensed by the Digital Transparency in the Public Realm project contributors under the Creative Commons Attribution 4.0 International (CC BY 4.0) License. Portions of the icons include elements of, or are derived from, the Material icons which are licensed under Apache License 2.0. For additional details, please refer to the information for the open standard on Github.

The public space limitations on feasibly posting lengthy privacy notices meant that creating the digital channel for individuals to easily access additional information — such as whether and with whom that information is being shared and how data is processed — was of particular importance.

During the design of the icons, Sidewalk Labs also considered how the DTPR project would meet the Office of the Privacy Commissioner (OPC) of Canada's guidelines for meaningful consent.[43] The OPC issued seven guidelines that Sidewalk Labs believes this DTPR system begins to address. These guidelines emphasize how important it is for organizations to inform individuals of their privacy practices in an understandable way. Organizations must balance transparency of key elements, while allowing individuals to control the level of detail they get and when. The OPC also stresses the user's perspective. Organizations are encouraged to be creative, design innovative solutions, and provide an interactive and dynamic process for consent and for individuals to follow up with more questions.

The DTPR project is an attempt to further the conversation and address issues of notice and transparency more broadly. While this project does not address all of the issues of consent around data collection in public spaces, Sidewalk Labs believes it is a meaningful step forward. Sidewalk Labs did not limit the project to personal information only, as there needs to be greater transparency and education regarding all the ways digital technology is used in the public realm. Sidewalk Labs believes digital transparency can empower users to meaningfully engage in what is fast-becoming a critical conversation of our time. And, equally important, transparency can nudge both users and data collectors towards best practices.

2.3.3 Supporting the growth of civic technology tools

Sidewalk Labs recognizes the important role digital tools can play in supporting civic engagement. Civic technology can provide ways for more people to participate in their communities, allow organizations to have better insight into decisions, and improve processes that may have previously only been manual or in person. Over the past two years, Sidewalk Labs has built prototypes in this domain, aiming to support existing civic innovators in their work. The long-term stewardship of these tools is being actively worked on in partnership with the civic organizations that were part of the prototyping from the beginning. None of these tools would be required for use in Quayside — the choice to use any civic tools would be at the complete discretion of government and local community organizations.

[43] The Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent," May 2018.

2.3.3.1 Collab: Digital tools as a support for inclusive community participation

While there are many reasons for the decline in civic participation, one contributing factor is a lack of transparency. It is not always clear how input will be used or if the organizations charged with community decisions are able to receive and act on feedback. Another factor is that people may face barriers to accessing opportunities to participate; even those who do participate may not always feel sufficiently knowledgeable on certain issues to meaningfully contribute.

To help address these challenges, governments and companies around the world have begun building tools that leverage technology to make participation more informed, transparent, and relevant to people's daily lives. The Digital Innovation Appendix highlights some of these approaches in section 4.5.4 — Inclusive and participatory practices.

These examples are part of a promising trajectory towards inclusive digital participation that could enable more people to better engage with and enhance the places they live, work, and visit. Sidewalk Labs' hope is that these tools kickstart a virtuous cycle: the more community members feel empowered to shape their communities, the more they will participate. The more they participate, the more decision makers can be more inclusive and responsive to community voices, inspiring more community members to participate. And so on.

There are many ways that digital tools — in coordination with strong in-person and more traditional approaches — can unlock greater civic participation. One promising approach is leveraging technology to bring transparency into processes and decision points that could allow community members to better understand the issues at hand, provide input, and, hopefully, feel satisfied that their voices have been heard. Sidewalk Labs believes that by providing community members with an informed, nuanced understanding of the required trade-offs of a decision, digital tools could even encourage more decisions that put collective good ahead of individual interests.

In scanning the landscape of technologies that support local decision-making, Sidewalk Labs was unable to identify a tool focused explicitly on making trade-offs transparent. Informed by this opportunity, Sidewalk Labs decided to create a prototype — one small contribution towards a more civically engaged urban future — through a digital tool that could support communities hoping to increase participation and make more inclusive, collaborative decisions.

Prototyping for inclusive participation through Collab

Sidewalk Labs selected Digital Public Square as a prototyping partner through a competitive request for proposals from a mix of United States- and Canadian-based organizations. Digital Public Square, a non-profit spun out of the University of Toronto, has a mission to rethink and redesign the way technology is used to support communities worldwide by finding ways for people to engage in healthy debate, share knowledge, and co-create solutions to their most pressing challenges.

Figure: Collab Prototype at 307

Sidewalk Labs began the project by analyzing different parts of the Quayside design to see what would be best suited for participation and adaptability once built, and which of these areas offer learnings that can best support existing neighbourhoods. Digital Public Square also conducted an initial round of research with Toronto-based neighbourhood associations to better understand how they invite participation in their communities today.

As a first use case, Sidewalk Labs and Digital Public Square created a prototype, now called Collab, that allows community members to propose their choices for events in public spaces and then walks them through the trade-offs associated with each proposal and how their individual choices impact the community. For example, a farmers market provides fresh produce and draws a lot of foot traffic, but the space may then feel too congested for a community picnic.

Privacy by design

Sidewalk Labs and Digital Public Square designed for privacy to be the default in the prototype. While many participatory planning tools require personal information, such as an email address, Collab was designed so it can be used without people submitting any information about themselves, as prototype development does not require this information. Sidewalk Labs is also transparent about the data Collab is collecting and how it is being used in Collab's Privacy Policy and Responsible Data Use Assessment (RDUA).

Inclusive feedback

To ensure the team was receiving inclusive feedback on how Collab could serve a diverse range of community members, Code for Canada's GRIT Toronto, described in the section above, was enlisted to convene ten participants — each from a different ward and representing a range of ages, backgrounds, and tech skill levels. GRIT gathered input on content, artwork, and navigation that Sidewalk Labs and Digital Public Square were able to implement within the prototype. (Learn more about this process in Code for Canada's post about testing Collab.)

The result is a prototype that aims to make the decision-making framework of public programming and all community inputs transparent and legible for all users. The team's hope is that Collab users will not only understand where their individual contributions fit into a community decision, but will also feel more trust in civic processes overall. The prototype is available to try at collab.sidewalklabs.com.

How might a community use Collab to influence decisions?

Collab engages community members in local decisions, shaping their neighbourhood through a transparent process that reveals the decision-making framework and all community inputs. Sidewalk Labs knows that digital technology alone is not enough for fostering quality, equitable local decision-making. In-person interactions and the overall governance of a place are the foundation. However, as has been shown through many successful digital government initiatives, technology can be thoughtfully integrated to enable greater transparency and participation.

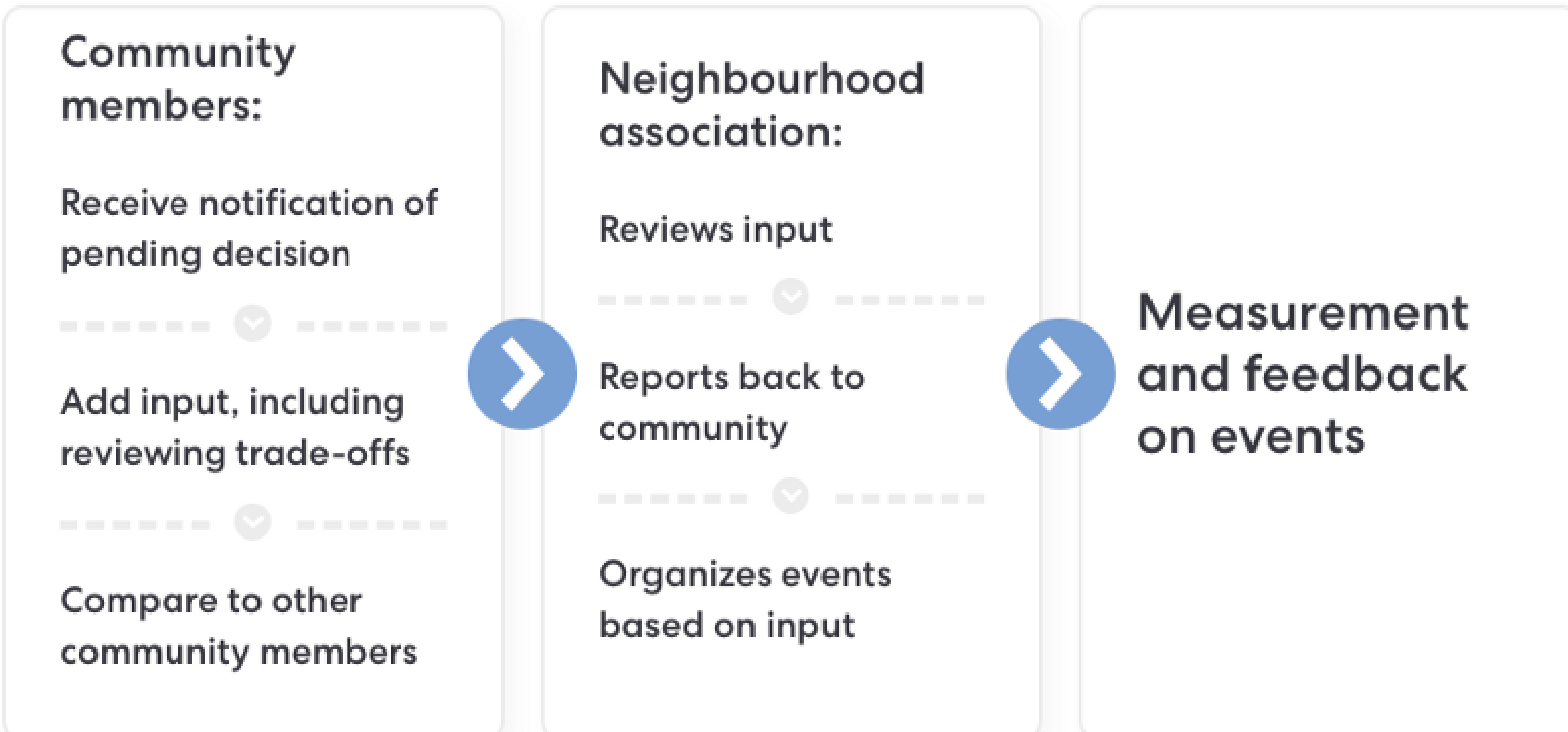
In the future, Collab could be used by organizations, such as a neighbourhood association, business improvement area, or public-space non-profit, to make more inclusive community decisions. Imagine a community planning an upcoming winter festival. Community members could receive a digital notification of a pending decision, add their input while considering the trade-offs, and transparently compare their choices to those of others in the community. The neighbourhood association could use the input to inform its decision, report the program and schedule to the community, and use other tools to receive feedback and measure the success of the event.

This is just one possible scenario. No matter how Collab develops or evolves with community input, the team's hope is that, with technologies like Collab serving as easy entryways to engagement, everyone can be activated to shape and become true stewards of our communities.

If government agencies and civil society believe that Collab is beneficial, they can choose to use it. Sidewalk Labs is optimistic that there is benefit, as we have seen multiple organizations express interest, including several community councils, a LGBTQIA+ community foundation, a community organizer, a broadband provider, an urban planning firm, and a number of government agencies looking for support in their work to bring diverse voices into their advocacy process.

It is also worth noting that the procurement process for governments considering digital tools like Collab to inform decision-making would follow established procurement procedures. There would be no requirement for government to use Collab, nor any unique treatment given to Collab in a competitive process.

Figure: How Might a Community use Collab to Influence Decisions?



Sharing prototype learning

Ahead of launching the Collab prototype, Sidewalk Labs and Digital Public Square established baseline key performance indicators to understand its success. An evaluation of the first three months (May-August 2019) of data from the prototype was recently executed. Per Sidewalk Labs' Privacy Policy and RDUA, Collab uses only non-identifying platform analytics to measure performance, along with anonymized Google Analytics for top-level traffic source data.

Table: Key Findings from Collab Prototype (Data as of: 15/08/19)

Visits	2,835 total visits to the website (Target: 5,000)
Plaza designs	852 completed plaza designs at 30% conversion (Target: 20% conversion) Certain events prove more popular than others overall: ● Just over half of all people chose a farmers market in their plaza ● Over a third also chose live music or community picnic (out of a total of nine event options plus "create your own") After learning trade-offs and benefits for the community, many users went back and changed their answers.
Events	159 user-generated events at 19% conversion (Target: 10% conversion) Sample events included: ● Zen garden ● Balloon animals ● Neighbourhood dance-off ● Movie night ● Dog park ● Bike repair workshop
Demographics	275 demographic entries at 32% conversion (Target: 10% conversion) Based on this optional demographic information, there was a diverse user base, but Sidewalk Labs believes the main audience was urban enthusiasts.

Traffic sources	70.7% direct, 20.6% referral, 5.2% organic search, 4.5% social
Feedback	31 feedback messages (Target: 20 messages) Several users were excited to see how the tool can be used for other forms of community planning. One suggested that the tool could be paired with a rendering engine so users can virtually experience different neighbourhood planning options. A number of users requested options to roll out single-use versions of the tool for quick debates (with options to swap in custom graphics or visuals from a royalty-free-use-system.) Example topics suggested by people who used Collab: ● Urban planning ● Park design ● Activities for kids ● Street art ● Community budgets ● Volunteer opportunities in local neighbourhood projects ● Programming in community centres ● Community dispute resolution

2.3.3.2 Helping communities measure impact and drive change through CommonSpace

The national public space charity Park People was one of the first groups Sidewalk Labs met in Toronto. After the work on the "North of the Water" study (described in further detail in Section 2.3.4.1), Sidewalk Labs learned about the work Park People was leading with the Public Space Incubator, and asked if there were any challenges they were facing to see if there might be opportunities to help support this important initiative.

A key issue Park People raised was around the methods for measuring the impact of public space prototypes. Urbanists have a long tradition of using data to champion the reform of public space. In the 1960s, Jan Gehl's careful documentation of people standing, sitting, waiting, and talking along Strøget, Copenhagen's main thoroughfare, made the case for pedestrianizing the street, and helped to transform the city into a global leader for public space.[44] More recently, after conducting public-life studies to inform TOcore, Toronto's new plan for downtown, the City of Toronto has begun to integrate the practice of public-life studies into their public-realm improvement and capital-planning processes. And Park People has been integrally involved in these efforts.[45]

But the tools used to study public space have changed very little since they were developed in the 1960s. Today, many managers of public space and community advocates still rely on clipboards or manual clickers to count the number of people in a space and classify what they are doing. This method results in a substantial portion of a study's budget being devoted to digitizing the paper sheets, which is costly and often also introduces mistakes.

To address this problem, Sidewalk Labs proposed developing a digital prototype, now called CommonSpace, that makes it easier for community groups to collect reliable data on how people use public spaces. To ensure CommonSpace would conform to established open data standards, Sidewalk Labs worked with the non-profit Gehl Institute that developed the "Public Life Data Protocol," which aims to establish a common format for the collection and storage of such data.

In fall 2018, Sidewalk Labs worked with Park People and the Thorncliffe Park Women's Committee to conduct a field test of CommonSpace in R.V. Burgess Park. The Thorncliffe Park Women's Committee was funded by Park People's Public

[44] Gehl: Making Cities for People. "Gehl Story: Copenhagen as the Laboratory."

[45] Gehl Studio and Public Work. 2018. Downtown Parks and Public Realm Plan: Public Space Public Life Study. Toronto: City of Toronto.

Space Incubator to further develop a community café and market the Committee had started at the park. The test concentrated on using CommonSpace to measure how increased programming and better café seating changed how people used the space. Local youth and other residents collected data on how many people came to the park and how the new chairs and programming affected what they did there.

The community team found that the park saw a massive, 365 percent spike in visitors on programming days, and that the activity was far more social, with large increases in people coming in groups, meeting new people, and staying into the evening. The study not only gathered valuable data that can help the Thorncliffe Park Women's Committee understand and communicate the impact of its efforts, but also enabled participants to learn about their community while changing how they think about the park.[46]

CommonSpace's code is open-source and based on an open-data standard, so it can be further developed by users in Toronto and around the world to gather the data needed to improve public life in their communities. The data gathered about people in public spaces is selected from fields defined by the Public Life Data Protocol schema — typically, it includes observed age, gender, posture (such as sitting, lying down, standing), and activity (such as commercial, consuming, conversing). There is also a free-text entry field for additional notes when required. There is no audio, image, or video data collected and surveyors are reminded to not record personally identifying information about the people they are observing.

Figure: Data Collection Volunteers for the CommonSpace Pilot in R.V. Burgess Park

[46] Park People. 2018. "What we learned from testing a new public life study tool." December 14, 2018.

2.3.4 Inclusive and participatory social infrastructure

While we now can use technology to connect with one another, it does not replace the need for face-to-face human connection. Strong community connections build social capital and are key to building thriving, healthy neighbourhoods. In fact, as digital technologies have become more a part of our lives, the importance of face-to-face interaction for democracy and social cohesion has grown. Recognizing this, a key approach to Sidewalk Labs' planning has been to prioritize social infrastructure — the physical spaces and services that shape interactions, organize communities, and provide the supports necessary to thrive in everyday life. Whatever its form — library, park, art gallery, health centre, weekly meetup — social infrastructure ties together communities and helps people reach their highest potential.

"When social infrastructure is robust, it fosters contact, mutual support, and collaboration among friends and neighbours; when degraded, it inhibits social activity, leaving families and individuals to fend for themselves...People forge bonds in places that have healthy social infrastructures — not because they set out to build community, but because when people engage in sustained, recurrent interaction, particularly while doing things they enjoy, relationships inevitably grow."

- Eric Klinenberg[47]

While many developments leave these considerations to the end and provide only the minimum required by government, Sidewalk Labs believes in weaving social infrastructure in from the beginning of planning to ensure that inclusive, participatory spaces are part of the fabric of the place and can contribute to a thriving community.

The Quayside proposal and planning process prioritizes the integration of thoughtful social infrastructure spaces with digital compliments in both outdoor and indoor areas, including parks and open space as well as the ground-floor spaces — the shops and cafés and daycare centres that enliven our sidewalks. While thoughtful integration of technology innovations can help to enable and enhance these connections, they do not replace them.

---

[47] Eric Klinenberg. Palaces for the People: How Social Infrastructure Can Help Fight Inequality, Polarization, and the Decline of Civic Life. New York: Crown, 2018. Page 5.

In Quayside, we envision a comprehensive network of parks and ground-floor spaces that promote "recurrent interaction" as the foundation of robust civic life. To ensure that the public realm plays a central role in Quayside, Sidewalk Labs plans to provide more than 40,000 square metres of outdoor open space and include a wide range of spaces that can appeal to different groups — from traditional parks to reclaimed street space made possible by expanded trip options to new opportunities for engaging with Toronto's lakefront. The ground floor proposal includes 90,000 square feet of built indoor space for social infrastructure, creating opportunities for a school, community organizations, and local service providers to activate these spaces, strengthen the community, and help community members thrive.[48] The interconnected relationship between outdoor and ground-floor spaces supports common goals around community connectedness and social cohesion.

Sidewalk Labs has engaged in proactive, holistic planning and co-creation with local community, government, and business partners to imagine what these spaces might look like, and how digital tools could help the community to activate them.

[48] For more background on the Public Realm plan, see the Master Innovation and Development Plan, Volume 1, Chapter 1, Page 146 - 167; and for ground floor social infrastructure spaces, Page 216-227.

2.3.4.1 Research for inclusive design principles in public spaces

Before embarking on any design work for Quayside, Sidewalk Labs commissioned a study by Park People, Canada's leading public space advocacy charity, and Doblin, Deloitte's human-centred design and innovation practice, to help inform people-first public space design. The result was the "North of the Water" study. The focus was on inclusivity and specifically engaging voices that often are not part of traditional consultation processes. The partners carefully screened and selected 40 people from across Toronto to participate in a qualitative research exercise focused on the question: What factors create a sense of belonging and ownership in public space?

Researchers spent an afternoon with participants in their homes or went on walks with participants in public spaces — both indoors and out — in different neighbourhoods to help answer this question. Most of the participants came from outside the downtown core and had never previously participated in a public consultation process.

In addition to the input heard during the broader public consultation process, the results from this user research effort helped shape the Quayside proposal and provide general recommendations for how to think about designing inclusive public spaces in diverse cities.

2.3.4.2 Research for inclusive design principles in indoor spaces

In addition to outdoor public spaces, the ground floors of a neighbourhood are foundational to supporting community interactions, to ensuring equitable opportunity to access services and amenities, and to enabling deep participation in shaping the community. There is a long history of street-level markets serving as vibrant public spaces. One of the most iconic examples is the agora of Ancient Greece. These central squares were framed by covered walkways called "stoa," where vendors sold goods and the public gathered to debate new ideas.

But modern cities often reserve the ground floor for retail or expansive office lobbies, which tend to be closed off from the street and built largely for commercial purposes. In these cases, the ground floor plays a limited role in promoting street life, and is constrained in its ability to accommodate other community and social uses, let alone for the community to actively participate in shaping those uses.

The past decade has also seen traditional retailers dying off, as the meteoric rise of e-commerce, the rigidity of long-term lease agreements, and soaring rents that incentivize landlords to hold out for high-value chains have led to papered storefronts. The retailers who have performed best amid these shifts are those who recognize that their stores are less about selling things and more about creating memorable experiences and enhancing social ties. A report by Ryerson University's School of Urban and Regional Planning, commissioned by Sidewalk Labs, provides evidence of this trend in Toronto: between 2007 and 2017, the share of traditional retail shrunk, while the category of food and beverage — the cafés and restaurants that create community — grew across Toronto's main streets.

These conditions set the stage for the next evolution of the ground floor: a return to the public markets of an earlier time, blending an assortment of uses from maker spaces to community meeting spots to food stalls, as well as traditional retail stores. Sidewalk Labs also recognizes the need for affordable spaces in urban communities for non-profit, community-based organizations and services who form a key part of the social support system for so many, and have dedicated approximately 30,000 square feet of space to a Civic Assembly (community space dedicated to civic life and community participation, including digital skillbuilding) and a Care Collective (community space dedicated to health and well-being) in Quayside.

Sidewalk Labs used a mix of in-depth research, public consultation, expert engagement, precedent research, policy requirements and prototyping to inform the proposal for the ground floor.

For example, the TOcore Community Services and Facilities Study Phase One recognizes a need to plan for more affordable, accessible, and appropriate spaces for delivering community services in downtown Toronto; furthermore, enhanced coordination in planning and delivering health care and community services, especially in parts of the city that are growing rapidly, has also been recognized as an urgent need.

To address this planning objective and advance Sidewalk Labs' commitment to inclusive, participatory planning, Sidewalk Labs began a co-design process for a community facility focused on health and well-being. In 2018, Sidewalk Labs partnered with a Toronto-based firm, Idea Couture, to learn more about how neighbourhoods can truly be drivers of community well-being and, by extension, individual health. Idea Couture specializes in human-centric and future-focused strategic design, and they know Toronto very well, as they live and work in the city.

To begin the project, Idea Couture analyzed current trends that could signal where the future of care is headed. This scan was followed by "ethnographic immersions," where researchers sat down with Toronto residents, health and human service providers, and representatives from community organizations for in-depth interviews. These conversations, with Torontonians who came from a mix of age groups and cultural, professional, and political backgrounds, were held across a wide variety of neighbourhoods and living, work, and recreation spaces in the city. The organizations visited include a Toronto Public Library branch, a community health centre, a youth centre, an affordable housing provider, and a social service organization supporting the homeless. What was uncovered was a complex picture of a city that recognizes the vital role community cohesion and social connection play in health and wellness.

To further build upon the insights gleaned from the immersions, Idea Couture and Sidewalk Labs convened a co-design charrette—a day-long gathering of people from the public, non-profit, and private sectors, many focused on health and community services, civic engagement, and urban planning. We asked participants to imagine what a community-based space focused on human connection and care would look like in 2028.

Through the course of the day, more than 90 ideas emerged. People frequently returned to the idea of using technology to give them more control over their well-being and a greater say in their care. Many identified the opportunity to better connect people and community programs—such as informal mentorships, volunteering, or peer-to-peer support—via digital tools. You can read the full Living Well on the Waterfront report to learn more about these insights and the community-oriented research and design concept development approach that generated them.

2.3.4.3 Spaces for equitable access to services, technology, and community participation

In the Master Innovation and Development Plan for Quayside, Sidewalk Labs proposed program ideas that would help create the conditions for more equitable access to services, technology, and community participation.

To truly achieve an innovative neighbourhood, there must be equitable opportunity for everyone who lives, works, and visits Quayside to participate. It can be hard in the rush of urban life for community members to meet each other and connect, let alone to join in the shared project of shaping their neighbourhood.

One key barrier to civic and social engagement is access to digital services. While 98 percent of Ontario households are in areas served by at least basic broadband, only 62 percent of low-income households have a connection at home. In this context, community spaces, like libraries, are critical for digital literacy and inclusion. A recent assessment survey[49] conducted by the Toronto Public Library found that 56 percent of respondents who accessed technology at the library could not otherwise. Of those people, 84 percent increased their digital comfort after their visit and 81 percent reported an increase in their level of community and social engagement. Physical hubs, supported by accessible software and supports, are essential to bridging the digital divide and providing equitable opportunity for people to participate in their community.

Quayside is an opportunity to imagine how civic engagement and social cohesion could be fostered from the beginning by providing the spaces, technologies, and conditions that help a community thrive. Sidewalk Labs recognizes there are many programs, policies, governing bodies, and design choices that could foster social cohesion and civic engagement. If successful, the civic innovations developed by community organizations, local governing bodies, developers, local businesses, or community members could be refined and replicated across the city, making Toronto's communities stronger.

As a result of public consultation, best practice globally, and the unique potential of co-location of multiple models together, the Quayside proposal includes a space dubbed the Civic Assembly, which would be the physical heart of civic life in Quayside by promoting community participation, digital skillbuilding, and creation.

The Civic Assembly could include space to:

- **Gather in flexible formats:** from large events and gatherings to smaller groups, the community would have access to a variety of spaces that can transform to meet their needs and offer programming by individuals, non-profits, and government. Digital technologies can

[49] Elizabeth Glass and Carmen Ho, *BRIDGE Technology Assessment Toolkit: Closing the Gap on Technology Access & Inclusion*, Toronto Public Library Board, February 26, 2018.

be integrated so that it is easy to book spaces, see announcements, learn about opportunities, and allow for easy setup through projectors and other hardware integration.

- **Build consensus and learn about the neighbourhood:** spaces for groups to participate in community building and placemaking, using digital tools and data about the neighbourhood. These spaces could allow community members to explore the latest community initiatives, weigh in on a pending issue, contribute their ideas, or vote for community projects using large screens and touch tables that visualize initiatives and facilitate conversation.

- **Develop digital skills and experience the latest technology:** staffed by digital experts who know the ins and outs of all of the technology in the neighbourhood — community members could access support for any of their digital needs and use the latest technologies to participate, learn, connect and create. Local leaders in the field could offer free digital and data literacy classes, as well as host open hours to facilitate input on digital tools and new use cases.

- **Spark creativity:** spaces for performance, creation, and fabrication with equipment and tools such as laser cutters, woodworking machines, and digital workstations.

As a result of co-design process described above, along with precedent research, the Quayside proposal includes a central space, called the Care Collective, which would be dedicated to enhancing health promotion, self-care, and community building, alongside the delivery of more integrated health care and community services.
The Care Collective could include space to:

- *Access services*: spaces for the delivery of health care and community services, including consult rooms, meeting rooms, flexible multi-purpose spaces, and bookable virtual consult rooms.

- *Learn, connect and support self-care*: a health resource centre where visitors could test, learn about, and borrow a range of curated digital health tools and apps recommended by care providers. Where staff could guide visitors to helpful resources in their community and lead educational programming focused on health literacy, digital health, and self-care.

- *Support mental well-being*: dedicated quiet sanctuary space could help people to maintain their mental well-being by providing a place to relax, relieve stress, and unplug in a tranquil, nature-infused environment.

If the MIDP is approved, Sidewalk Labs plans to further advance the implementation of the Care Collective and Civic Assembly by forming a planning relationships with partner organizations which can help to lead a participatory process for design, program development and tenant identification. The broad program concepts proposed provide ample opportunity for co-creation and exploration beyond the initial ideas, and can (and should) be refined.

Section 3

Growing the Canadian Urban Innovation Ecosystem

Abstract

This section makes clear that the strength of the greater Toronto region's local innovation ecosystem was a primary reason for embarking on this project, and that fundamentally the project's success relies upon partnering with Canadian innovators. The roadmap details initiatives that would begin immediately following the signing of Principal Implementation Agreements with Waterfront Toronto, through the long-term, enduring impact of establishing a global hub for urban innovation anchored by Canadian values and companies.

Table of Contents

Figures

Tables

Section 3: Growing the Canadian Urban Innovation Ecosystem

Few cities can match the greater Toronto region's unique set of assets: a vibrant ecosystem of innovative technology businesses and accelerators; an exceptional talent pool and world-class academic institutions; and an open and diverse society that values inclusive growth, civic engagement, and forward-looking city-building. This was a foundation for Waterfront Toronto's Quayside RFP, which sought to catalyze the innovation ecosystem growing on the waterfront.

Supporting the continued growth of a strong Canadian urban innovation ecosystem aligns with both Sidewalk Labs' mission and our business. Our business has three key activities, each with specific benefits for Canadian innovators.

- First, we seek to build urban developments that incorporate quality design and technologies into placemaking to improve urban life. Core to this business is the integration of leading technologies from existing companies, and supporting the development and distribution of these solutions to address common urban challenges globally. To implement Quayside, Sidewalk Labs will prioritize Canadian companies with local expertise as suppliers and support them in achieving global growth.
- Second, where there are unmet needs in the market, i.e., gaps that would prevent the project from achieving critical outcomes, we develop products to address them. Through a global patent pledge for Canadian-resident innovators, open standards, and a net-revenue sharing agreement with the public sector, the Sidewalk Labs proposal would leverage the success of these new products to benefit the local innovation ecosystem and community into the future.
- Third, through a venture capital fund and infrastructure-focused affiliate, Sidewalk Labs will hold, acquire, invest in, and enable financing for, strategic partners that we see as integral to the future of cities. This will create expanded opportunities for startups and later-stage Canadian companies to access new capital for growing or expanding their businesses, constructing cutting-edge infrastructure, and bringing new products to market.

Sidewalk Labs believes that through a series of reinforcing initiatives, the Quayside project would lead to enduring value creation for the innovation ecosystem in Canada. Urban development and infrastructure innovation operate on a long time scale, advancing over many years from approvals through design and engineering to implementation and ongoing operations. Sidewalk Labs is committed to supporting Canadian innovators at all stages of this project's evolution, since a thriving ecosystem is essential to the company and project's success.

3.0.1 The urban tech industry in Canada, today and tomorrow

Urban innovation sits at the intersection of two of the defining trends of the 21st century: global urbanization and technological change. The combination of tangible infrastructure with intangible knowledge, technology, and services makes the business of urban innovation unique. The most rapid growth in the global economy today is in the "intangible" economy, an economy that is driven by ideas, knowledge, technology, and services.[1] Assets in the intangible economy include brands, computer software, patented technology, and data, which can generate ongoing profits at lower marginal cost making them fundamentally different from tangible assets.[2] Competitiveness in the intangible economy is important to spur economic growth. Urban innovation, importantly, is not exclusively part of the intangible economy. The infrastructure sector, is also a major growth industry; according to a report by the McKinsey Global Institute, the world will need to invest US$3.3 trillion in infrastructure every year to support expected growth through 2030.[3] A large proportion of this infrastructure will be within cities.

Urban innovation, broadly defined, is among the fastest growing sectors globally, attracting, by some measures, more venture capital investment than other high-growth fields like biotech and artificial intelligence. The urban technology industry is defined by Richard Florida as technology businesses that operate primarily within an urban context, such as transportation, housing and accommodation, and infrastructure. Between 2016 and 2017, its share of global venture capital funding grew from 13 percent to 22 percent.[4] Canada, given its long-standing leadership in infrastructure building and the "tangibles" economy combined with its rich existing knowledge economy and technology ecosystem, is well-positioned to lead in the urban innovation industry where the digital, physical, and policy worlds meet. Doing so would address major public goals and deliver economic benefits across the knowledge, manufacturing, and construction sectors.

Sidewalk Labs isn't the only global player seeking to use advanced technology to enable solutions to big urban challenges. There are other approaches to urban solutions being widely exported around the world that do not have the

---

1 Robert Asselin and Sean Speer, "A New North Star: Canadian Competitiveness in an Intangibles Economy," *Public Policy Forum*, April 4, 2019.

2 Asselin and Speer, "A New North Star."

3 Jonathan Woetzel, Nicklas Garemo, Jan Mischke, Martin Hjerpe, and Robert Palter, "Bridging Global Infrastructure Gaps," McKinsey Global Institute, June 2016.

4 Richard Florida, "The Rise of 'Urban Tech,'" *CityLab*, July 10, 2018.

protection for personal privacy and autonomy that are rooted in core Canadian values. There is a need to challenge these approaches and to build an open, democratic approach to 21st century technology and urbanism. Sidewalk Labs is intentionally advancing its flagship effort in Canada and Toronto because of the local values. Canadian businesses are proud of their values of inclusiveness, openness, and respect for individual rights and privacy, and Sidewalk Labs similarly grounds its work in these principles.

3.1 Conditions of a successful urban innovation ecosystem

Innovation is greatly facilitated by the cross-pollination of ideas from different people and organizations in close proximity to one another. When people from universities, research centres, technology companies, and other thought leaders have opportunities to work together and to share ideas innovation flourishes. This is often referred to as a "triple helix model of innovation," and is the innovation strategy that has informed Waterfront Toronto from its beginning. Economic clusters, from Silicon Valley to the Toronto-Waterloo corridor, show that cross-pollination from a few successful businesses can spawn exponential growth of other businesses in related fields. Related companies nearby provide an easily accessible market for products and services. As they mature, successful businesses also help to develop a strong local talent pool — engineers, managers, and others that are experienced in growing businesses and operating in mature environments. Bigger companies can provide an umbrella under which start-ups can grow.[5]

The initiatives and commitments Sidewalk Labs has proposed, outlined in section 3.2, align with the key conditions for successful ecosystem development:

- Access to Capital and Talent,
- Market Access, and
- Ecosystem Innovation Capacity.

The development of a successful economic cluster requires a complex set of conditions and the participation of a range of stakeholders. In collaboration with others, the Quayside project can serve as a catalyst to further grow an already strong technology and innovation ecosystem and can position Canada and the Greater Toronto Area as an urban innovation leader in this rapidly growing sector.

[5] Martin Neil Baily and Nicholas Montalbano, "Clusters and Innovation Districts: Lessons From the United States Experience," Brookings Institution, May 2018.

Table: Visualizing the Core Conditions Necessary for a Successful Urban Innovation Ecosystem

Access to Capital & Talent ($ and expertise)	**Market Access** (sophisticated buyers at home and abroad)
Ecosystem Innovation Capacity (physical and digital infrastructure, policies, research & standards)	

3.1.1 Access to capital and talent

Key ingredients to enable Canadian companies to scale up and become anchors of a thriving technology ecosystem are capital and management talent. Canada and Toronto are already endowed with world-class technology talent, and with creative entrepreneurs seeking to build global businesses. The Canadian venture capital market also performs well as it ranks amongst the top countries in the world for availability of capital, although this investment has not resulted in a commensurate number of scaling Canadian companies.[6] The Quayside project is a unique opportunity for Canada to add to both capital and talent, with support for scaling up. Upon approval of the project, Sidewalk Labs will be an anchor investor, in both venture capital and urban infrastructure, alongside Canadian partners. An additional injection of capital in the local market, focused on urban innovation, will help Canadian companies to raise the money needed to stay and grow independently in Canada. Alongside capital injections, investments in talent will help to strengthen the sector. Through both the development of skilled managers with experience scaling up a startup, alongside Sidewalk Labs' investments in cutting-edge research by supporting the creation of the Urban Innovation Institute, the Quayside project will also contribute to growing the talent pool in Toronto, a critical element needed to build global companies.

3.1.2 Market access

A successful Canadian innovation ecosystem benefits both from sophisticated local buyers working with local companies and from access to global markets. Partnering with Sidewalk Labs, a company with its flagship project in Toronto and with global reach, is a valuable opportunity for Canadian firms. Canadian technology and talent is world class, but small and medium-sized Canadian companies face significant barriers to growth for a variety of reasons, including few opportunities to sell to local customers who are global market leaders. From scale-ups that are competing globally, to small and medium-sized businesses in Canada seeking a key first or

[6] Charles Plant, "Does Canada Have Enough Venture Capital? Does Canada Have Enough Venture Capital Funding?," Impact Centre, September 2019.

early customer with a global footprint, the Quayside project presents an opportunity for Canadian businesses. Not only is Sidewalk Labs able to act as a local buyer, the partnership can extend to other major urban development projects around the world. The imprimatur of contributing to Quayside, Sidewalk Labs' showpiece development, can increase visibility and viability for these companies globally.

3.1.3 Ecosystem innovation capacity

Urban innovation is complex and it takes more than talent, capital and promising businesses to create a strong and sustainable economic and intellectual engine. It requires broader systems change. Innovative businesses thrive in innovative environments — in places where policies and perspectives, standards and regulations, are forward thinking and where cross-sector thought leadership can support the responsible development of the ecosystem. The Quayside project is poised to set the standards for innovative urban developments around the world. Canadian values will be setting the agenda on critical issues like data privacy that will govern all players in this space. Operating in this evolving environment gives an incomparable advantage to Canadian businesses, who not only gain early experience with the new standards, but will also play a key role in developing, testing, and refining them.

3.2 Sidewalk Labs' proposed initiatives for growing the Canadian urban innovation ecosystem

The following table summarizes Sidewalk Labs' proposed initiatives for growing the Canadian urban innovation ecosystem, organized by specific activities tied to the underlying conditions for a successful ecosystem.

Table: Initiatives for Growing the Canadian Urban Innovation Ecosystem

Activity	Overview	Sidewalk Labs' Proposal	Timing
#1 INVEST Invest in local businesses and their talent	Ecosystem growth relies on both access to capital and access to experienced talent to support business expansion. Sidewalk Labs will invest in both, as well as pledge its software and hardware patents covering digital innovations to further invest in the competitiveness of Canadian companies.	**Urban Tech Venture Fund** ● Following implementation agreements, Sidewalk Labs would invest $10M into an early-stage urban technology venture fund focused on Canadian companies. ● Consistent with standard fund strategies, assuming a successful deployment of the initial fund, Sidewalk Labs and its partners anticipate raising additional funds that can further support the scale-up of the Canadian urban tech ecosystem as it matures.	Initial capital contributions upon completion of the Implementation Agreements: 2020.
		Sidewalk Infrastructure Partners (SIP) ● With initial co-anchor partners Alphabet and the Ontario Teachers' Pension Plan, SIP will be available to provide financing for operators of advanced infrastructure systems, enabling access to capital for innovative projects that may have non-traditional risk profiles.	Initial Sidewalk Toronto-related financings: 2021.

Activity	Overview	Sidewalk Labs' Proposal	Timing
#1 **INVEST** Invest in local businesses and their talent (cont'd)		**Patent Pledge** ● Providing global access to Sidewalk Labs' pledged patents allows Canadian-resident innovators to build on these digital innovations and enhance them fostering growth of the sector at large.	Effective upon completion of the Implementation Agreements: 2020.
		Talent Excellence ● Sidewalk Labs will establish an advisory network and work closely with corporate venture partners to support talent development for entrepreneurs, offered alongside its venture investments. ● As a strong addition to the waterfront innovation corridor, comprised of both established and emerging companies in the urban innovation ecosystem, Quayside could be a global magnet for talent and support a concentration of sector expertise. ● The proposed Urban Innovation Institute could also act as a talent accelerator, delivering programs dedicated to skills and talent development.	Establish an advisory network program through the venture fund: 2021. Talent programming through the UII and cluster development: 2021 and beyond.

Activity	Overview	Sidewalk Labs' Proposal	Timing
#2 **PROCURE & PROMOTE** Procure from Canadian businesses and promote these partners abroad	Based on initial estimates, there are 18 major digitally enabled services, including over 50 subsystems, envisioned for the Quayside project (see section 1.3 for more details). Many services and subsystems contain extensive hardware and software components that Canadian companies will be well-positioned to deliver. Sidewalk Labs will not deliver most of the components needed to execute on its proposal in Toronto, rather it will seek out best-in-class solutions. Whether procurement is led by Waterfront Toronto or Sidewalk Labs, the Quayside project provides an opportunity for local companies to sell to local buyers, an advantage for businesses in close proximity to the project. Partners in the Quayside project will benefit from association with the Sidewalk Labs brand as we promote Toronto-based solutions internationally. Enabling access for Canadian companies to global markets is fundamental to their growth and that of the urban innovation ecosystem.	**Procurement** • Sidewalk Labs will engage with the innovation ecosystem, including local accelerators and incubators, to identify high-potential Canadian companies able to meet the needs of the project. • In procurements that Sidewalk Labs leads, we are committed to prioritizing Canadian companies as proponents, recognizing the need to secure best-in-class solutions and fair value. • For engagements anticipated to result in IP creation, Sidewalk Labs would consider how Canadian companies can continue to grow their businesses with other parties seeking to develop solutions for urban challenges.	Ecosystem engagement: Ongoing Mass procurements for implementation would begin once building permits are issued: 2021.
		Innovations Portfolio • Quayside is Sidewalk Labs' flagship project, so we plan to market the innovations successfully implemented in Toronto globally. This means promoting the portfolio of technologies and companies that have contributed to the project. Sidewalk Labs plans to feature these partners in an online innovations portfolio to provide global visibility for our partners.	As soon as procurement begins, Sidewalk can begin promoting its established partnerships: 2021.

Activity	Overview	Sidewalk Labs' Proposal	Timing
#3 CONTRIBUTE Contribute to the development of local capacity to innovate and support the growth of the sector	A thriving urban innovation ecosystem is essential to the success of the project. Sidewalk Labs is only one player in the development of a sustainable urban innovation cluster and will contribute to supporting the growth of the ecosystem in a range of ways from seeding a new Urban Innovation Institute that provides an opportunity for local urban innovation leaders to form a cluster, to contributing to innovations in trusted data sharing, to standards setting, and providing shared value on future product sales with the public sector.	**Urban Innovation Institute (UII)** ● Recognizing the importance of early actions to engage academia and the innovation ecosystem in the development of a new Urban Innovation Institute, Waterfront Toronto and Sidewalk Labs will develop a plan for distributing, upon entering into implementation agreements, $10 million in seed capital to support the early activation of the UII. ● For example, the UII could anchor a hub for data collaboration, a resource to foster quantitative urban research and evaluation capacity and advance models for trusted data sharing.	Initial capital contributions upon completion of the Implementation Agreements: 2020.

Activity	Overview	Sidewalk Labs' Proposal	Timing
#3 CONTRIBUTE Contribute to the development of local capacity to innovate and support the growth of the sector (cont'd)		Trusted Data Sharing • Cross-sector data sharing has enabled quality of life improvements through aligning multiple sectors to common public policy goals. There is widespread recognition across all sectors that greater data sharing can have substantial benefits for public policy outcomes and city operations, and spur new forms of knowledge and value creation. • Waterfront Toronto and Sidewalk Labs share a commitment to testing and establishing new models for trusted data-sharing in order to achieve Waterfront Toronto's priority outcomes and other key policy priorities. Sidewalk Labs is committed to contributing data, technological expertise and resources to this effort, and to leveraging the strengths of existing models where applicable.	Ongoing

Activity	Overview	Sidewalk Labs' Proposal	Timing
#3 CONTRIBUTE Contribute to the development of local capacity to innovate and support the growth of the sector (cont'd)		Proposed Villiers West Innovation Hub ● Based on the performance at Quayside, Waterfront Toronto recognizes that there could be substantial public benefits by providing for an area of future expansion of the initial phase beyond Quayside to the area such as Villiers West to further Waterfront Toronto's objectives, particularly in relation to economic development. Expansion to other lands would be subject to future Waterfront Toronto approvals and any applicable land disposition processes required by the City of Toronto.	2027
		Standards Setting ● With the leadership of governments working with Waterfront Toronto, non-profits, Canadian businesses, and other stakeholders, Sidewalk Labs will contribute to precedent-setting open standards that will form the basis of the Quayside implementation and establish a precedent for future smart cities projects around the world.	Ongoing
		Value Share with the Public Sector ● Sidewalk Labs would share value with the public sector through a global net revenue sharing agreement on "Testbed Enabled Technologies."	Effective upon completion of the Implementation Agreement: 2020.

3.2.1 Investing capital, intellectual property, and talent

Sidewalk Labs is proposing a series of initiatives that address the need for investment in the ecosystem — in the form of capital, intellectual property, and talent.

3.2.1.1 Urban tech VC fund

To start, in concert with a definitive transaction for the eastern waterfront, Sidewalk Labs would establish a venture capital fund focused on Canadian companies. Intentionally starting small, Sidewalk Labs would commit $10M to a Fund I, and is already seeing interest from Canadian corporate innovation arms and respected individuals to grow the fund. It is expected that Canadian investors would make up at least 50 percent of the fund. Consistent with standard fund strategies, assuming a successful deployment of the initial fund, Sidewalk Labs and its partners anticipate raising additional funds that can further support the scale-up of the Canadian urban tech ecosystem as it matures. The approach will be based on insights from this initial fund.

Over the last 18 months, Sidewalk Labs has engaged with over 300 Canadian urban tech companies, helping inform the fund's emerging investment thesis. Canada has a strong base of companies at the Seed and Series A stage, and by launching the fund Sidewalk Labs can help accelerate the growth of these companies. The fund would have both a strategic and a financial mandate, strengthening its ability to contribute to a robust urban tech ecosystem. It is important to back companies that can scale and provide market returns, so the Canadian tech sector can have more anchor growth-stage technology companies. A key criterion for investment will be ensuring companies are aligned with responsible data use principles.

In its investments, the fund will not lay claim to a company's intellectual property (IP). As with traditional VC investments, our investment thesis rests on the assumption that retaining IP will be integral to the success of Canadian companies, and this is foundational to the fund's practice. The VC fund's advisory network would provide further support to local founders regarding their IP strategy. In addition, this network, which would include expertise from Canada and the United States, would be dedicated to supporting mentorship and talent development for portfolio companies and the ecosystem more broadly, helping expand knowledge among Canadian innovators on best practices for scaling companies and reaching global markets.

Recognizing that it takes more than just capital to scale companies and augment their potential, Sidewalk Labs would support the venture fund's portfolio through access to our expertise, pilot opportunities, customer contracts, and global network of contacts. Additionally, the fund would establish an advisory network of experts that can assist with a wide range of topics, from implementing responsible data use practices to building out a marketing team. These experts would include leaders in technology fields, as well as active CEOs of growth-stage startups who can help groom the next generation. Advisory experts would come from both Canada and the United States, as Sidewalk Labs believes connecting Canadian entrepreneurs with market opportunities across North America is important to supporting scale.

Key to the fund would be the involvement of anchor Canadian corporations, as well as industry-relevant international players. By working together, additional capital would go into the market and add further strategic value to the portfolio in terms of providing customer contracts, industry expertise, and access to C-level staff. This collaboration could help grow and scale companies faster, which would assist in establishing Toronto and Canada as a global urban technology leader. As Sidewalk Labs raises future funds, participation from other corporate investors would also increase. This would provide a steady source of strategic venture capital, which has consistently been much less abundant in Canada than in the United States.[7]

By focusing solely on Canadian urban technology startups, the goal of this effort would be to unlock capital and support from other players in the ecosystem around this vertical. By leading investment rounds, the fund can also spur additional industry investment or support from the existing funds in the VC community. This will help further drive the establishment of a robust urban tech ecosystem in Canada. Starting with a smaller fund enables Sidewalk Labs to begin working with partners shortly after completing implementation agreements. Fund I is as a strategic first step that will validate and solidify processes that support portfolio engagement with Sidewalk Labs and other investors' corporate innovation programs.

Sidewalk Labs also intends to partner closely with incubators and accelerators to further the development of relevant programs and support for urban technology focused on startups and scale-ups. This can plug directly into the current activities of institutions like MaRS, DMZ, CommuniTech, Creative Destruction Lab, the Impact Centre, and others, which are regularly identifying ventures ripe for investment.

3.2.1.2 Supporting advanced infrastructure in Canada and around the world

An overemphasis on reducing risk and associated yields means that cities, businesses, and traditional investors and developers are unprepared for how technology will disrupt and enable infrastructure, especially new approaches to infrastructure that achieve greater sustainability. While the urban tech VC fund would be focused on early-stage tech companies, Sidewalk Labs has already established a company focused on supporting advanced infrastructure in Canada and around the world. Sidewalk Infrastructure Partners (SIP), with initial co-anchor partners Alphabet and the Ontario

[7] James McLeod, "Venture Capital Funding Flat in 2018, but Industry Players Say Investment Ecosystem Is Strong," *National Post,* March 15, 2019; "US Venture Capital Investment Reached $130.9 Billion in 2018, Surpassing Dot-Com Era," *Pitchbook*, January 10, 2019; "The Global Unicorn Club," *CB Insights*.

Teachers' Pension Plan (OTPP) — one of the most widely respected institutional investors in the world — holds, acquires, and invests in advanced infrastructure projects, as well as the technology companies applying innovations to these projects worldwide. SIP believes the transformative promise of advanced infrastructure will require a new manner of thinking about the application of digital technology to real assets.

The Quayside development proposal incorporates a series of advanced infrastructure systems, from a thermal grid to dynamic streets. It is contemplated that stapled SIP financing (on terms to be described in requests for proposals or other procurement documents) would be offered as an option for operators of advanced systems, such that Canadian operators of advanced systems that are successful proponents in a procurement could elect to utilize such stapled SIP financing if they choose.

3.2.1.3 Proposed patent pledge

Sidewalk Labs is committed not only to supporting the development of Canadian intellectual property, but in fact investing its own intellectual property to support the growth of the Canadian innovation ecosystem. In the MIDP, Sidewalk Labs offered a patent pledge that declared it would allow Canadian-resident innovators to build on top of any digital innovation patents covering software or hardware that Sidewalk Labs files in Canada. While many in the ecosystem appreciated a patent pledge, there was concern that restricting the pledge exclusively to Canada would in fact limit the potential growth of Canadian companies that took advantage of the pledge. It is well-known that one of the most significant challenges facing Canadian innovators is reaching substantial scale and expanding beyond the Canadian market; thus, if the pledge was only applicable to Canadian patents, promising innovations that would reasonably seek to scale might be inhibited. Based on this feedback, rather than limiting the pledge to Canadian patents, Sidewalk Labs has decided to also include all of its digital innovation software and hardware patents across the globe, ensuring that the pledge aligns with the foundational objectives of supporting Canadian-resident innovators. Sidewalk Labs proposes to make its patented digital urban innovations available to Canadian-resident innovators without fear of patent infringement, enabling them to independently leverage its proprietary technologies and thereby accelerating the development of city-enhancing initiatives. This pledge would go into effect immediately after the signing of Principal Implementation Agreements with Waterfront Toronto, and would be subject to defensive termination as further described below.

Addressing patent concerns

Patents can play a key role in spurring or supporting the innovation ecosystem by enabling parties to protect inventions developed through rigorous research and development efforts. In recent times, however, some parties have become concerned that holders of patents may have an advantage that has the opposite effect. Sidewalk Labs heard those concerns expressed in connection with the Quayside plan and wanted to take a proactive step in alleviating them.

Also with respect to concerns, the deterrent effect of litigation for patent infringement in North America and other countries with other strong patent regimes is real and largely due to very high defence costs, which can balloon into millions of dollars.[8] To combat this reality, some companies conduct searches, and/or hire legal counsel to do the same, seeking to identify whether an invention could be infringing, in order to minimize their exposure to lawsuits. Some companies also go so far as to obtain a legal opinion that a proposed course of activity would not infringe a third party's patent rights, also known as a freedom to operate opinion. In 2010, a freedom to operate opinion over software was estimated to cost at least USD $10,000.[9] This cost has presumably increased over the last decade due to increased filings of software patents, market crowding, and typical legal fee increases over time.[10] To many entrepreneurs, this cost is prohibitive, so the choices left are to avoid innovating in a particular area or to innovate and hope to not be deemed infringing and sued. Large technology companies in the United States recognized this innovation deterrent as a serious enough issue that resolutions were sought. One such resolution, notwithstanding that it may reduce some of the value of the patent to the patent holder, was the introduction of patent pledges by companies such as Microsoft, IBM, and Google, among others.

Sidewalk Labs believes that the availability of this pledge would stimulate innovation within this landscape, similar to conclusions drawn by various scholars looking into the effect of patent pledges.[11] Providing a patent pledge can stimulate innovation in areas ancillary to those of the pledged patents as well, providing a foundation for innovation in the broader subject area. In the Quayside plan, this would equate to generating a base of innovation on digital-enabling innovations which, once deployed, should result in more efficient urban cities.

Content of the pledge

By virtue of the patent regime in Canada, no intellectual property rights under the Patent Act are obtained until a patent is granted by the Canadian Intellectual Property Office. Hence, only granted Canadian patents would be subject to the pledge. This feature of the patent regime is echoed in other countries as well, such that only granted patents from other jurisdictions would be subject to the pledge. The

[8] Steven Garland, Kevin Graham, Daniel Hnatchuk, "Canada," *Patent Litigation Law Review*, Edition 2, November, 2018. Note that the latter article discusses costs for plaintiffs; however, defence costs are thought to be in the same ballpark.
[9] Gene Quinn, "Differences Between Patent Searches & Infringement Clearance," *IP Watchdog*, January 21, 2010.
[10] "Open Source and Patent Non-Assertion Pledges: A Comparative Analysis," Institute of Computer and Communications Law Centre for Commercial Law Studies, Queen Mary, University of London, October, 2014.

[11] See footnote 58 in Jorge L. Contreras, "The Evolving Patent Pledge Landscape," Centre for International Governance Innovation, April, 2018.

pledged patents would include a series of patents developed and filed by Sidewalk Labs, which feature hardware or software that enable digital innovations. All the pledged patents would be listed online for clarity on the definitive number of publicly available patents that can be leveraged by Canadian-resident innovators. These innovators would then have the ability to develop and sell innovations that utilize those patents worldwide without fear of facing patent infringement suits by Sidewalk Labs, subject to the defensive termination feature of the pledge explained below. The pledged patent list would be updated regularly as new applicable patents are granted.

The pledge would protect Canadian-resident innovators from infringement lawsuits by Sidewalk Labs save in one circumstance. Should an applicable innovator taking advantage of the pledge or its affiliates assert a case of patent infringement against Sidewalk Labs or any of its affiliates (constituting only Sidewalk Labs family companies[12]), the benefit of the pledge would fall away in respect of that third party and ordinary intellectual property laws would be reinstated.

Strategy to file in Canada

Another concern Sidewalk Labs heard in conducting consultations was a fear that patent filings would not be made in Canada, and therefore no patents would actually be pledged. To ensure clarity on this matter, Sidewalk Labs commits to file corresponding patent applications in Canada for the digital-innovation-enabling hardware or software technology on which Sidewalk Labs develops and files a patent application in any jurisdiction around the world, including the United States. Any such granted patents would be listed online as a pledged patent.

Additional considerations for the Quayside plan

In addition to the issues noted above, Sidewalk Labs has heard some concern expressed over how intellectual property would be treated by Sidewalk Labs in this project, including concerns over using the Canadian ecosystem to develop innovations but not contributing any of the value back to Canada.

As Sidewalk Labs stated in the MIDP, it is its desire to build out an urban innovation ecosystem that proves the innovations initiated through this project but also spurs economic development and cultivates an urban innovation cluster where startups, non-profits, private actors, government agencies, and other entrepreneurs from across the globe can build and prove out new technologies. As a result, it is in everyone's interest to consider ways to ameliorate these concerns to ensure Sidewalk Labs' project does not stifle innovation in the Quayside geography or more broadly in Canada, and it sees the patent pledge as a key facet in this strategy.

The development of intellectual property would certainly form a part of Sidewalk Labs' business strategy. However, asserting

[12] This family excludes parent company, Alphabet Inc., as well as sister companies under common ownership such as Google, Waymo, and so on.

patents is not a cornerstone of Sidewalk Labs' business model. Sidewalk Labs is in a unique situation in that it both wishes to and is able to share the value of certain key intellectual property developed for the Toronto project with the tech community in Canada to stimulate a much-desired innovative ecosystem. Specifically, Sidewalk Labs' goal is to build next-generation communities that combat problems it has identified in global cities today. An important part of the advancements in these communities would be patented digital-innovation-enabling technologies. Rather than monopolizing such patented technologies, Sidewalk Labs would prefer to stimulate the innovation ecosystem in Canada by allowing Canadian-resident innovators to leverage its work to enhance the rate of innovation to a level that Sidewalk Labs alone could not achieve. As global citizens, we are all in a race to make cities more sustainable, affordable, and inclusive, among other ambitious goals, and our competitor is the status quo. We must all work together to build the types of communities we want our children and grandchildren to enjoy in future.

3.2.1.4 Scaling talent excellence

One of the rarest and most critical elements required to build and grow companies to global scale is experienced management talent.[13] These are individuals who have learned how to take a startup with a nascent idea and transform it into a major business. Take the Toronto-Waterloo corridor. Thanks in large part to the success of BlackBerry Limited (formerly known as Research in Motion) and several other companies, there was a large cadre of experienced managers who participated in growing globally competitive companies. This concentration of experience created a talent engine that has built the region into a major global technology cluster.

Working on the Quayside project, both directly for Sidewalk Labs as it grows into a major global business and for partner companies as they scale, provides the local talent pool with a unique opportunity to gain new experience and skills in a precedent setting project. Sidewalk Labs has already worked with over 130 Canadian firms and consultants on a wide range of innovative projects and will continue to both hire its own employees and work with local companies in a wide range of capacities. Working with Sidewalk Labs or our partners to build Quayside, will create a talent pool that is in high demand and that has unique insights into the urban innovation market. Some of this talent may in turn start new companies or provide management expertise to help promising companies grow and scale.

Strong management talent with the skills required to lead and grow companies is needed to match Canada's technical talent. In the near term, Sidewalk Labs' contributions to

[13] Dan Herman and Sarah Marion, "Scaling Success: Tackling the Management Gap in Canada's Technology Sector," Lazaridis Institute for the Management of Technology Enterprises, Wilfred Laurier University, March 2016; Stuart Crainer and Des Dearlove, "Death of Executive Talent." *Management Review* 88, no. 7 (July/August 1999): 16–23.

growing this cadre of management talent include a management talent acceleration program offered alongside Sidewalk Labs' venture investments. This would include advisory services from a network of successful c-suite executives that Sidewalk Labs would bring together to support early-stage and scale-up companies where we invest.

The Urban Innovation Institute could also deliver programs dedicated to skills and talent development, including support for entrepreneurs-in-residence drawn from those companies participating in Quayside as well as the wider ecosystem. Early work to define the key capabilities of the UII would consider how it can function as a talent accelerator.

As the Quayside plan moves further along in its implementation, it is anticipated that it would continue to attract high-growth businesses and their talent to Toronto, expanding the pool of managers with the expertise needed to complement the region's other strengths. Comprised of both established and emerging companies in the urban innovation ecosystem, Quayside will be a global magnet for talent and support a concentration of sector expertise.

3.2.2 Supporting market access through procurement from Canadian businesses and promoting these partners abroad

Sidewalk Labs is proposing a series of initiatives and practices to address the challenge of providing Canadian companies market access, both locally and globally. Fundamentally, these include specific efforts to source Canadian companies to participate in procurements, breaking ties in Canadian companies' favour during procurements, and then supporting the global distribution of Canadian partners.

3.2.2.1 Procurement of Canadian technology for implementation

Procurement for the Quayside project will be one of the most impactful levers for advancing the growth of the Canadian innovation ecosystem. Once building permits are issued and construction begins, there would be substantial procurement of technologies for the development itself. Depending on the system being purchased, some procurements would be led by Waterfront Toronto on its own behalf or on behalf of governments, and other procurements would be led by Sidewalk Labs. Based on initial estimates from the design and engineering that informed the MIDP, there are 18 major digitally enabled services, including over 50 subsystems, envisioned for the Quayside project. Many services and subsystems contain extensive hardware and software components that Canadian companies will be well positioned to deliver. In procurements that Sidewalk Labs leads, the company is committed to sourcing local companies to bid whenever possible, recognizing the need to secure best-in-class solutions and fair value.

In the proposed approach, Waterfront Toronto, Sidewalk Labs, and its partners would procure a vast array of goods and services for the Quayside project. These procurements will be governed by various principles, depending on whether it will be Sidewalk Labs, another private business, or a public-sector organization conducting the procurement. When conducting procurement, public-sector organizations, broader-public-sector organizations, and private-sector organizations each have a different set of default rules from various sources that apply to them. Furthermore, a purchaser may agree to adopt more rigorous procurement standards, as Sidewalk Labs did when entering into the Plan Development Agreement, where in Schedule D it agreed to abide by specific principles that would govern a framework for procurement after execution of the implementation agreements, and in addition, to abide by fair and arm's-length procurement standards.

With respect to the acquisition of technology in Sidewalk Labs' project in Toronto, the following forms of procurement need to be considered:

Procurements conducted by Waterfront Toronto

Waterfront Toronto is an independent entity that was created by three levels of government and is governed by a provincial statute.

Waterfront Toronto is subject to its own private-sector procurement rules[14] and has voluntarily adopted and posted a procurement policy on its website describing the rules that the organization generally follows when conducting procurements. Whenever Waterfront Toronto is conducting a procurement for technologies in connection with the Quayside project, Sidewalk Labs would expect Waterfront Toronto's ordinary procurement policy to apply, subject to any amendments or special exceptions that may be adopted within the policy.

[14] If Waterfront Toronto receives $10 million or more in provincial funding, then in the calendar year following receipt of such funding, Waterfront Toronto will be subject to external procurement rules applicable to Broader Public Sector entities pursuant to the *Broader Public Sector Accountability Act*.

Innovation procurement[15]

Many organizations — including those in the public sector — are turning to innovative methods to improve procurement outcomes. This is often referred to as "innovation procurement." Innovation procurement inherently involves solving a problem — but where the solution may not exist or may be difficult to describe, or where there may be a variety of completely different solutions to choose from. In addition, solving the problem may require significant collaboration with vendors, and may involve risk- and reward-sharing as a solution is developed and implemented. For these reasons, innovation procurement is also referred to as "problem-based" procurement or "challenge-based" procurement. The purchaser poses a problem or challenge to the marketplace and uses an open-ended process to evaluate potentially wide-ranging solutions. To effectively navigate the potential challenges of an open-ended process, innovation procurement generally involves two core features:

- **First, it requires early-stage research and market engagement.** Although traditional procurement processes require some measure of background research and vendor contact, for innovation procurement (where the purchaser may be unable to clearly describe its problem or needs, let alone what a solution might look like), such work is essential. Through research and dialoguing with vendors, the purchaser can get a general understanding of the context, issues, needs, and parameters, and better frame their needs and how the resulting procurement process will unfold. Purchasers should consider a wide range of methods of gathering information and early market engagement. Through formal information solicitations, trade shows, reverse trade shows, advance notices, and other strategies, purchasers can glean critical insights into how to frame their needs and structure their procurement.

- **Second, it benefits from a flexible and accommodating competitive process.** This means that the competitive procurement process (such as described in a Request for Proposals) includes mechanisms that permit dialogue and refinement. For example, by having a competitive dialogue phase, a purchaser can have separate, confidential one-on-one meetings with each bidder before it finalizes its specifications and needs, and calls for final bids. This inherently benefits purchasers (who can improve and better inform their ask) and bidders (who gain better visibility into the purchaser's needs to improve their bid). Also, it means that the specifications and the evaluation criteria must accommodate significantly different solutions. This is done by crafting specifications so that they are "outcomes-based" (such as specifications about final outcomes, not how to achieve those outcomes), and framing evaluation

[15] "BPS Primer on Innovation Procurement," Supply Chain Ontario, Ministry of Government and Community Services, 2016; "Innovation Procurement Toolkit," Healthcare Supply Chain Network.

criteria so that they evaluate the value that a solution brings and the extent to which it can achieve the stated outcomes. The aim is to avoid specifications and evaluation criteria that are unnecessarily narrow or short-sighted, foreclosing on innovative proposals.

Innovation Procurement is an active area where Ontario is a leader. For example, the Municipal Innovation Exchange (MIX) is an emerging centre of excellence, using procurement as a tool to build innovation capacity and explore complex municipal challenges. MIX is a joint effort led by the City of Guelph, in partnership with the City of London, City of Barrie, and the MaRS Discovery District.

It is important to note that public procurement rules (to the extent applicable to a purchaser) do not prohibit dialogue with potential bidders as part of background research or market engagement. Similarly, those rules do not prevent the use of flexible competitive processes. It is critical that purchasers ensure that competitive procurement processes are fair and that they take steps to manage fairness risks at each stage of the process. However, the upside of innovation procurement can be considerable — it can improve the ultimate "fit" between the purchaser's needs and the market's capabilities, and lead to a more efficient and effective procurement process.

While deploying a full suite of strategies and methods for innovation procurement can involve significant time and resources (best reserved for high-value/high-impact problems), purchasers can still incorporate some innovation-procurement elements into their less critical processes. Sidewalk Labs would encourage and support Waterfront Toronto in integrating innovation procurement processes into its framework for approaching procurements of both critical and lower-impact items in Quayside to facilitate acquisition of the best possible solutions for each of Waterfront Toronto's key objectives.

Procurements conducted by Sidewalk Labs

To fulfill Sidewalk Labs' commitments in the Plan Development Agreement and subsequent Principal Implementation Agreements, Sidewalk Labs must procure goods and services from third parties. Some of these procurements would include procurement of technology. In these procurements, Sidewalk Labs would seek to ensure the Canadian ecosystem is aware of all procurements and prioritize Canadian companies by breaking ties in their favour. The specific mechanisms to achieve this, while ensuring best-in-class and fair value, will be further clarified through engagement with the industry.

As a privately held company, only the common law of tendering applies to procurements by Sidewalk Labs except to the extent that it agrees otherwise by contract. When entering into the Plan Development Agreement, Sidewalk Labs agreed to abide by certain additional standards after execution of the Principal Implementation Agreements, namely, fair and arm's-length procurement standards, which "will seek to balance — in the public interest — the use of market-based sourcing, on the one hand, and the direct facilitation of Purposeful Solutions for innovation, on the other hand."

For every technology that Sidewalk Labs procures through market-based sourcing (which includes all technologies not produced by Sidewalk Labs), Sidewalk Labs would abide by fair and arm's-length procurement standards informed by the principles enumerated in Schedule D of the Plan Development Agreement, namely, consultation, flexibility, value, fairness, and compliance. As to when this might occur, Sidewalk Labs could be procuring technologies in its role as lead vertical developer. For example, Sidewalk Labs may procure a technology for use in tall timber buildings, which would be physically integrated into buildings by vertical development partner(s) for Quayside Sidewalk Labs will lead implementation of advanced infrastructure systems in accordance with the Innovation Plan, subject to Waterfront Toronto's review and approval. "Advanced infrastructure" includes the thermal grid, pneumatic waste systems, and other non-traditional systems as proposed in the MIDP. To the extent Sidewalk Labs proposes to move forward with advanced infrastructure, with Waterfront Toronto's approval, Waterfront Toronto will not be held responsible for delivery or operation of such advanced infrastructure.

Intellectual property in procurement

Sidewalk Labs is committed to supporting the intellectual property rights of Canadian product and service providers who participate in the provision of those products and services in Quayside. These commitments include the recognition that developing solutions for contemporary urban challenges will require collaborative inputs from multiple parties. For engagements anticipated to result in IP creation, Sidewalk Labs would consider how Canadian companies can continue to grow their businesses with other parties seeking to develop solutions for contemporary urban challenges.

3.2.2.2 An urban innovations portfolio to support global distribution

Canadian companies cannot only benefit through integration of their solutions into Quayside, but through achieving greater global distribution. From new road traffic signalling technology, to new approaches in weather protection, to tall timber construction techniques, to new approaches in design for pedestrian safety, many new technologies and solutions will be implemented as part of the Quayside plan. Canadian companies will be closely integrated partners on the Quayside plan, in industries ranging from technology to construction to engineering. Sidewalk Labs has no intention or ability to develop all of these technologies, products, and services on its own. This provides a substantial opportunity for supporting high-growth scale ups, a key area to advance Canadian competitiveness.[16]

Quayside is Sidewalk Labs' flagship project, so Sidewalk Labs plans to market the successful innovations implemented in

[16] Raly Chakarova and Craig Ruttan, "Defying Gravity: Building a Scaleup Ecosystem," World Trade Centre Toronto, 2019.

Toronto globally. Canadian companies would benefit from Sidewalk Labs' global reach and distribution. This would include establishing a highly visible urban innovations portfolio comprised of the partners that are integrated into Quayside. Participation in Quayside will be a calling card that will open doors on projects around the world. Furthermore, Sidewalk Labs will actively promote its partners to the initiators of other Sidewalk Labs projects around the world.

Sidewalk Labs' future projects will require many component products and services produced by its partners, therefore, success in marketing its urban solutions worldwide would lead to more sales for its partners' products and services, and the successful development of Sidewalk Labs' partners' products and services would improve the appeal of Sidewalk Labs' solutions.

Figure: Illustration of Urban Innovations Portfolio, Globally Showcasing Canadian Partners in the Quayside Plan

We plan to highlight the partners with whom we have successfully worked at Quayside in an online space that would afford truly global visibility for their products and services. Such an online portfolio would benefit emerging and established companies by accelerating routes to global markets and new customer acquisition. For Sidewalk Labs, the early creation of this ecosystem would draw on partners working with us in Toronto and showcase these solutions. Curation of best-in-class solutions to form an integrated and implementable solution is a core part of what Sidewalk Labs can do. Sidewalk Labs wants its partners to emerge as genuine beneficiaries from their relationship with us.

The urban innovations portfolio would afford product and service providers an expanded brand presence, and the opportunity to be regularly featured and showcased as leaders in the provision of urban solutions as part of Sidewalk Labs' global sales activities. Sidewalk Labs will promote its portfolio of partners not only to help advance their global reach, brand recognition, and access to new markets, but also to signal to the market that these solutions meet high data-privacy, responsible data use, and sustainability standards in order to advance higher standards of practice internationally.

3.2.3 Contributing to the development of local innovation capacity to support the growth of the sector

Investment in, procurement of goods and services from, and promotion of Canadian companies are all activities that Sidewalk Labs can lead on executing. The success of these activities, however, depends on the strength of the underlying urban innovation ecosystem. Innovative businesses thrive in innovative environments. In order to support ongoing innovation and leadership across the ecosystem, Sidewalk Labs is proposing a series of initiatives that contribute to strengthening the underlying ecosystem foundations. In many cases, the role of Sidewalk Labs is to support the work of others or even to provide funding to establish new, arm's-length institutions that can help steward the growth of the ecosystem.

3.2.3.1 Seeding an Urban Innovation Institute

Toronto has an extraordinary existing network of urban innovation leaders, from accelerators to companies to academic institutions to major corporate businesses to innovative public-sector agencies. A need that Sidewalk Labs has heard from the ecosystem is that the city could benefit by having an organization embedded in Quayside that could support the ecosystem's ability to come together and to test new ideas, which could provide core infrastructure for applied research, and which could provide a home to foster knowledge and skill development. To address this challenge and support further building out a robust foundation for the local urban innovation ecosystem, Sidewalk Labs has proposed $10 million to fund the business planning and early activation of an independent Urban Innovation Institute (UII). The goal of this proposed commitment is to establish a new institution that is complementary to the city's extraordinary existing institutions, and that helps support and advance the work of local urban innovation leaders. The UII would build on the strength of the existing innovation corridor on Toronto's waterfront, including tenants such as George Brown College, Corus Entertainment, OCADU, MaRS, Artscape, Remix, HXOUSE, and other.

From now until the signing of implementation agreements in December 2020, Sidewalk Labs and Waterfront Toronto will work together to define the priorities and roadmap for distributing this $10 million seed capital. Following definitive agreements, a portion of this $10 million could, for example, be used to immediately support research chairs at Canadian universities in areas critical to the ecosystem's success — for example, trusted data sharing, urban digital policy, and AI ethics. The rest of the initial seed funding could be granted to a consortium of universities and accelerators that together over three years would have the resources to develop the long-term roadmap for the Institute, including critical milestones that could unlock additional contributions from Sidewalk Labs and other potential funding partners. The programming of the selected consortium would incorporate the insights from the work of the research chairs.

The Urban Innovation Institute is intended to help firmly establish Toronto as a world leader in the research and development of urban solutions. Sidewalk Labs would not be directly involved in the governance or operations of the UII and instead has proposed an independent governance model to enable flexibility with respect to structure, partnerships, and relationships with other institutions and organizations. The UII and its partners would independently select avenues of research and intellectual property policies would be in keeping with participating institutions' own policies.

The UII could be modeled on [world-class research centres like the institutes of the Fraunhofer Society in Germany], which conduct applied research geared towards advancing technology and improving people's lives. While each institute in the Fraunhofer Society operates independently, they receive funding for conducting research into specific problems from various private-sector partners, as well as from the public sector.

Some of the qualities and potential initiatives that would distinguish the UII could be:

- Being part of a neighbourhood purpose-built for innovation.
- Deeply integrating research and assessment of the many social and ethical implications of technology in our cities today.
- Accessing unique insights and influencing work taking place right outside its doors, by virtue of being physically embedded within a new and growing

neighbourhood that itself is a showcase for applied research and advanced urban solutions.

- Rapidly discovering issues that reflect on-the-ground realities and debates, therefore greatly accelerating the development of solutions in concert with thoughtful policy.
- Supporting a data collaboration hub, a first-of-its-kind, large-scale computing resource dedicated to aggregating data at the urban scale and advancing frameworks for trusted data sharing.

The UII would involve Toronto's innovation ecosystem, including universities and colleges, engaging their faculty in cutting-edge research and creating learning opportunities for their students. It would produce an evidence base that would facilitate more informed public policy decisions around all aspects of urban innovation, making Toronto a global centre of urban research and thought leadership.

Sidewalk Labs has engaged with a number of institutions and civic groups across Toronto on the UII and believe that there is interest in key stakeholders coming together to lead to its creation, supported by seed funding from Sidewalk Labs. This includes academic institutions, but it also would involve many other actors from the technology ecosystem in the private, non-profit, and public sectors. Once established, the UII could bring leading researchers and innovators from across the globe to Toronto.

Finally, in addition to its research role, the UII could advance a broader mandate to advance talent development and promote dialogue, public education, and programming. The UII can serve as a coalescing node through which entrepreneurs, public and civic leaders, the business community, academics, and city residents can collaborate to address pressing urban challenges. It could work to disseminate its research and best practices to the broader community, to serve the goal of improving urban policy and planning and enhance civic dialogue. It could also work to build an urban innovation skills base, in collaboration with entrepreneurship programs at universities and colleges and with local innovation ecosystem partners such as MaRS, Brookfield Institute, the Impact Centre, and DMZ, among others. In order to realize the potential of urban innovation and scale its benefits, learning opportunities should also extend to both public- and private-sector leaders to support them in learning new skills and enhancing the capacity for mutually beneficial collaboration.

Table: Showing the Unique Innovation Challenges an Urban Innovation Institute Could Help Address

<table>
<tr><th>Innovation Challenge</th><th>Potential Institute Role</th><th>Outcomes</th></tr>
<tr><td>Researchers and developers lack real-world experimentation and prototyping opportunities</td><td>Incubate and Accelerate.
The UII could reduce the time, cost and regulatory burdens of developing exceptional urban innovations and bringing products to market with processes that allow for real-world prototyping to create unparalleled abilities to deploy and scale.</td><td rowspan="3">Faster deployment of better products integrated across urban systems

More impactful and responsible development of products that reinforce one another under shared principles and standards

Expanded knowledge and insight across a larger community of urban innovators</td></tr>
<tr><td>Urban technologists too often work in silos, without integration across urban systems</td><td>Exchange and Improve.
With a focus on integration across urban innovation verticals, the UII could develop new ways for practitioners to work together, integrating information-sharing, research, and development environment that brings together thinkers and makers from diverse backgrounds, to create complementary urban innovation products, and facilitate continuous improvement.</td></tr>
<tr><td>Urban technologists and city builders have no common innovation principles or clear place to come together</td><td>Assemble and Lead.
The UII could create a space for cross-sector exchange and operate on core principles and priorities that create the conditions for true collaboration. Education and events in a world-class venue could engage a range of urban innovation stakeholders, and a new urban innovation data hub and analytics library could foster learning globally.</td></tr>
</table>

Execution

Sidewalk Labs proposes seed funding of $10 million to support a diversity of early programs and the creation of a consortium of organizations to stand up the UII. If the project is approved, this support is intended to enable:

1. A detailed business plan to establish the UII as an independent entity, including articulation of the mandate of the UII and how the entity would not create a financial burden for governments or the broader public sector;
2. Development of a framework for applied research and programs that:
    - identify key urban policy issues the UII will seek to tackle;
    - explore the establishment of a data collaboration hub;
    - develop approaches to incubating urban innovations in an effort to accelerate their path to market; and
    - provide public-sector and entrepreneurship support including skills and talent development.
3. Global visibility of the establishment of the UII and the growth of the urban innovation ecosystem in Toronto.

Sidewalk Labs understands that a similar framework was undertaken in establishing the Vector Institute.

Sidewalk Labs would propose to develop a series of key milestones with the consortium as part of the agreement. Once achieved, the UII could unlock further support from Sidewalk Labs following this initial three-year period.

3.2.3.2 Cross-sector trusted data sharing to foster innovation

There is widespread recognition across public, private, non-profit, and academic sectors that greater data sharing can have substantial benefits for public policy outcomes and foster innovation. There are many emerging governance structures and technical solutions being developed and piloted around the world to make data accessible in secure, privacy-preserving, and responsible ways to achieve public policy outcomes and support local businesses.[17]

An important part of the Quayside project is the commitment by Waterfront Toronto and Sidewalk Labs to testing and establishing new models for trusted data sharing. In the draft MIDP, Sidewalk Labs proposed an “Urban Data Trust” that would be a new government-sanctioned entity to support responsible data use and trusted data sharing. With Waterfront Toronto and its government stakeholders taking

[17] For an overview, see section 4.5.3 on Responsible Data Sharing.

the lead on data governance, establishing the Urban Data Trust as a new entity for this project is no longer being pursued. However, exploring data trusts and other models of trusted data sharing remain a priority.

Fundamental to the original “Urban Data Trust” proposal was the recognition that data collected in the public realm could reasonably be considered a public asset, and thus it was important to develop mechanisms for this data to be shared for public benefit. The objective of supporting trusted data sharing remains integral to the project and can be pursued separately from the regulatory functions that govern data collection.

Many of the digitally enabled services[18] proposed for Quayside will require some form of data exchange between them to enable effective operation and achievement of Waterfront Toronto’s priority outcomes. Sidewalk Labs is committed to implementing robust and secure data exchange mechanisms for the proposed digitally enabled services. However, those mechanisms are different from creating a way for third parties to re-use and apply that data for public benefit.

To further the goal of data as a public asset, Sidewalk Labs suggests that a hub for data collaboration be created (potentially anchored at the Urban Innovation Institute) and be operated collaboratively with cross-sector partners to support the data access needs of the public and third parties.

The hub could provide the technical infrastructure and organizational support required to advance trusted data sharing and collaboration across the many organizations and sectors working in the field of urban innovation — overseeing access to and enabling the application of datasets that could be useful for Canadian companies, as well as research on and assessment of the outcomes enabled by the digital innovations themselves.

The future of the smart cities industry will require accountability for achieving public policy objectives, and trusted data sharing is essential to providing cross-sector confidence that smart cities are legitimately achieving public benefits.

Benefits of cross-sector data sharing

The cities that we inhabit are mirrored by a parallel structure of data — data that is created and collected to deliver public services and operational systems. A city’s data infrastructure — containing information about its physical form, the programs and services available, and its residents and businesses — includes data collected and managed by public agencies, as well as by the private-sector organizations that operate within the city.

Cross-sector data sharing has enabled quality of life improvements through aligning sectors to common public policy goals, such as reducing greenhouse gas emissions or

[18] See section 1.3 for additional information on the digitally enabled services proposed for Quayside

improving road safety. Cities make the data they collect freely available for others to use in order to foster transparency and accountability, spur private-sector innovation, and enable civic action. Trusted data sharing can open new data to citizens, who are increasingly technologically savvy and able to identify and develop citizen-led solutions to local problems. Private-sector organizations are increasingly developing offerings and products that enable the public sector to leverage the data that they hold for public outcomes.[19] Cities and public agencies are also increasingly seeking access to data collected by private-sector organizations to help understand and tackle the different challenges they face.[20] There is widespread recognition across all sectors that greater data sharing can have substantial benefits for public policy outcomes and city operations, and spur new forms of knowledge and value creation.[21]

For example, initiatives like the New Lab's Circular City program are exploring how "circular data" — the collection, production, and exchange of data and business insights between public- and private- sector stakeholders — can facilitate economic development to benefit both government and businesses. Crucially, business benefits extend beyond the companies generating the 'circular data'. Cross-sector data sharing can generate benefits across an entire ecosystem that includes government, businesses providing data, businesses outside the direct collaboration, as well as the public at large.[22]

Making data available for re-use and application by third parties can also advance the goal of equitable data access to benefit the public interest. This objective is rooted in advice from multiple sources, including:

- public consultations in which Torontonians expressed the sentiment that certain types of data could reasonably be considered a public asset;
- a Data Governance Advisory Working Group convened by Sidewalk Labs, which advised defaulting to making data accessible as appropriate; and
- the Sidewalk Toronto Fellows, who recommended developing an open-data portal to encourage innovation for public good.[23]

Defaulting to making appropriate data accessible and in accordance with defined data standards clearly advances this objective.[24] However, the benefits of data sharing and exchange must be balanced with risks to privacy and people in mind.

[19] For example, Mastercard's data philanthropy program and Waze Connected Citizens.
[20] Jack Hardinges, "Do Cities Have Access to the Private Sector Data They Need to Make Effective Decisions?," Open Data Institute blog, July 23, 2019.
[21] See section 4.5.3 for examples and additional information.

[22] *The Circular City*, New Lab City, New York, 2019.
[23] Sidewalk Toronto Fellows Report, Page 37.
[24] See section 1.5.2 for additional information on Sidewalk Labs' commitments.

Design considerations and challenges for data sharing efforts

Existing research on data collaborative structures emphasizes the importance of defining the purpose of the collaborative, and that each use case may require the development of its own set of structures as the public outcomes and nature of the data and data processing activity will vary.

There are several design considerations that should be contemplated for data sharing efforts, which can take any number of forms and can cover an entire spectrum of data access[25], collaborative structures[26], and technical architectures.

These design considerations include[27]:

- **Purpose** of the data sharing activities or the nature of the problem to be solved, which informs the organizational model.
- **Costs** — the availability of both data and human capital, as well as the incentives of the different parties involved, which drives the business model.
- **Potential risks** involved in sharing the data, such as risks to personal privacy, which then informs the organizational structure as well as the technical architecture.

Data sharing is an inherently costly and risky activity for organizations. No matter the data sharing model, every party involved expends resources (for example, expert staff time or to develop technology solutions) and is exposed to some level of risk (depending on the proposed use of and type of data).

The potential to derive benefit from data re-use cannot be realized until after both costs and risks have been incurred — this reality is one of the major reasons why data sharing is not broadly realized. Other barriers include the transaction costs related to developing bespoke contractual agreements for data sharing, which introduces even more friction into potential collaborations[28].

A potential approach for Quayside — a data collaboration hub

In order to unlock the value of data for public and ecosystem benefit, Sidewalk Labs suggests the establishment of a data collaboration hub — a large-scale data-access and computing resource dedicated to aggregating data at the neighbourhood scale.

---

[25] "The Data Spectrum," Open Data Institute website, accessed September 17, 2019 and "Mapping the Wide World of Data Sharing," Open Data Institute website, accessed September 19, 2019.
[26] GovLab, Data Collaboratives Explorer, accessed September 17, 2019.
[27] Summarized from GovLab, Data Collaboratives Canvas, accessed October 1, 2019.

[28] The Contracts for Data Collaboration initiative is one recent effort that seeks to help address this barrier by creating a shared repository of contractual clauses.

Defining an approach to support trusted data sharing in Quayside will support achievement of Waterfront Toronto's priority outcomes around *urban innovation* and *economic development*. An organizational and technical capacity to advance trusted data sharing can not just help ensure that digitally enabled services are implemented responsibly and delivering public benefit, but can also help support the growth of the local innovation ecosystem and address other pressing policy priorities.

This resource would complement the other digital infrastructure proposals in section 1.4 that enable the "testbed" characteristic of the neighbourhood as requested in Waterfront Toronto's concept for Quayside. Those digital infrastructure proposals - Koala, SDN, SuperPON, distributed verifiable credentials - focus on making it easier to deploy and test new technologies. A data collaboration hub could augment that digital infrastructure by enabling collaboration between researchers, policy analysts, and innovators to evaluate the effectiveness of technologies piloted at the testbed.

It could also help set priorities for data sharing in a manner that reflects both user demand and potential beneficial impact. Academic researchers and institutions already enter into data sharing agreements and establish data portals and computing environments that advance scientific collaborations to achieve specific objectives, making them well placed to lead and coordinate the stewardship of data to achieve — and crucially, measure — public outcomes.

A hub for data collaboration could provide a resource for fostering innovation and quantitative urban research that would be unlike anywhere else. This data collaboration hub could oversee access to the datasets collected through the digitally enabled services at Quayside that could be useful for research that assesses the public outcomes enabled by the digital innovations themselves - this type of connected data and data access has been noted as crucial to "core analyses that can make healthier, more equitable communities possible."[29]

This data collaboration hub could also explore operational and technical solutions for multi-sector data sharing in ways that protect privacy while ensuring visibility into data re-use and applications. Sidewalk Labs believes it would also be important to advance a research agenda that examines and assesses the effectiveness of cross-sector collaborations in cities, explores data ethics, and advances privacy-preserving methodologies that can unlock the value of data in trusted ways.

Exploring the potential of these ideas will be a key topic for Sidewalk Labs' discussions with stakeholders in the coming months. For example, discussions with stakeholders could include the following topics:

- Identifying initial priorities for trusted data sharing. These could be use-case driven by Waterfront

[29] Aaron Orkin, "Sidewalk Labs Project Is a Public Health Opportunity," *Toronto Star*, July 30, 2019.

Toronto's priority outcomes, ensuring that the supply side (data streams) is being matched by policy demand for the research that the data can potentially be used for.

- Exploring methods to develop and implement state-of-the-art technical architectures for data sharing and auditable computing, such as using synthetic data, differential privacy, and homomorphic encryption; and engage academic and industry experts alike in critiquing and testing the approaches.
- Enabling the development and sharing of repeatable frameworks for trusted data sharing, including business and organizational models and technical architectures. The hub could specifically foster knowledge sharing of how those frameworks can be applied, with both collectors and potential users of data.
- Analyzing the ethics and potential risk/benefit trade-offs of data re-use activities , which could be led by academic or partner institutions. Traditions of independent peer review can be applied to help ensure that data applications are appropriate and potentially beneficial, or conversely, that potential impacts of the use of certain data are adequately studied. This could complement and help address an increasing need to advance ethical data use practices as advanced computing techniques are increasingly used in research.[30]

[30] Jane C. Hu, "The Tricky Ethics of Using YouTube Videos for Academic Research," *Pacific Standard*, June 7, 2019.

With the diversity of non-profit, public-sector, academic, and private-sector actors in Canada already exploring a variety of governance models and advancing technical architectures to enable trusted data sharing, dedicated resources to establish this collaborative function could accelerate and amplify the efforts of the existing ecosystem. One way to advance this might be to have the collaboration hub anchored at the Urban Innovation Institute (UII); this would be explored as part of the areas of UII's business planning enabled by Sidewalk Labs' $10 million contribution.

Local precedents of data sharing efforts

There are a multitude of organizations and companies working to pilot and implement new frameworks, approaches, and tools for data collection, beneficial use, and responsible data sharing in Toronto, Ontario, and throughout Canada. These are efforts that can inform the development of an approach to trusted data sharing at Quayside, and offer a glimpse of the level of interest and activity in data sharing that already exists in the local innovation ecosystem. A non-exhaustive list of these efforts is included below as a reference.

- MaRS Discovery District:
    - With Waterfront Toronto, advanced an international multi-sector stakeholder workshop to explore practical solutions for responsibly sharing data in order to unlock the potential of smart cities and developed a

primer on Civic Digital Trusts for the general public.
    - Worked with Compute Ontario to develop design recommendations for an Ontario Personal Mobility Data Trust, including developing a board game to help participants explore the dynamics and incentives for stakeholders to join a data trust.
    - Funded by the Public Health Agency of Canada (PHAC) to identify new sources of data and new approaches to modernize population health measurement, has launched The Healthy Neighbourhood Data Challenge to "identify and create novel datasets, data sources, and analytical methodologies to better understand the physical environment" and support the design of healthier neighbourhoods. Applicants may come from any sector, including academia and the private and public sectors.
- Toronto-based ThinkData Works developed Namara, a product that synthesizes the massive variety of open datasets that have been released by every level of government across dozens of jurisdictions. Namara makes data discoverable and available in a standardized way from a common, central repository enabling residents and businesses to use public data effectively. The platform not only enables use of data, but also has the potential to protect and limit its use where appropriate.
- Toronto-based Cinchy has developed an enterprise-grade Data Collaboration Platform that enables people, systems, and artificial intelligence to securely collaborate on data within a real-time network. This architecture completely eliminates the need for organizations to perform complex data integrations (i.e. make data copies) that are mandatory with the traditional "app-centric" approach to delivering new technology. Cinchy allows owners to maintain complete control of their data by allowing them to offer secure access to third parties, rather than sharing copies. Cinchy is currently operational within several tier-1 banks and commercial real-estate companies who use it as a foundational platform to deliver hundreds of mission-critical projects with embedded data privacy.
- Canadian company Sightline Innovation has a patented data trust and AI software product (SID and SIMON) that enables data governance, control and auditable interoperability of data assets between trusted data partners. Their products help protect against data compliance risk, capitalize on data monetization capabilities and leverage data assets for securitization. SID uses a variety of technologies to provide a means of defining scalable data policy constructs, preserve privacy and enable distributed AI computation. They currently work with the Public Health Agency of Canada, the City of Toronto and on data trust project deployments with the Canadian Superclusters program. They are also working with a global professional services firm and IOT firm on large

scale Municipal Data Trust deployments. Sightline has defined an open data agreement standard, DIFANO, to enable interoperability of data between organizations and enable the automation of data sharing legal agreements between them.

- Researchers Lisa Austin and David Lie at the University of Toronto have developed a legal-technical infrastructure they have termed a "safe-sharing site" that offers an alternative to the strategy of de-identifying data and releasing it, a process that doesn't reduce the risk of re-identification to zero. The goal is to provide a privacy-protective environment where computations are performed securely without the release of any raw data, and where data use is transparent and auditable.[31]
- Mozilla Foundation and Canadian company Element AI recently announced a strategic partnership to begin collaborating to explore data trusts as a way to give both citizens and consumers more control – and greater social return – over the use of their personal information.[32] The partnership will fund and support policy and legal research, along with the technical and design components necessary to make data trusts a practical reality. This partnership builds on the work Element AI had previously conducted with Nesta, exploring data trusts as a way to reform current models of data governance and restore public trust.[33] Mozilla is a nonprofit that believes the internet must always remain a global public resource, open and accessible to all.
- Ontario's Smart Metering Entity (SME) is a public-sector body with a mandate to share data with public and private third-party actors in the public interest. SME developed a centralized data governance system to manage smart meter data on electrical consumption and protect consumer privacy. SME enables third-party access to de-identified data to spur innovation in the development of new products and services.
- Toronto-based smart thermostat company Ecobee runs a "donate your data" program, which enables users to share anonymized data with researchers to address sustainability, health, and comfort challenges.
- The Maple Leaf Sports and Entertainment Foundation's MLSE Launch Pad is creating a data trust to collect and share data among Ontario non-profits to better measure and understand how sport can help improve the lives of youth.
- Toronto Public Library (TPL) is a global leader in its work to support digital literacy and practices of digital knowledge sharing. The organization's core values include equity, inclusion, diversity, integrity, and intellectual freedom. Based on this work, TPL was

---

[31] Lisa M. Austin and David Lie, "Safe Sharing Sites," *New York University Law Review,* forthcoming 2019.

[32] Element AI, "Element AI and Mozilla Foundation Partner to Build Data Trusts and Advocate for the Ethical Data Governance of AI," 2019

[33] Element AI and Nesta, *Data Trusts: A New Tool for Data Governance*, 2018.

mentioned in the Toronto Region Board of Trade's 2019 report as a potential authority for developing a Toronto Data Hub and related policies.

If the project is approved, the Urban Innovation Institute and the consortium that advances it could serve to coalesce these efforts in a way that enables knowledge sharing and learning, and foster future tests and pilots of these innovative approaches in collaboration with local innovation hubs and accelerators. A portion of the Urban Innovation Institute seed funding could support exploring business models and possible approaches to establishing a data collaboration hub together with consortium partners.

Working closely with Waterfront Toronto, a key priority as the project progresses will be defining the business model and operations for trusted data sharing, including how Toronto and Ontario's unique companies and organizations could play a role.

3.2.3.3 Potential Villiers West urban innovation campus

Toronto's waterfront has already become an important corridor of activity driving innovation. First-movers included the offices of Corus Entertainment and George Brown College. Recently, the Daniels Waterfront City of Arts opened, including new cultural incubators like the Remix Project, HXOUSE, Artscape Daniels Launchpad, and OCADU's waterfront presence. Menkes' Waterfront Innovation Centre is under construction and will be home to an expansion of MaRS to the waterfront and a major consolidated global office for the communications agency WPP. Hines is planning two tall timber buildings in Bayside that will further this innovation corridor up to Parliament Slip. Waterfront Toronto has also established a partnership with Beanfield Microconnect, which pioneered one of Canada's first open-access high-speed networks, providing broadband options for all tenants in the area and dramatically higher speeds than North American averages. This work led to Toronto being selected as the Intelligent Community of the Year by the Intelligent Community Forum (ICF) at its annual summit in New York. The title is awarded to the community that best creates inclusive economic opportunity and improves competitiveness through the use of broadband and information technology to collaborate, innovate, attract investment, improve the delivery of government services, and raise the quality of life for its residents.

Based on the performance at Quayside, Waterfront Toronto recognizes that there could be substantial public benefits by providing for an area of future expansion of the initial phase beyond Quayside to the area such as Villiers West to further Waterfront Toronto's objectives, particularly in relation to economic development. Expansion to other lands would be subject to future Waterfront Toronto approvals and any applicable land disposition processes required by the City of Toronto.

In the MIDP, Sidewalk Labs proposed the creation of an urban innovation hub on the western side of Villiers Island. This hub would be home to a mix of tenants and the Urban Innovation Institute (UII), and would serve as a campus for the sector and an economic and cultural engine for the area. Sidewalk Labs also proposed building a new Google Canadian headquarters to anchor the development proposal. While both Quayside and Villiers West would be mixed use, the high concentration of commercial uses in Villiers West would be a key economic catalyst to support Waterfront Toronto's overall revitalization of the Port Lands and to support the city's objective, as detailed in the Port Lands Planning Framework, of distinguishing waterfront revitalization in the Port Lands by focusing on a greater proportion of non-residential and innovation economy uses.[34] Sidewalk Labs will evaluate whether whether or not to seek to proceed with these or alternative plans for Villiers West, subject to required public approvals.

To serve as an anchor for the new district, Alphabet would target up to 500,000 square feet. That would be sufficient to accommodate as many as 2,500 jobs, the majority of which would be for Google employees (though actual hiring would depend on market conditions and business requirements). Securing Google as a main tenant would allow development to proceed much sooner than simply waiting for market conditions to change. Fundamental to Google's approach is the concept of a connected campus that encourages collaboration with neighbouring businesses, institutions, and communities. In the past, this approach has included maintaining active partnerships with local universities and supporting an emerging ecosystem of new small businesses and startups. In just the last year, Google Canada has supported important ecosystem initiatives with incubators and accelerators, including Communitech and DMZ, and the intent would be to further ecosystem-building initiatives at Villiers West.

Villiers West would be designed as an innovation campus that models a new approach to expanding technology headquarters in dense urban areas. In addition to the expanded Google Canada headquarters and a permanent home for the UII, there would be additional space for startups and civic innovators, including companies working in digital media that would complement the growing film district farther to the east. The innovation campus on Villiers West would be a perfect location to seed and grow innovative Canadian companies that can build their business locally in a cutting-edge environment.

Consistent with Sidewalk Labs' inclusive and mixed-use development approach, the hub would have extensive public programs throughout the ground floors and be seamlessly interwoven with the neighbouring park and eventual residential developments to the east.

It is well recognized that innovation is greatly facilitated by the cross-pollination of ideas from different people and

[34] For more information, please see the Planning Policy Justification Report written by Urban Strategies, which evaluates the proposed development plans contained in the MIDP against the provincial and municipal land-use policy and planning framework.

organizations in close proximity to one another.[35] Economic clusters show that cross-pollination from a few successful businesses can spawn exponential growth of other businesses in related fields as knowledge, talent, and capital flow within a tight geographic and relational network. Customers, advisors, and investors are more easily accessible when clustered and working in an environment open to innovative approaches and solutions. An urban innovation hub means that companies would have an opportunity to implement their solutions, within a supportive infrastructure and policy environment, at a district scale close to home.

Unique conditions to support community and urban innovators

A combination of unique physical and digital conditions in Villiers West will support further ecosystem growth.

The urban design of the campus would be based around expanding public access and deeply integrating office uses with residential areas. By integrating the campus into the street network, with connections to the rest of the city running to and through the site, the innovation hub can become a vital part of the community rather than a closed campus. Flexible ground floor space would host retail, production, arts, and community uses, with public passageways and interior arcades providing additional ways to move through the site, inviting a range of uses and visitors.

[35] Michael Porter, "The Competitive Advantage of Nations," *Harvard Business Review*, March–April 1990, 83–84.

Sidewalk Labs has emphasized flexibility and adaptability in the built environment to create the conditions for rapid innovation. For example, streets, public spaces, and buildings would have electric power, connectivity, and built-in rigging, making it easy for film shoots to take place with minimal disruption. This same infrastructure is valuable for urban tech startups working on new products that require installation in the urban environment. Today, one of the biggest barriers for many urban tech companies is an initial deployment, because of the difficulty of getting approvals to integrate with power, connectivity, poles, and buildings. To tackle this challenge, Sidewalk Labs has designed a standardized mount called "Koala" that would make it fast, inexpensive, and safe to install a device on a light pole or other street fixture by providing a sturdy physical mount as well as power and network connectivity. Sidewalk Labs estimates its mounts would reduce the time of installation by roughly 92 percent — down from 30 hours today to two hours.

Sidewalk Labs believes that the success of Villiers West as the hub of an urban innovation cluster should be measured in part by the number of Canadian innovations tested, refined, and implemented in the district. Sidewalk Labs has learned from the development of other ecosystems, such as the web and the iPhone, that to be successful, third parties depend on open hardware and software as well as on agreed-upon standards and protocols to successfully deploy their ideas. This digital infrastructure is a core condition for innovation. A set of published standards around open data architecture, access, and sources would enable third parties to build upon a shared foundation, supported by a common set of security, formatting, and communication standards.

3.2.3.4 Precedent-Setting Standards

The value generated by the Quayside plan for the Canadian ecosystem is not only about business opportunities. It is also about making sure that a Canadian approach can help shape the standards for smart city projects worldwide. When civic leaders from around the world look to implement cutting-edge urban solutions in their own cities, it is Toronto that they could see as the model. Canadian businesses can work now with Waterfront Toronto, government partners, and Sidewalk Labs to pioneer industry-setting open standards that will form the basis of the Quayside implementation and be used in smart cities projects around the world.

This standard setting is already underway, and using the project as a vehicle can help advance this work. Sidewalk Labs intends to further engage with the work underway by groups such as the CIO Strategy Council to build on their existing efforts to establish standards that value inclusiveness, openness, public interest, and respect for individual rights and privacy. These standards include the ethical design and use of automated decision systems and third-party access to data, and will inform the groundwork for Sidewalk Labs' global responsible technology standard.

The CIO Strategy Council is accredited by the Standards Council of Canada (SCC) to develop and submit standards to SCC for acceptance as National Standards of Canada. The first set of these standards – CAN/CIOSC 101 on the Ethical design and use of automated decision systems was recently approved and published[36]. Efforts to develop several other standards are underway, and the draft standard for privacy and third party access to data that is currently available for public review.

Our engagement is intended to focus on the role that Sidewalk Labs can play in spurring standards (where necessary), and otherwise supporting the development of related standards, and in addition on the ways in which this process can feed into the work Sidewalk Labs is already undertaking in engaging the wider Canadian innovation ecosystem.

For example, the UII could serve as an effective venue to deliver accreditation programs based on these standards as part of broader efforts to foster skill building and build sector capacity. These standard-setting initiatives by the Canadian public and private sectors will become the basis of Quayside. They will deeply inform the work of Sidewalk Labs as it works towards a responsible and accountable model for smart cities globally. Sidewalk Labs believes that responsible technology includes a framework of responsible data use and a

[36]" CIO Strategy Council publishes National Standard of Canada for Automated Decision Systems." October 2, 2019. https://ciostrategycouncil.com/2019/10/cio-strategy-council-publishes-national-standard-of-canada-for-automated-decision-systems/

commitment to responsible artificial intelligence underpinned by the principles of beneficial purpose, transparency and clarity, accountability, and a respect for human dignity.

3.2.3.5 Sharing value over time with the public sector

In the draft MIDP, Sidewalk Labs proposed entering into a first-of-its-kind profit-sharing agreement in which the public sector would receive a share of Sidewalk Labs' global profits on "Testbed Enabled Technologies" for a period of 10 years starting from the first sale to a second customer. Based on Waterfront Toronto's request, Sidewalk Labs has agreed to shift to a revenue stream on products and services piloted in Waterfront Toronto-facilitated testbed area, based on global net revenues, where net revenue will mean all consideration received by Sidewalk Labs less agreed upon deductions. The percentage and time frame for the value share will be finalized before entering into the Principal Implementation Agreements.

Testbed Enabled Technologies are those that are deployed at scale for the first time in Sidewalk Labs' project in Toronto. Such deployment should not have been possible but for the public sector creating the conditions for innovation required to effectively pilot the solution. Such conditions may include actions and inputs that are required to effectively pilot the solution (for example, giving access to physical space, mandating the use of common software standards to enable compatibility and interoperability, facilitating required regulatory approvals, providing sufficient scale to achieve desired outcomes, and providing an ecosystem that integrates all of these conditions).

Background research

Before providing this proposal, Sidewalk Labs conducted research to identify relevant precedents for the value share of future upside generated from businesses or products enabled by the public sector providing access to physical space, regulatory relief, or other conditions comparable to those Waterfront Toronto has proposed. Sidewalk Labs supplemented this research with a report from a globally recognizable consulting firm, asking them to look into any comparable examples where a public sector organization, quasi-public-sector organization, real estate developer, or a corporate or academic campus provided value to a private-sector organization for innovative development and where some value in future upside was agreed to be shared back. The conclusion Sidewalk Labs drew from all this research is that this proposal is truly unique. Of all the examples found, only one featured a scenario similar to the proposal for Toronto: several public entities created an innovation zone between Orlando and Tampa, Florida, as a testing ground for a private third party to conduct testing on connected and automated vehicles and their communications with other objects. In this innovative project, no value was shared back with the public sector on future value created from the testing. Rather, the entities running the innovation zone collected fees for use of the testing facility during the testing period.[37]

Sidewalk Labs also found examples of more traditional business arrangements in which the public sector made lands available for exploitation of certain business lines, such as landfill methane gas collection, to facilitate sales by private entities, with the private entity providing a royalty back to the public sector. Sidewalk Labs found one Canadian example in which the royalty rate received by the public sector was 4 percent of methane gas sales.[38] In a U.S. example, a private company paid a 2 percent royalty on methane gas sales for the first 3 years and 4 percent each year thereafter to the public party during the 20-year term of the contract.[39] Another U.S. example featured the public sector receiving a 13 percent royalty share over methane gas sales. The higher royalty rate owed in this transaction was warranted due to the private party only operating and maintaining the system, not building or installing it.[40] None of these examples featured innovation by the private party that might result in future upside that could be shared back with the public party.

Sidewalk Labs is also aware of examples where universities have provided private parties with access to their intellectual property for private exploitation. In an example from Canada, Simon Fraser University provided Analog Devices with a perpetual license to use, make, have made, import, develop, modify, enhance, copy, reproduce, promote, market, sublicense, sell, offer for sale, and distribute specific technology. Analog Devices had to pay a 1 percent royalty on revenue with a cap up to USD $100,000. However, if the corresponding patent application was not issued by the U.S. patent office with device claims, the royalty rate was reduced to 0.5 percent and the cap became USD $50,000. In a U.S. example featuring a license by Lawrence Livermore National Laboratories to various private parties over specific technology, a royalty fee of 3–5 percent of revenue was owed by the various licensees depending on the technology.

The above examples were the closest comparators Sidewalk Labs was able to find and, for the most part, they are not

[37] See explanation of Suntrax project jointly developed by Florida's Turnpike Enterprise (FTE), Florida Polytechnic University, Florida Department of Transportation (DOT), National Aeronautics and Space Administration (NASA), summarized in the Deloitte Report which will be made public when it is finalized.

[38] See explanation of Integrated Gas Recovery Systems Public-Private Partnership Arrangement with Essex-Windsor Regional Landfill (Ontario), summarized in the Deloitte Report which will be made public via the Sidewalk Toronto website, in the document library, when it is finalized.

[39] See discussion of Concession/Property Rights Related Agreements between Renovar Energy and Baton Rouge, summarized in the Deloitte Report which will be made public via the Sidewalk Toronto website, in the document library, when it is finalized.

[40] See discussion of public-private partnership agreement between the City of Fort Smith, Arkansas and Neo Corp, summarized in the Deloitte Report which will be made public via the Sidewalk Toronto website, in the document library, when it is finalized.

overly similar to what is proposed in Toronto. Hence, after canvassing all the publicly available examples, we found no situation where a stake in future upside on an innovation was shared with a public-sector organization that provided opportunity akin to what Waterfront Toronto has offered. This lack of precedent supports our hypothesis that Sidewalk Labs' proposal is unique.

3.3 Next steps for engaging the urban technology ecosystem

This proposal is merely a first step towards Sidewalk Labs' long-term commitment to growing the urban technology ecosystem in Toronto and Canada. Over the coming years, Sidewalk Labs intends to build on these initiatives, and to develop new initiatives based on feedback from stakeholders in Toronto and across the country.

3.3.1 Engaging across all sectors

Sidewalk Labs has been engaging with stakeholders within the Canadian innovation space to better understand their challenges, where they see opportunities, and how Sidewalk Labs' efforts can best support the ecosystem. Sidewalk Labs has crafted these initiatives in response to what it has been hearing. These initiatives align with what Sidewalk Labs believes to be its strengths and with what it believes will deliver the best results. Sidewalk Labs intends to continue engaging with the innovation ecosystem in Canada over the coming months to hear feedback on it proposals and intends to take a proactive approach to engaging a range of stakeholders — each of which plays a key role in the health of the ecosystem.

3.3.1.1 Incubators and accelerators

Sidewalk Labs will continue to engage with a range of incubators and accelerators in the ecosystem to better understand how these proposed initiatives can generate value for Canadian ventures. This includes MaRS, Ryerson DMZ, the Impact Centre at the University of Toronto, Communitech, and others across the region that are connected to the startup community in Canada and internationally. Because of their specialized insight into the challenges and opportunities facing Canadian ventures, representatives from various incubators and accelerators will be asked to provide feedback on Sidewalk Labs' proposals related to the Urban Innovation Institute, the programs to scale management excellence, the procurement of Canadian technology, as well as Sidewalk Labs' approach to mobilizing venture capital in the sectors related to urban technology. Sidewalk Labs will meet with these representatives in the initial planning stages of the initiatives and throughout their implementation.

Sidewalk Labs has been engaging with many leaders in the ecosystem to discuss how the Quayside plan could best support the evolving urban innovation ecosystem in the

Toronto region. For example, Sidewalk Labs has shared its proposed initiatives with MaRS to gather feedback and worked to incorporate as much feedback as possible into this document. Sidewalk Labs has also been discussing with Brookfield Institute for Innovation and Entrepreneurship about independent, thought leadership research they might lead in this evolving space, working closely with accelerators like MaRS, DMZ and others in the region. This could include near-term initiatives such as convening a range of stakeholders and preparing a position paper to define the urban innovation sector and the unique opportunity for Toronto, in addition to recommendations on how best to support the continued maturation of this sector. The outcomes of these engagements will be an important input to Sidewalk Labs' thinking around the creation of enduring value for the ecosystem, and Sidewalk Labs would participate as appropriate.

3.3.1.2 Academia

Sidewalk Labs believes in the importance of advancing work on the Urban Innovation Institute quickly. Sidewalk Labs recognizes the central role that academic institutions would play and intends to continue early discussions with key institutions about how best to structure the Urban Innovation Institute (UII) and to gather feedback on its other proposed initiatives. The growth of the Canadian urban innovation ecosystem requires advancing applied research and innovation capacity-building for all key stakeholders from startups to government. The UII could serve as a hub for research focused on urban challenges that helps to inform the future of city-building by facilitating closer integration with prototyping and policy execution efforts.
The first set of discussions with representatives from academic institutions will focus on establishing a process to identify a lead for the UII consortium and key issues that would need to be considered in the contribution agreement Sidewalk Labs has proposed. Sidewalk Labs is proposing to enter into an agreement with a single institution for funding the UII and they will be responsible for establishing the consortium and providing initial administrative support for the UII. Sidewalk Labs will be seeking feedback on this approach from academic institutions, including those who were involved in establishing the Vector Institute, which was set up using a similar strategy.

Ongoing discussions with academic institutions will provide further guidance on how the UII could involve Toronto's innovation ecosystem by engaging their faculty in cutting-edge research and creating learning opportunities for their students, as well as explore the idea of a cross-sector data collaboration hub. These ongoing engagements will be critical to identifying the institutional gaps within the ecosystem that the UII can service, as well as ensuring that the UII complements existing institutions.

3.3.1.3 Civil society

Civil society, including civic leaders, non-profit organizations, and those working at the intersection of technology and public interest, would have a critical role to play in the UII and in establishing approaches to trusted data sharing and standard setting.

Sidewalk Labs has committed to working with standard-setting bodies in Canada to support their work for a global responsible technology standard. This engagement demonstrates a genuine commitment to following Canadian-set standards and a collaborative approach to the further development of standards with Canadian partners. This engagement will include meetings with the Standards Council of Canada and the CIO Strategy Council regarding the many new standards that are under active development and being considered.

3.3.1.4 Canadian companies

Canadian companies are the cornerstone of the ecosystem Sidewalk Labs wishes to support. Sidewalk Labs will undertake proactive outreach to Canadian companies, both startups and scale-ups, in conjunction with its venture outreach that is already underway. During the first phase of consultations, Sidewalk Labs would seek feedback on the proposed initiatives intended to benefit Canadian companies working in the urban innovation space. The companies being considered for consultation represent different industries related to urban innovation, with a focus on infrastructure, construction, and information communication technology. In addition to Toronto-based companies, Sidewalk Labs is also seeking to engage companies headquartered outside of the city core and in other parts of Canada.

For example, Sidewalk Labs met with York Link - York Region Economic Development - which is mandated to facilitate partnerships for the business community in York Region, to learn about the Region's significant technology cluster and the ecosystem beyond Toronto. This initial meeting resulted in Sidewalk Labs appreciating the breadth of innovation in the region that could contribute to the project. The next step will be further engagements directly with companies in York Region to share more about the opportunities presented by the project and to get guidance and advice on how initiatives proposed by Sidewalk Labs could be improved to align with the interests of other the broader sector. This model of engagement can then be replicated in other regions of the Greater Toronto Area, recognizing that different part of the ecosystem possess unique specialities.

Furthermore, Sidewalk Labs seeks to engage with stakeholders who have a broader view of the private sector as a whole who could offer feedback on Sidewalk Labs' efforts to create enduring value to the Canadian urban innovation ecosystem. National and regional business associations and CEO councils will have important insights into the needs of the Canadian private sector related to urban innovation.

Section 4

Overview of Existing Policies and Approaches for Smart Cities and Digital Governance

Abstract

One of the frequent requests from Waterfront Toronto, their advisors such as the Digital Strategy Advisory Panel, and the public has been an acknowledgement by Sidewalk Labs of the existing policy context in which the Master Innovation and Development Plan (MIDP) is situated. The Sidewalk Toronto project is part of a larger discussion taking place across Canada and internationally about the best ways to use technology responsibly to improve cities. This conversation necessarily brings government, civil society, and the private sector together. Government is actively leading on new policies, and there are strong precedents in Canada and internationally to build upon. This section aims to provide this context, and also to contribute to a broader civic discussion on smart cities — recognizing both their challenges and opportunities.

Table of Contents

Figures

Tables

Section 4: Overview of Existing Policies and Approaches for Smart Cities and Digital Governance

4.1 Introduction

In the past decade, cities have leveraged new technological tools and increasing amounts and types of data to better deliver and expand services. Data is a critical feature in cities fulfilling their mission to residents. As the UN Secretary General's Independent Expert Advisory Group on a Data Revolution for Sustainable Development noted in 2014, "*Data are the lifeblood of decision-making and the raw material for accountability. Without high quality data providing the right information on the right things at the right time; designing, monitoring, and evaluating effective policies becomes almost impossible.*"[1] As new technologies continue to come together in the digital and physical worlds, the opportunities for individuals, industries, and governments to use data and information continue to grow.

Many governments have started investing heavily in digital infrastructure and technology, as well as crafting public strategies to shape opportunities and respond to the range of challenges that smart city technologies present. In this vein, Waterfront Toronto — the public advocate and steward of waterfront revitalization formed by federal, provincial, and city governments — issued a 2017 Request for Proposals (RFP) calling for an "innovation and funding partner to help think through tough urban challenges and create a strong and compelling vision" for the development of Quayside, a 4.9-hectare (12-acre) parcel of land on the Toronto waterfront. Across Toronto, and Canada more broadly, a nascent ecosystem of digital policies and vigorous public discourse about ethics and technology has advanced along with the call for innovation and investment.

It is against this backdrop that the draft Master Innovation and Development proposal (MIDP) from Sidewalk Labs envisions Quayside as a model of inclusive urban growth enabled by digital innovations and technologies.

4.1.1 Purpose of this section

One of the frequent requests from Waterfront Toronto, their advisors, such as the Digital Strategy Advisory Panel, and the public has been an acknowledgement by Sidewalk Labs of the existing policy landscape in which the MIDP is situated. This section aims to provide this context and to contribute to a broader civic discussion on smart cities that recognizes both their challenges and opportunities. Sidewalk Labs recognizes the varied political and ethical concerns that accompany technology use. This section discusses some of the ways in which communities are addressing these concerns through a

[1] Data Revolution Group. 2014. *A World That Counts: Mobilising the Data Revolution for Sustainable Development.*

range of governance and technological approaches, giving specific attention to the Canadian policy landscape and highlighting national and international initiatives in urban innovation and technology. This section is not an attempt to provide a full history of smart cities or an exhaustive review of digital innovation, but, rather, it is an attempt to outline current policies, conversations, and select precedents that have informed this proposal and continue to influence Sidewalk Labs' thinking. Readers interested in the Canadian context specifically should refer to works by the organizations Open North and Future Cities Canada, such as the Open Smart Cities Guide[2] and How To Be Smart(er) in Mid-Sized Cities in Ontario[3].

Sidewalk Labs also recognizes the rapidly evolving environment of this proposal, with new commentary, research, and policy being actively developed. Accordingly, this section offers a snapshot in time and is understood as one step in the urban innovation conversation, which will continue to unfold.

4.2 Critical topics in digital governance and technology

The increasing use of technology and digital infrastructure in cities and in our daily lives has produced new capabilities in approaching urban challenges, such as mobility and sustainability. It also has enabled many cities to achieve better outcomes and gain efficiencies for public benefit. For example, the city of Boston was able to save $5 million per year and eliminate 20,000 pounds of carbon emissions by optimizing bus routes for Boston's public schools.[4] In London, a collaboration between a design studio and the Royal London Society for Blind People's Youth Forum created an app called Wayfindr that directs visually impaired transit users through London Underground stations using smartphones and Bluetooth beacons.[5]

Technology innovation has always been fundamental in cities. Across history, cities have been shaped by the advent of new technologies, such as the steam engine, electricity, elevators, and the private car. Today, there is incredible potential for digital innovation to improve urban living. Yet meaningful cooperation is necessary to realize the benefits of urban digital innovations in a responsible way.

At the same time, the increasing use of digital technologies in our urban infrastructure and public service delivery has ushered in a number of political and ethical questions. Around the world, as well as in Toronto, communities are voicing concerns about:

[2] OpenNorth. "Open Smart Cities Guide V1.0," April 2018.
[3] Code for Canada and Evergreen, "How to be Smart(er) in Mid-Sized Cities in Ontario," February 2018.
[4] Jane Wiseman, "Discovering the True Value of City Data Experts," *Data-Smart City Solutions,* Harvard Kennedy School Ash Center for Democratic Governance and Innovation, November 8, 2017.
[5] Katie Collins, "Wayfinder app helps the blind navigate the Tube," *Wired,* August 12, 2014.

- **Privacy and surveillance:** How is privacy preserved? How are security risks reduced?
- **Ethics and inclusion:** Who has a voice? How can cities ensure equitable access to services? How do ethics and values play a role in technology development?
- **Transparency and accountability:** Who is accountable? How are decisions made? How is data controlled, shared, and retained?
- **Adaptability:** What makes cities flexible and able to accommodate change?

These topics are a critical part of responsible smart city development and of our digital society more broadly. Included below are brief summaries of these key challenges and concerns.

4.2.1 Privacy and surveillance

A digital society increases the amounts, types, and granularity of data available about individuals and their activities. This increase in data also expands the potential for surveillance.[6] And surveillance can compromise the right to privacy and our values in a free society.

The Office of the Privacy Commissioner (OPC) reports that 92 percent of Canadians have concerns about privacy.[7] Privacy and surveillance risks can originate from the mundane — from common items in our homes, such as smart devices (Roomba maps the floors of your home) to our smartphones apps (weather apps can track detailed locations and movements of users). There also is emerging research that demonstrates that techniques which once offered privacy protection, like anonymization, no longer consistently safeguard identity.[8]

Security is a fundamental component in preserving privacy. Security relates to the technical architecture and practices fundamental in protecting digital infrastructure and data from breaches, attacks, and thefts. With the increasing number of devices and volume of data, there is more to protect across a range of actors and instruments. Privacy breaches and thefts have been reported over a range of industries and sectors, including, for example, consumer brands (e.g., pharmaceutical company Merck in 2017, hospitality company Marriott in 2018, and banking services company Capital One in 2019) and government and reporting agencies (e.g., the U.S. Office of Personnel Management in 2015; and Equifax in 2017). Service interruptions from cyber attacks are on the rise and, increasingly, governments are targets, with attacks impairing the delivery of public services (e.g., attacks in

[6] Teresa Scassa and Merlynda Vilain, "Governing Smart Data in the Public Interest: Lessons from Ontario's Smart Metering Entity," Centre for International Governance Innovation, July 10, 2019.

[7] Business Council of Canada, "Data Driven: Canada's Economic Opportunity," July 22, 2019.

[8] Gina Kolata, "Your Data Were 'Anonymized'? These Scientists Can Still Identify You," *The New York Times*, July 23, 2019.

Estonia in 2007, Atlanta in 2018, multiple attacks in Ontario in 2018, and attacks in Baltimore in 2019).

4.2.2 Ethics and inclusion

The growing reliance on digital technologies in everyday activities raises concerns about bias, discrimination, and exclusion. Existing and emerging techniques in computing, including artificial intelligence (and machine learning), rely on algorithms that can obscure visibility into how they function and distance people from decision-making. Historically, algorithms have not been held to the same standard of transparency as human decision-making, despite the potential for great (or even greater) impact.[9]

There is an increased recognition of how bias and discrimination can be encoded in data and computational design. Recent examples of such issues include: judicial systems that rely on data that is the product of racially discriminatory beliefs and practices to determine bail requirements; hiring models that penalize female candidates; lending terms that charge racial minorities higher interest rates; voice recognition technology that can't recognize speech impediments or disorders; and, in research fields, tests that fail to recognize different mobility abilities. The lack of diversity in technology also underscores such concerns and highlights the risk of creating technology in seclusion from its users.

As scholars and advocates inside and outside the tech industry have highlighted, historically there has been little discussion about ethical decisions in technology, nor a robust forum for such discussions. In addition to exclusion created by bias and discrimination, communities are concerned about a lack of the access, skills, and financial resources required to participate in or benefit from an increasingly digital society. Even with free and open access to digital infrastructure and assets (such as data), a lack of skills and other factors can exacerbate existing differences in achievement or benefit.[10]

4.2.3 Transparency and accountability

Individuals and communities are calling for more transparency in data collection and use. There is a lack of public knowledge about how data is collected, used, gathered, shared, and stored, both from online digital platforms as well as from the government and various actors in the public realm. For example, a nationally representative survey in the UK found that half of respondents would like to know how their data from online accounts and activity is used

[9] Will Knight, "Biased Algorithms Are Everywhere, and No One Seems to Care," *MIT Technology Review,* July 12, 2017.

[10] Bianca Wylie, "Open Data Endgame: Countering the Digital Consensus," *CIGI Paper* No. 186, Centre for International Governance Innovation, August 20, 2018. Sean McDonald, "The Open (Data) Market," *Medium,* February 1, 2016.

but don't know how to find out this information.[11] The OPC reports that 64 percent of Canadians don't have a good understanding of what the national government does with personal information.[12]

The issue of meaningful consent is pertinent to such transparency concerns. In the same UK survey, 89 percent of respondents wanted clearer terms and conditions of use.[13] An analysis of privacy policies across websites, apps, and social media sites found that these policies are, on average, 4,000-5,000 words and require 20 minutes to read.[14]

There is also a related concern and a lack of understanding about who decides what to do with data.[15] This is a general area of confusion for most residents in cities worldwide.[16] As Canadian legal scholars have noted, the context and parties involved determine the applicable laws, which vary depending on sector and type of information.[17] From a stewardship and regulatory perspective, historically siloed governance structures in the public sector don't address the broad-reaching nature of data.[18]

4.2.4 Adaptability

An additional set of concerns arising around technology includes the risk of investing in systems that lack flexibility or create an overreliance on vendors. Proprietary systems run the risk of creating silos, stifling interoperability, and creating vendor lock-in. Many governments have faced such challenges in IT contracting (e.g., New York City's internal wireless network and many other IT projects across U.S. states and the federal government). Through the lens of procurement, large projects carry substantial risks for failure — by some estimates, 52 percent of projects with budgets over $10 million have failed to meet budget, schedule, or user

[11] doteveryone, "*People, Power and Technology: the 2018 Digital Attitudes Report,"* February 22, 2018.
[12] Phoenix Strategic Perspectives Inc., "*2016 Survey of Canadians on Privacy Final Report*," Office of the Privacy Commissioner of Canada, December 2016.
[13] doteveryone, "*People, Power and Technology: the 2018 Digital Attitudes Report,"* February 22, 2018.
[14] Jonnathan Coleman, "Here's How Long It Would Take to Read All the New Privacy Updates," *Medium*, May 23, 2018.
[15] Theo Bass, Emma Sutherland, and Tom Symons, "Reclaiming the Smart City: Personal data, trust and the new commons," *Decode,* July 2018.
[16] Phoenix Strategic Perspectives Inc., "*2016 Survey of Canadians on Privacy Final Report*," Office of the Privacy Commissioner of Canada, December 2016.
[17] Teresa Scassa and Merlynda Vilain, "Governing Smart Data in the Public Interest: Lessons from Ontario's Smart Metering Entity," *Centre for International Governance Innovation,* July 10, 2019.
[18] Teresa Scassa and Merlynda Vilain, "Governing Smart Data in the Public Interest: Lessons from Ontario's Smart Metering Entity," *Centre for International Governance Innovation,* July 10, 2019.

expectations, and another 41 percent were abandoned or restarted all together.[19]

4.2.5 Summary and overview of the following sections

Sidewalk Labs recognizes these challenges and is deeply committed to thoughtfully addressing them. The future of society depends on successfully advancing responsible uses of technology that harness the extraordinary benefits while managing risks.

The following sections provide a snapshot of the diversity of policy responses, approaches, and tools being developed by governments, academia, and public and private sectors, both in Canada and around the world, in order to harness technology's benefits and address these challenges.

4.3 Privacy regulations in Canada and around the world

The protection of personal information is governed in several different ways in Canada. There are privacy laws that apply to public-sector entities, to organizations in the private sector, and to the health sector. There are also privacy torts, which provide data protections in addition to privacy laws[20], and other laws, such as Canada's anti-spam legislation, which place restrictions and requirements on how organizations can use personal information such as email addresses.[21] Canada has a mature set of privacy laws, regulations, and protections, and this context is important when considering Sidewalk Labs' Master Innovation and Development Plan (MIDP) and this Appendix.[22] This section first provides an overview of the private and public sector privacy laws in Canada and then provides an overview of privacy and data protection laws in two other jurisdictions before shifting to an overview of the Canadian digital policy context in the next section.

4.3.1 Privacy and the private sector in Canada

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the collection, use, and disclosure of personal information in the course of commercial activity. PIPEDA applies to all businesses and non-profit entities (to the extent they are engaged in commercial activities), such as Sidewalk Labs.

[19] Laura Gerhardt and Mark Headd, "Why We Love Modular Contracting," *18F*, April 9, 2019.

[20] For example, some recently recognized torts in Ontario include "intrusion upon seclusion" (*Jones v. Tsige*, 2012 ONCA 32) and breach of privacy and appropriation of personality (*Vanderveen v Waterbridge Media Inc*,, 2017 CanLII 77435 (ON SCSM)).

[21] Canadian Radio-television and Telecommunications Commission, "Canada's Anti-Spam Legislation", August 13, 2019.

[22] Chantal Bernier, "Sidewalk Toronto subject to strong existing privacy laws, principles," *The Star*, October 25, 2018.

PIPEDA applies to the handling of “personal information,” which is broadly defined as any information about an identifiable individual (with certain defined exceptions, such a business contact information). Along with information such as names and fingerprints, personal information can also include things such as bank account numbers and IP addresses, depending on the context and whether they can be associated with an identifiable individual.[23]

PIPEDA is a principles-based statute, and its core requirements are articulated around 10 principles.

1. **Accountability.** PIPEDA makes an organization responsible for personal information under its control, which includes personal information held by its service providers. As a result, an organization’s service providers must be bound to comply with Canadian privacy laws in processing personal information. This is usually done by contract.

   PIPEDA also requires organizations to designate a privacy officer who is generally accountable within the organization for PIPEDA compliance matters.

2. **Identifying purposes.** PIPEDA requires an organization to identify the purposes for which it collects personal information at, or before, the time of collection from an individual and prior to use or disclosure of the personal information for the identified purposes.

3. **Consent.** Subject to limited exceptions, PIPEDA requires the knowledge and consent of individuals for the collection, use, or disclosure of their personal information. Consent can take two forms: (i) express consent, which is explicit, unequivocal, and does not require any inference as to whether the individual has consented; and (ii) implied consent, where consent is implied by the circumstances and the individual’s conduct.

   Generally, express consent must be used for collections, uses, or disclosures that: (i) involve sensitive information, (ii) are outside the reasonable expectations of the individual, or (iii) create a meaningful residual risk of significant harm. In other circumstances, implied consent may be appropriate.

   To make consent meaningful, people must understand what they are consenting to. Consent is valid if individuals understand the nature, purpose, and consequences of the collection, use, or disclosure of their personal information.

   Individuals generally have the ability to withdraw consent on reasonable notice, subject to legal or contractual restrictions.

4. **Limiting collection.** PIPEDA requires that when collecting personal information, organizations must only collect personal information that is necessary for identified

[23] Office of the Privacy Commissioner of Canada, “Personal Information” PIPEDA interpretation bulletins, October 2013.

purposes. Organizations should also collect personal information by fair and lawful means. Also, when collecting personal information, organizations must only collect personal information that is necessary for identified purposes.

5. **Limiting use, disclosure, and retention.** PIPEDA requires organizations to only use or disclose personal information for purposes that are identified to individuals at the time they provided consent, except where otherwise permitted by law. PIPEDA requires that organizations retain personal information only for as long as is it is needed for the purposes noted above, unless a longer time period is required by law.

6. **Accuracy.** PIPEDA requires organizations to keep personal information as accurate, complete, and up-to-date as is necessary for the purposes for which it was collected.

7. **Safeguards.** PIPEDA requires organizations to protect personal information using safeguards appropriate to the sensitivity of the personal information. In addition, PIPEDA imposes a privacy breach notification regime, under which organizations must notify affected individuals and report to the Privacy Commissioner of Canada any breach if it is reasonable to believe that the breach creates a "real risk of significant harm to the individual."

8. **Openness.** PIPEDA requires organizations to make readily available to individuals information about their privacy policies and practices.

9. **Individual access.** With some exceptions, PIPEDA gives individuals a right of access to their own personal information, and to know how it has been used and disclosed. Individuals also have the right to correct certain information in an organization's records.

10. **Challenging compliance.** PIPEDA requires organizations to provide individuals with a means of raising concern about the organization's compliance with PIPEDA.

The Privacy Commissioner of Canada oversees compliance with PIPEDA.

4.3.2 Privacy and the public sector in Canada

Public sector organizations are governed by privacy legislation that is specific to their level of government. Federal government institutions are subject to the Privacy Act.[24] In Ontario, provincial government institutions are subject to the Freedom of Information and Protection of Privacy Act (FIPPA)[25] and municipal government institutions are subject to the Municipal Freedom of Information and Protection of Privacy

[24] Privacy Act, R.S.C., 1985, c. P-21.
[25] Freedom of Information and Protection of Privacy Act, R.S.O., 1990, c. F.31.

Act (MFIPPA).[26] These acts are supplemented by government policies and directives to ensure that institutions at the same level of government are consistent in their privacy practices.

Each act applies to the handling of "personal information," which is broadly defined as any information about an identifiable individual — although each act sets out somewhat different exceptions to that term.
Although the federal act, on the one hand, and the provincial and municipal acts, on the other hand, are framed somewhat differently, all three acts embody the same overarching purposes — namely, to protect the privacy of individuals and to provide individuals with a right of access to their personal information. These acts are founded on the notion that privacy protection is essential to ensuring public trust in government institutions.

Unlike PIPEDA, which is founded on the consent of individuals, these acts are founded on the authority of a government institution to engage in certain authorized activities. Although many government institutions share common authorized activities (such as activities inherent to being an organization or to handling personal information for employment or security purposes), the full scope of each institution's authorized activities will vary based on its mandate and authorizing legislation.

[26] Municipal Freedom of Information and Protection of Privacy Act, R.S.O., 1990, c. M.56.

Generally, these acts (as supplemented by policies and directives) address the following principles:

1. **Authority to collect.** Government institutions are to collect personal information only for the purposes of their authorized activities.

2. **Direct collection.** Government institutions must collect personal information directly from individuals, except in limited circumstances.

3. **Notice requirements.** Government institutions must inform individuals about the collection of their personal information, except in limited circumstances.

4. **Authority to use and disclose.** Government institutions must limit their use and disclosure of personal information to authorized activities.

5. **Accuracy.** Government institutions must take steps to keep personal information accurate.

6. **Security.** Government institutions must deploy measures to prevent the loss, theft, or unauthorized use or disclosure of personal information.

7. **Access.** Government institutions must respect individuals' right to access their own personal information, subject to limited exceptions.

8. **Disposal.** Government institutions must securely dispose of personal information, and may be required to deposit it with government archives.

9. **Appeals and powers.** The acts grant the applicable privacy commissioner with various powers to address privacy complaints.

The Privacy Commissioner of Canada oversees compliance with the Privacy Act. The Information and Privacy Commissioner of Ontario oversees compliance with FIPPA and MFIPPA.

4.3.3 Contextual information: global precedents and laws

Modern privacy and data protection laws do not operate in jurisdictional silos. This is because data is an intangible asset that flows between borders; privacy laws in one country can have an impact on governments, businesses, and individuals in another country.[27] Many organizations have offices or stores all over the world, in addition their headquarters and, with some exceptions, digital platforms and apps can be accessed all over the world.

One example of the push for alignment of laws is the European Commission's determination of whether a country outside of the European Union provides an adequate level of data protection. This determination is important, as it allows personal information to flow from individuals in the EU to that third country.[28]

Canada currently has been recognized as providing adequate protection to the EU, but this adequacy status will be reassessed.[29] This section aims to provide an overview of privacy and data protection laws in two jurisdictions that are among the most impactful on Canada and elsewhere.

The United States currently lacks an umbrella data protection law that applies to all companies in all states. Instead, data protection in the United States is regulated by a range of state and federal laws that are often specific to certain industries or types of data.[30]

At the federal level, Section 5 of the Federal Trade Commission ("FTC") Act has been employed heavily in the data privacy and security space, based upon its prohibitions

[27] See, for example, this announcement from the Office of the Privacy Commissioner of Canada, "New European privacy regulation will impact Canadian businesses," February 22, 2018.

[28] European Commission, "Adequacy decisions
How the EU determines if a non-EU country has an adequate level of data protection," accessed on October 11, 2019.

[29] Innovation, Science and Economic Development Canada, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians," May 21, 2019.

[30] Catalin Cimpanu, "51 Tech CEOs Send Open Letter to Congress Asking for a Federal Data Privacy Law," *ZDNet*, September 10, 2019.

against "unfair" and "deceptive" acts. The FTC has used its Section 5 authority liberally to, among other things, hold companies responsible for violating the promises they made in their public-facing privacy policies and failing to implement reasonable security measures. There are also federal laws and regulations applying to personal information collected by financial institutions,[31] health information collected by health providers and other covered entities,[32] the use of email and phone numbers for marketing and transactional messages,[33] and information collected online about children under the age of 13 (i.e. the Children's Online Privacy Protection Act, or COPPA).[34] At the state level, a myriad of additional laws and regulations must be considered, such as those related to data breach notification, biometric data collection, online privacy policies, and state-specific security requirements.[35]

The current U.S. approach to data protection is markedly different than the approach taken in other jurisdictions, including Canada and the European Union (EU). In the EU in particular, the recently enacted General Data Protection Regulation (GDPR) helped to usher in a new wave of attention to data protection issues across the world by enhancing rights for data subjects (any individual person who can be identified, directly or indirectly, through an identifier, such as a name) and imposing significant penalties for noncompliance by authorities, with fines up to the greater of 20 million euros or 4 percent of worldwide revenue.

It is against this backdrop of existing and emerging privacy laws that the California Consumer Privacy Act (CCPA) was enacted. For the first time in the United States, the CCPA will impose an omnibus set of requirements, including the right to increased transparency, the right to access, the right to deletion, and the right to opt out of sales. The CCPA applies to companies doing business in California that collect personal information about California residents and that meet certain threshold criteria, such as having annual revenue above $25 million or annually collecting personal information concerning at least 50,000 California residents. Although portions of the CCPA will go into effect January 1, 2020, the California attorney general's office is not permitted to enforce

[31] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801–6809, together with the act's Privacy Rule and Safeguards Rule.
[32] Health Insurance Portability and Accountability Act of 1996, as amended, together with Privacy Rule and Security Rule (citations too numerous and disparate to succinctly cite).
[33] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. §§ 7701–7713 (for email); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (for phones).
[34] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506, together with implementing regulations.
[35] See, for example, California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579 (online privacy policy law); Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth of 2008, Mass. Gen. Laws ch. 93H; 201 Mass. Code. Regs. 17.00 (state data security requirements); Illinois Biometric Privacy Act: 740 Ill. Comp. Stat. 14/1–99 (2008) (biometric data law); and California Notice of Security Breach Act: Cal. Civ. Code §§ 1798.29, 1798.80–1798.84 (2002) (data breach notification law).

the CCPA until the earlier of July 1, 2020, or six months after the attorney general issues regulations to implement the law.

With California leading the way, a number of other states are considering more broad-ranging privacy laws. Legislative activity has also been heating up at the federal level, with a number of laws being introduced that would either set a minimum bar for data protection or pre-empt any conflicting state laws. In light of the continued attention being given to technology companies and data privacy, it is likely that new laws and regulations will continue to emerge in the years to come.

4.4 The Canadian digital policy landscape

At all orders of government, Canada is exploring the opportunities and impact of an increasingly digital society. The following policies and initiatives are driving conversations and innovation across Canada and inform the context of Quayside. It is a rapidly evolving landscape.

4.4.1 Waterfront Toronto

As the name suggests, Waterfront Toronto is the public advocate for and steward of overseeing the revitalization of 800 hectares (1,977 acres) of Toronto's waterfront. Formerly known as the Toronto Waterfront Revitalization Corporation, it was formed and seed-funded by the governments of Canada, Ontario, and Toronto in 2001 with a mission to deliver social benefits and increased economic competitiveness through innovative approaches to infrastructure and redevelopment.

4.4.1.1 Quayside plan development agreement and digital principles

In March 2017, Waterfront Toronto issued an request for proposal (RFP) for Quayside, seeking a partner to develop nearly five hectares of the Toronto waterfront with four main objectives:

1. Design a sustainable, resilient, and innovative urban development project.
2. Create a complete community.
3. Provide a testbed for building, energy, and economic development.
4. Develop new partnership models.

These objectives became the basis for the five priority outcomes that Waterfront Toronto has defined for the Quayside project:

- Job creation and economic development
- Sustainable and climate-positive development
- Housing affordability
- New mobility
- Urban innovation

Through consultation with government shareholders and the community, Waterfront Toronto has developed Draft Digital Principles to inform the evaluation of project proposals from any private company working in the waterfront, including that of Sidewalk Labs. The draft principles include:

1. Everyone will have access to, and benefit equally from, digital solutions.
2. Digital solutions will be open, ethical and resilient.
3. Everyone will be able to understand how their data is being collected and used, and how organizations can and will be held accountable for their practices.
4. Strong privacy protections will be in place at all times.
5. Data and systems will remain under local control and be subject to local laws.

Waterfront Toronto notes that the core foundation of these Draft Digital Principles is that any project proposed to Waterfront Toronto must represent ethically responsible innovation that reflects public values and preserves or enhances the public good. Waterfront Toronto notes that these principles supplement established federal and provincial laws, with which all proposals must comply.

4.4.1.2 Intelligent Communities Guidelines

As reflected in resolutions on a set of "Threshold Issues" with Sidewalk Labs approved by Waterfront Toronto's Board in October 2019, Waterfront Toronto is working to advance responsible data use by Sidewalk Labs and all other private sector companies working on the waterfront, along with creating opportunities for trusted data sharing. Going forward, Waterfront Toronto is developing "Intelligent Communities Guidelines" that will apply to private companies deploying digitally enabled solutions in the designated waterfront area. Similar to Waterfront Toronto's existing Minimum Green Building Requirements that have raised the bar for sustainability, these Intelligent Communities Guidelines will be enforced through contract with private companies in the Designated Waterfront Area.

4.4.1.3 Digital Strategy Advisory Panel

Waterfront Toronto created the Digital Strategy Advisory Panel (DSAP) in April 2018 to provide objective and expert advice on issues of digital governance, initially with respect to the technological innovations in the Quayside project but also going forward for all waterfront-related projects. Specifically, DSAP is to "ensure that principles of ethical use of technology, accountability, transparency, protection of personal privacy, data governance, and cyber security are upheld,"[36] while also promoting innovation and economic development.

The DSAP mandate includes:

- Ethical use of technology;
- Privacy;
- Cyber security;

[36] Waterfront Toronto, "Digital Strategy Advisory Panel Members," accessed September 19, 2019.

- Data governance;
- Intellectual property;
- Shared benefits and business models;
- Commercial and operating agreements; and
- IT architecture and platforms.[37]

DSAP's 15-member panel includes academic, government, and industry experts in law, technology, and policy.

4.4.2 The City of Toronto

Toronto is one among several Canadian cities pursuing a municipal smart city strategy.[38] In addition to Toronto's long-established Open Data Initiative, the City is currently advancing the creation and adoption of new digital governance principles and policies, supported by City Council's Issue Notes for smart cities and information and technology.[39, 40]

[37] Waterfront Toronto, "Waterfront Toronto Digital Strategy Advisory Panel Mandate & Operating Protocols By-Laws - Version 0.7," March 16, 2018.
[38] Tracey P. Lauriault, Rachel Bloom, and Jean-Noé Landry, "Open Smart Cities in Canada: Assessment Report," *SocArXiv*, April 11, 2018.
[39] Waterfront Toronto, "Smart Cities Initiatives," accessed September 19, 2019.
[40] Waterfront Toronto, "Smart Cities Initiatives," accessed September 19, 2019.

4.4.2.1 City-wide Digital Infrastructure Policy Framework and Governance Model

The City is currently developing an expansive range of policies and approaches to digital and data governance that will be used to inform the City's evaluation of the Quayside proposal and other projects. In February 2019, the City Council adopted a motion on Data Governance and Smart Cities to develop a "City-wide policy framework and governance model associated with digital infrastructure, such as smart cities, and a work plan for implementation."[41] Recognizing that the City already utilizes smart city technology and collects data from residents in a variety of ways — from the Toronto Transit Commission PRESTO Card, to traffic cameras, to online registration for recreation programs[42] — the framework and model will formalize some existing practices, as well as institute new approaches, roles, and tools. The development of the Digital Infrastructure Policy Framework and Governance Model will be led by the City Clerk and Chief Information Officer and guided by the principles of privacy, transparency, accountability, public ownership and public interest protection, equity, and human rights. A report by the Deputy City Manager of Infrastructure and Development Services in June 2019 provided more

[41] City of Toronto, "City Council Decision - Data Governance and Smart Cities," accessed September 19, 2019.
[42] City of Toronto, "City Council Notice of Motion - Data Governance and Smart Cities," accessed September 19, 2019.

details of the contents of the policy framework and governance mode. Specifically, it defined:

- A future vision and principles for the use of digital tools and data collection to advance City goals for the human, built, economic, and natural environments;
- A description and definition of the City's digital infrastructure;
- A review of Provincial and Federal legislative regulatory and policy contexts;
- A governance model, including the roles of key groups and individuals;
- A set of existing and emerging regulations and policies to guide decision-making on internal and external proposals, such as those developed by Waterfront Toronto and Sidewalk Labs; and
- A work plan with priority areas for proactive future action.[43]

Public consultation is scheduled for the third quarter of 2019 and the report is expected to be presented to the City's Executive Committee by the end of the year. The Quayside proposal will be evaluated by the City of Toronto based on a number of criteria, including its "alignment with existing and emerging digital infrastructure and data governance policies."[44]

[43] City of Toronto, "EX6.1 Report for Action, Quayside – Update," accessed September 19, 2019.
[44] City of Toronto, "Data Governance and Smart Cities," *City Council Notice of Motion*, accessed September 19, 2019.

4.4.2.2 Digital rights principles

The Cities for Digital Rights is an international coalition to "protect and uphold human rights on the internet at the local and global level."[45] It is led by the cities of Amsterdam, Barcelona, and New York and has the support of the United Nations Human Settlements Programme (UN Habitat). The Declaration of Cities for Digital Rights promotes five principles:

1. Universal and equal access to the internet and digital literacy;
2. Privacy, data protection, and security;
3. Transparency, accountability, and non-discrimination of data, content, and algorithms;
4. Participatory democracy, diversity, and inclusion; and
5. Open and ethical digital service standards.

Since forming in November 2018, nearly 30 other cities have supported the declaration. In June 2019, the Toronto City Council adopted a motion to authorize the City Manager to sign on to the Declaration of Cities for Digital Rights. Additionally, it directed City staff and resources towards programs and initiatives that carry out the declaration's principles. These include digital literacy and safety programs with the Toronto public library; new internal policies and practices for ethical digital standards; enhanced digital tools

[45] Cities for Digital Rights, "Declaration of Cities Coalition for Digital Rights," accessed September 19, 2019.

for digital public engagement and outreach; and partnerships with community, technology, and business stakeholders on urban public policy issues.[46] An update on this effort is expected in City Council in November 2019.

4.4.2.3 Open-data initiatives

Toronto's Open Data Initiative started in 2009 and has continued to grow its offerings and impact. Beginning with the release of a catalogue and online portal of municipal data sets, the official Open Data Policy was adopted in 2011. The Open Data Policy outlines both the rules of the public release and digital publication of data sets as free and machine-readable resources for public use and benefit and designates a broad range of City executives and resources responsible for compliance. Open data is shared through an open government license.

The 2018 Open Data Master Plan expands and formalizes the Open Data Policy. The five-year plan provides a strategic framework and roadmap that positions open data as a valuable resource that can improve the delivery of public services, engage residents in government decision-making, and transform approaches to public problem-solving. To provide such value, the Open Data Master Plan adopted six guiding principles championed by the International Open Data Charter:

1. Open by default;
2. Timely and comprehensive;
3. Accessible and usable;
4. Comparable and interoperable;
5. Improved government and citizen engagement; and
6. Inclusive development and innovation.

Today the portal includes 309 data sets covering a range of topics, including but not limited to public services, facilities, and assets in health, public safety, environment, business and more. The Open Data Portal does not include all available municipal open data. For example, the Toronto Police Service maintains and publishes open data on crime, traffic, administrative and geographical boundaries, and budgets on a separate portal. A limited number of data sets, such as shapefiles for police boundaries and police facility locations, are offered on both the City of Toronto's portal and the Toronto Police Service's portal.

4.4.2.4 Data sharing across sectors

In 2016, the City of Toronto mandated that private transportation companies, including companies such as Uber and Lyft, share data regarding vehicles for hire. Through Chapter 546 of the Toronto Municipal Code and the Vehicle-for-hire Data Sharing Agreement, private transportation companies must collect and share data with the City on a daily basis. This data includes, but is not limited to:

---

[46] City of Toronto, "City Council Decision - Cities for Digital Rights - June 18, 2019," accessed September 19, 2019.

- Driver data, including personal information such as driver's licenses, criminal reference checks, and driving and insurance records.
- Vehicle data, including license numbers, make and model, and safety inspection certificates.
- Trips data, including date, pick-up and drop-off locations and times, number of passengers, time between service request and start of trip, and fares.

As stated in the Data Sharing Agreement, the City uses this data for business purposes, like processing driver licensing applications, monitoring compliance, and carrying out enforcement. Data is stored for three years before it is destroyed. Unlike other cities such as Chicago and New York, none of this data is published on Toronto's Open Data Portal.

In 2017, the City estimated that the data sharing effort improved business processes and gained efficiencies, including saving 22,500 staff hours and reducing license fees for the industry.[47]

4.4.3 Province of Ontario

The Province of Ontario is advancing two initiatives that bolster data and digital practices in the provincial government — the Ontario Data Strategy and the Simpler, Faster, Better Services Act. The Ontario Data Strategy is expected to be finalized by the end of 2019.

4.4.3.1 Ontario Data Strategy

The Ministry of Government and Consumer Services is actively developing the Ontario Data Strategy with the dual purpose of "explor[ing] new opportunities for data use" and "protecting people's data rights from growing risk."[48] Announced in early 2019, the government seeks a strategy that achieves three goals:

1. **Trust and confidence** through best-practice privacy protections.
2. **Economic benefit**, including support for data-driven business.
3. **Better, smarter government** through developing public-sector skills and capacity in data and technology.[49]

The proposed strategy is intended to guide practices within government as well as in the private sector. It is considering data held by government (such as locations and traffic patterns) as well as personal data held by businesses (such as

[47] Brian Jackson, "City of Toronto enters era of the 'sharing economy' with award-winning digital solutions," *itbusiness.ca*, June 14, 2017.

[48] Ontario Ministry of Government and Consumer Services, "Ontario's Data Strategy," accessed September 19, 2019.

[49] Ontario Ministry of Government and Consumer Services, "Promoting Trust and Confidence in Ontario's Data Economy: Discussion Paper," 2019.

purchases and preferences). Specifically, regarding cities and technology companies, the Ministry proposed the following smart cities principles:

- Guarantee that Ontarians' privacy and personal data are protected, managed responsibly, and kept secure;
- Put people first by ensuring that Ontarians are the primary beneficiaries and valued partners in the opportunities created by the project;
- Create responsible and good governance systems that are democratic, accountable, and transparent;
- Enact leading, best technical practices that ensure chosen technologies use open software and open standards, and are secure, interoperable, locally procured, flexible, durable, and scalable; and
- Educate the public on the risks associated with the project and provide meaningful opportunities for local residents to participate and engage in the creation of the smart city.[50]

These smart cities principles align closely with the general principles that guide the overall creation of the strategy. These principles include:

- Data privacy and protection is paramount;
- Data policies must be beneficial, transparent, and easy to understand to the people of Ontario;
- Data is necessary for effective and responsible government decision-making;
- Data should be collected responsibly and kept safe and secure; and
- Data is a key economic and social driver.[51]

The strategy is being developed through multiple rounds of public consultations as well as through a newly formed Minister's Digital and Data Task Force. Announced in June 2019, the eight-member Task Force includes experts with backgrounds in law, policy, technology, and academia and serves in an advisory capacity on the strategy.

Through the initial round of consultations, which included nearly 800 respondents, four areas of consideration were identified and will inform the continued engagement. The focus areas include: privacy, data protection, and data governance; consumer protections; human and civil liberties; and public education and awareness.[52] The next round of consultations are scheduled for August and September.

4.4.3.2 Simpler, Faster, Better Services Act

The Simpler, Faster, Better Services Act introduces improved government digital and data practices in public service

[50] Ontario Ministry of Government and Consumer Services, "News Release: Ontario Takes Action to Protect Privacy and Personal Data," May 30, 2019.

[51] Ontario Ministry of Government and Consumer Services, "Ontario's Data Strategy," accessed September 19, 2019.

[52] Ontario Ministry of Government and Consumer Services, "Promoting Trust and Confidence in Ontario's Data Economy: Discussion Paper," 2019.

delivery to benefit resident experience and personal privacy. As part of the 2019 Budget Bill, the Act cuts across ministries and legislation, updating an estimated 20 acts or regulations for more streamlined and modern government processes[53]. The Act builds on the Ontario Digital Service's 2018 Digital Action Plan and 2017 Digital Services Standards, formalizing a number of existing digital principles and integrating related data management principles.

The Act aims to transform government service delivery to put people first through:

- Better access to digital services;
- Improved, co-designed digital services;
- Increased availability of useful government data; and
- Expanded integration of data and digital resources into the broader ecosystem of service providers, including municipalities, local boards, universities, and health systems.[54]

To achieve these goals, the Act recognizes the interdependency between useful data and high-quality public services. It calls for effective data management, data sharing, and interoperable technologies within government and public services providers and authorizes the Minister of Government and Consumer Services to appoint a Chief Digital and Data Officer (CDDO). The CDDO would guide the proposed transformation and create a Digital and Data Action Plan.

The CDDO would be expected to establish standards and promote digital and data management principles to enable increased and improved public digital service delivery. These include:

- **Digital service standards**, including requirements for data collection, management, and use in the creation and delivery of digital services.
- **Open-data standards**, including requirements to make data publicly available; data formats and technical standards for reporting frequency and manner; and data-use licences.
- **Digital principles** promoting inclusive, user-centred design and implementation; continuous improvement; effective data use; security and privacy; and interoperable and scalable technology.
- **Data management principles** supporting machine readable and easily accessible data formats; no-cost or cost-reasonable data provision; public data reuse, including commercial and non-commercial use; and current, accurate, and complete data.

[53] Ontario Ministry of Government and Consumer Services, "News Release: Ontario's Government Delivers Simpler, Faster, Better Services for Ontarians with New Digital Plan," April 30, 2019.
[54] The Government of Ontario, Canada, "Simpler, Faster, Better Services Act," 2019.

4.4.4 Government of Canada

The national policy landscape is rapidly evolving across a number of ministries. The recently announced Digital Charter is just the latest in a series of active consultation and policy development conversations examining the role of data and technology in governance that is being held by stakeholders from multiple sectors, and seeking to balance risk and privacy concerns with a mandate to spur innovation and economic development.

4.4.4.1 The Digital Charter and National Digital and Data Consultations

Both the Digital Charter and National Digital and Data Consultations demonstrate Canada's efforts to support innovation and economic competitiveness and to actively address related challenges in economic and digital transformation.[55]

Canada's Digital Charter outlines guiding principles for the government's efforts to build a foundation of trust while growing the economy through innovation and digital transformation. Announced in May 2019 by the Minister of Innovation, Science, and Economic Development, the Charter is positioned to inform future decision-making on government initiatives, including investments. The Charter's ten principles are:

1. **Universal access,** including connectivity, tools, literacy, and skills to fully participate in the digital economy.
2. **Safety and security** in the digital platforms and services used online.
3. **Control and consent** in the sharing and use of personal data.
4. **Transparency, portability, and interoperability**, meaning clear access to personal data and the ability to share or transfer with ease.
5. **Open and modern digital government** that delivers public services and provides a responsive and agile regulatory framework.
6. **A level playing field** in the online marketplace for Canadian businesses to thrive and provide consumer protections.
7. **Data and digital for good**, including ethical data use for public benefit.
8. **Strong democracy** through supporting freedom of expression and protection against disinformation and other threats.
9. **Freedom from hate and violent extremism.**

[55] While not specifically related to digital rights, the Canadian Charter of Rights and Freedoms, part of Canada's Constitution Act, 1982, also provides for the protection of fundamental privacy rights in several sections (the Charter applies to governments, and not to private individuals, businesses or other organizations).

10. **Strong enforcement and real accountability**, including "clear and meaningful" fines for breaking laws and regulations.[56]

Some media outlets have noted that these principles are proposed to apply to all federal legislation, yet such application would require changes in the Personal Information Protection and Electronic Documents Act (PIPEDA), the federal Privacy Act, The Competition Act, and Canadian anti-spam legislation.[57] Such changes are currently under review. For example, the Department of Justice is leading the examination of the Privacy Act, while the Innovation, Science and Economic Development Canada (ISED) is leading a review of the PIPEDA, with both efforts looking to modernize the existing frameworks.[58]

The Digital Charter was created after and informed by the National Digital and Data Consultations. From June through October 2018, six digital innovation leaders representing multiple sectors in technology, business, and law, led 30 roundtables throughout the country, reaching 580 participants and gathering nearly 2,000 ideas online.[59] The Consultations were an extension of the larger Innovation and Skills Plan Strategy, which started in 2016 and includes over 30 initiatives and programs, such as the Innovations Super Cluster Initiative, Digital Literacy Exchange, and Intellectual Property Strategy, to name a few.

The Consultations were organized around three themes: skills and talent; unleashing innovation; and privacy and trust.[60] Public input highlighted key concerns and priorities within each theme.

For **skills and talent** in the changing economy and job landscape, the participant priorities included, but were not limited to:

- Opportunities to gain a more holistic skill set, including digital literacy, upskilling, and reskilling.
- Access to talent, including recruiting and retaining top-level international students and global talent.

[56] Innovation, Science, and Economic Development Canada, "Canada's Digital Charter: Trust in a digital world," *Government of Canada*, 2019.
[57] Howard Solomon, "Canada announces Digital Charter, promises serious fines to business for not protecting privacy," *IT World Canada*, May 21, 2019..
[58] Innovation, Science, and Economic Development Canada, "Strengthening Privacy for the Digital Age, " *Government of Canada*, accessed September 19, 2019.

[59] Innovation, Science, and Economic Development Canada, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians," *Government of Canada*, accessed September 19, 2019.
[60] Innovation, Science, and Economic Development Canada, "Positioning Canada to Lead in a Digital- and Data-driven Economy," *Government of Canada*, accessed September 19, 2019.

- Diversity, inclusivity, and accessibility in designing technology and digital services, as well as frameworks for the labor market.[61]

With regard to **unleashing innovation** and remaining competitive in adopting digital technology, respondents expressed interest in:

- Expanding connectivity, supporting digital infrastructure, Canadian research and development, and deepening affordability.
- Building capacity for technological adoption within businesses of all sizes and embracing a culture of resilience and risk.
- Developing multi-sectoral partnerships to increase competitiveness, provide skills and offer new types of accreditation.[62]

Respondents offered the following concerns about **privacy and trust**:

- Greater trust and control in data access, ownership, use, consent, and control to both residents and digital service providers.
- Clear, modern, and responsive regulatory and marketplace frameworks.
- Increased responsible data use and sharing for public benefit, through representative and unbiased data and secure data management, like data trusts.
- Additional support in providing greater security on digital platforms and tools.[63]

Many of these responses are reflected in the Digital Charter's ten principles.

4.4.4.2 Open data initiatives

A range of open government and data initiatives have developed in Canada over the past decade. These include open-data approaches, such as the Open Data Portal, Open Government Partnership, G8 Directive on Open Data, and International Open Data Charter, as well as the Directive on Open Government.

Canada launched the federal Open Government Portal in March 2011. The government cites a range of benefits from providing open data, including accountability and transparency; support for research, consumers, and

[61] Innovation, Science, and Economic Development Canada, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians," *Government of Canada*, accessed September 19, 2019.

[62] Innovation, Science, and Economic Development Canada, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians," *Government of Canada*, accessed September 19, 2019.

[63] Innovation, Science, and Economic Development Canada, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians," *Government of Canada*, accessed September 19, 2019.

commercial industry; and common, reusable resources.[64] The portal uses the Sunlight Foundation's Ten Principles for Opening Up Government as guiding principles. These include:

1. **Completeness**, with data published in entirety and without aggregation.
2. **Primacy**, with data published by the primary source and with details on how and for what purpose data was collected.
3. **Timeliness**, where data collected is released quickly to the public.
4. **Ease of physical and electronic access**, including reducing barriers to access and employing interfaces accessible to residents with a wide range of skills.
5. **Machine readability** and documentation to ease processing.
6. **Non-discrimination**, including the absence of memberships or registration.
7. **Use of commonly owned standards**, including storage formats.
8. **Licensing**, in which open data is covered under Canada's Open Government License
9. **Permanence**, where information can be tracked over time.
10. **Usage costs** that are free of charge.

Currently, the national portal consists of nearly 82,000 data sets, of which approximately 85 percent are geospatial datasets or maps. A full list is available on the portal and facilitated through a mandated data inventory.

Complementary to Canada's open data portal, Canada is part of global consortiums supporting open data, including the Open Government Partnership, the G8 Charter on Open Data, and the International Open Data Charter.

Canada joined the Open Government Partnership (OGP) in 2012. A nearly 100-member organization, the OGP advocates for more transparent, accountable, responsive, and effective government through supporting cross-sector partnerships between government and civil society and the creation of national action plans.[65] The current Canadian 2018-2020 National Action Plan was led by a multi-stakeholder forum made up of 12 representatives from civil society and federal government which guide the development and implementation of the plan. Based on in-person and online public engagement reaching over 10,000 people and gathering over 5,000 ideas, the Plan details ten commitments related to open government and open data. The ten commitments in the current plan are:

1. **User-friendly open government**, including increasing quantity and quality of tools for collaboration between government and residents, expanding open-by-default adherence, and developing open data privacy guidelines.

[64] "Open Data 101," *Government of Canada*, accessed September 19, 2019.

[65] Open Government Partnership, "Our Process," accessed September 19, 2019.

2. **Financial transparency and accountability**, including common contracting data standards across Canada.
3. **Corporate transparency** to safeguard against misuse by and facilitate data sharing with corporations.
4. **Digital government and services**, prioritizing the development of a digital policy and data strategy roadmap, using open-source code in digital products, and improving transparency and awareness of the government's use of artificial intelligence.
5. **Open science**, including a portal offering open access to federal scientist publications, and implementation of a digital identification system.
6. **Healthy democracy**, supporting international norms on diversity and transparency of information online.
7. **Access to information**, including improved transparency about government held personal information.
8. **Feminist and inclusive dialogue**, which requires new assessment tools, inclusive participation and design methods, and better access to data.
9. **Reconciliation and open government** between Indigenous Peoples and the Government of Canada, with increased capacity for data use.
10. **Canada's open government community** acting as a global leader.[66]

[66] "Canada's 2018-2020 National Action Plan on Open Government," *Government of Canada*, 2018.

Canada also signalled its leadership in open government with signing the G8 Charter on Open Data in June 2013. The G8 Charter recognizes the economic and social value of open data, outlines five strategic principles guiding access to open data, and gathers commitments to create member-country open-data action plans. The five principles are:

- Open data by default;
- Quality and quantity;
- Usable by all;
- Releasing data for improved governance; and
- Releasing data for innovation.

These principles are largely in line with the Canada's Open Data principles and the priorities detailed in the National Plan for Open Government. Analysis from the Sunlight Foundation in 2014 suggests that Canada succeeded in fulfilling these principles.

In March 2018, Canada adopted the International Open Data Charter, which outlines six principles for publishing data. Widely accepted — the City of Toronto adopted these principles as part of the Open Data Master Plan, for example — and similar to the G8 charter, the six principles are:

- Open by default;
- Timely and comprehensive;
- Accessible and usable;
- Comparable and interoperable;
- For improved governance and citizen engagement; and
- For inclusive development and innovation.

Many of these efforts were formalized in the 2014 Directive on Open Government, which aims to "maximize the release of government information and data of business value to support transparency, accountability, citizen engagement, and socio-economic benefits through reuse, subject to applicable restrictions associated with privacy, confidentiality, and security."[67] The Directive applies to all federal governmental departments under the Financial Administration Act, with few exceptions. The Department of Information Management leads and is responsible for the cross-departmental effort.

4.4.4.3 Data Strategy Roadmap for the Federal Public Service

The 2018 Data Strategy Roadmap for the Federal Public Service creates a framework for the Federal Public Service and makes specific recommendations to enable the Government of Canada to deliver value to residents from the data the government holds. Developed jointly by the Office of the Chief Statistician, Statistics Canada; the Office of the Chief Information Officer, Treasury Board Secretariat; and the Deputy Secretary to the Cabinet, Privy Council Office, the Roadmap is — in their own words — "ambitious." Specifically, the Roadmap demands that "how the Government of Canada collects, manages and governs data—and how it accesses and shares data with other governments, sectors, and Canadians—must change."[68]

Emphasizing the potential value of data, the Data Strategy Roadmap identifies 21 specific changes the government can make in four key areas: data governance; people and culture; environment and infrastructure; and data resources.

To build a foundation of governance, the Roadmap recommends:

- **Greater oversight to leverage better data**, including establishing senior level decision-making body for horizontal data issues, creating a Canadian Chief Data Steward and enterprise data leadership; and developing new frameworks for ethical and secure data use.
- **Building data analytics capacity and culture**, requiring departmental data strategies and portfolios with clear roles and responsibilities, and creating a central working group focused on data-driven decision-making.
- **Accelerating collaboration** through inter- and intra-governmental collaborations, including data sharing initiatives.

[67] "Directive on Open Government," Government of Canada, accessed September 19, 2019.

[68] "A Data Strategy Roadmap," Government of Canada, 2018.

- **Supporting Indigenous Peoples data strategies**, including reducing reporting requirements and co-developing data sharing strategies.[69]

To ensure government has the people and culture with the capacity for data, the Roadmap highlights:

- **Supporting ongoing learning and development** within government staff by evaluating current skills and data literacy; aligning HR with targeted training; and developing a digital academy.
- **Encouraging job seekers to choose government positions**, through competitive hiring practices.[70]

To provide the environmental and digital infrastructure that enables data-driven action, the Roadmap proposes:

- **Strengthening and modernizing infrastructure** by establishing a common set of data needs and process for adopting data tools, and acquiring digital and data needs.
- **Aligning legislative and policy frameworks**, including review of the Privacy Act, PIPEDA, and the Statistics Act; supporting a "tell us once" approach; and streamlining data sharing agreements.

[69] Anil Arora, Alex Benay, and Matthew Mendelsohn, "Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service," *Government of Canada*, 2018.
[70] Anil Arora, Alex Benay, and Matthew Mendelsohn, "Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service," *Government of Canada*, 2018.

- **Working with partners**, including inter-jurisdictional data sharing and leveraging current work to build the digital identity ecosystem.[71]

To develop data assets and resources within government, the Roadmap advances:

- **Better understanding of currently held information** through creating a centralized view of government held data, a data quality framework, and long-term management strategy of digital government assets.
- **Strengthening analysis and experimentation in government**, including enhanced analysis techniques and increased data generation to enable performance measurement, program evaluation, and policy development.
- **Fostering innovation and risk-taking** in public service by leveraging outcomes of existing pilot projects, such as scaling artificial intelligence to reduce the burden of administratively intensive tasks and technology solutions to enable data sharing.
- **Making government more open and more transparent** by expanding public access to government held data; promoting open government; and growing adherence to open-by-default principles.

[71] Anil Arora, Alex Benay, and Matthew Mendelsohn, "Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service," *Government of Canada*, 2018.

- **Supporting innovation in the economy** through increasing access to public- and private- sector data, including pursuing the creation of a Canadian open-data trust or pool.[72]

The Data Strategy Roadmap was established in September 2019 as a short-term milestone to initiate the recommended efforts, with the expectation to continue to expand and scale actions over time.

4.4.4.4 Strategic Plan for Information Management and Information Technology 2017-2021

Issued by the Chief Information Officer, with oversight, guidance, and input from the Committees on Enterprise Priorities and Planning and the Treasury Board Secretariat, the Strategic Plan for Information Management and Information Technology outlines the priorities for the Government of Canada's investment in information management and technology. The Plan includes over 70 strategic actions to support the goal of "secure, reliable, accessible and agile digital business solutions" that drive public service delivery.[73] Broadly, the strategic actions include:

- **Service** through providing technologies that result in improved services for residents incorporating service management; cloud-first approaches; technology modernization such as blockchain and artificial intelligence; data sharing; and any required policy or legislative changes.
- **Manage** the transition to a digital culture through governance; aligning enterprise architecture practices, such as standardizing metadata and creating a data valuation framework; prioritizing agility and innovation; and assessing the sustainability of investments.
- **Security** in safeguarding sensitive government data and collecting personal information in service delivery through in-depth defence of the network, end-point devices, patch management, and administrative privileges; trusted solutions and services, including cyber-authentication and a secure communication service for classified information; and awareness and understanding.
- **Community** of high performance and support, advancing the workforce and workplace and digital collaboration.

[72] Anil Arora, Alex Benay, and Matthew Mendelsohn, "Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service," *Government of Canada*, 2018.

[73] Treasury Board of Canada Secretariat, "Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021," *Government of* Canada, accessed September 19, 2019.

Many of the actions identified in the Strategic Plan are included or superseded by other strategies or plans. For example, digital- and data- specific items are the Government of Canada's Digital Charter or the Data Strategy Roadmap. Similarly, cloud-first initiatives are included in the Cloud Adoption Strategy, which guides department decisions for cloud deployment and service models and outlines how to manage security risks and approach data residency.

4.4.4.5 Responsible Use of Artificial Intelligence in Government Initiative

The Responsible Use of Artificial Intelligence in Government is a multi-year initiative led by the Treasury Board Secretariat that creates an ethical framework to evaluate the use of artificial intelligence (AI) in the provision of government services. It includes the Directive on Automated Decision Making and the associated Algorithmic Impact Assessments.

The April 2019 Directive on Automated Decision Making aims to "ensure that Automated Decision Systems are deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent, and interpretable decisions made pursuant to Canadian law."[74] It applies to any part of the government looking to use a system, tool, or statistical model to assist or make administrative decisions in public service delivery.

The Directive requires several processes to evaluate or use any decision-making system, including:

- **Algorithmic Impact Assessments** (AIA), containing 60 questions about business goals, data, technology, decision context, and oversight.
- **Transparency**, including providing notice and explanations of decisions; government access to software components; and release of source code.
- **Quality assurance,** including testing and monitoring outcomes and validating data quality; expert peer review; employee training; security assessments; legal consultations; and human intervention.
- **Recourse** for clients.
- **Reporting** on results in meeting program goals.[75]

Reflecting the evolving nature of AI and the continuous need to support responsible and fair decisions, both the Directive and the AIA are designed to be updated.

[74] Government of Canada. 2019 "Directive on Automated Decision-Making."

[75] Government of Canada. 2019 "Directive on Automated Decision-Making."

4.4.4.6 The Digital 9

The Digital 9 (D9) is a collaborative network of several governments with a common goal of harnessing technology to improve citizens' lives. Countries share practices, collaborate to solve common problems, identify improvements to digital services, and support and champion growing digital economies.

In 2018, member countries signed a charter that outlines a mutual commitment to digital development and leadership through 9 core principles:

- user needs
- open standards
- open source
- open markets
- open government
- connectivity
- teach children to code
- assisted digital
- commitment to share and learn[76]

Member countries include Estonia, Israel, Mexico, New Zealand, Portugal. Republic of Korea, United Kingdom and Uruguay.

[76] Government of Canada. 2019. "D9 Charter."

4.4.4.7 Overview of policy approaches

The state of digital governance is actively in development, with several related and new digital strategies created across different orders of government within Canada.

As illustrated in the Table below, policy approaches are taking a variety of forms, are at different stages of implementation, address multiple overlapping topic areas and build on a foundation of privacy legislation.

These offer a picture of an evolving landscape that aims to address public needs and protection, and to position Canada to benefit from digital infrastructure and technologies.

Table: Summary Table Illustrating Existing Privacy Legislation, Digital Policies and Strategies Being Advanced by the City of Toronto, the Province of Ontario and the Government of Canada, and the Smart Cities and Relevant Digital Governance Topics they Address

		Topic Areas				
	Policy Approach	**Privacy and Data protection**	**Digital Rights and Ethics**	**Data Governance and Sharing**	**Participation and Inclusion**	**Open and Agile Technical Architecture**
City of Toronto						
Open Data Master Plan	Strategy			X		
Open Data Policy	Policy			X		
Data Sharing Agreements	Policy			X		
Digital Infrastructure Policy Framework and Governance Model	Goal setting	X		X		
Declaration of Cities for Digital Rights	Policy	X	X		X	
Province of Ontario						
Freedom of Information and Protection of Privacy Act (FIPPA)	Legislation	X		X		
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)	Legislation	X		X		
Open Data Directive	Policy			X		
Ontario Data Strategy	Goal setting	X	X	X	X	X
Digital and Data Task Force	Consultation	X	X	X	X	
Simpler, Faster, Better Services Act	Policy	X		X		X

	Policy Approach	Privacy and Data protection	Digital Rights and Ethics	Data Governance and Sharing	Participation and Inclusion	Open and Agile Technical Architecture
Government of Canada						
	Canada's Constitution	X	X	X	X	
The Personal Information Protection and Electronic Documents Act (PIPEDA)	Legislation	X		X		
Privacy Act	Legislation	X		X		
Digital Charter and Proposals to Modernize PIPEDA	Goal setting and Policy	X	X	X	X	X
National Digital and Data Consultations	Consultation	X		X	X	
Open Data Program	Program			X		
Open Government Partnership National Action Plan	Strategy			X		
Directive on Open Government	Policy			X	X	
Data Strategy Roadmap	Strategy	X		X		
Strategic Plan for Information Management and Information Technology	Strategy			X		X
Responsible Use of Artificial Intelligence in Government	Strategy		X	X		
The Digital 9	Charter				X	X

4.5 Opportunities in existing and emerging practices

Cities looking to strengthen trust and build more robust communities are addressing societal challenges through a combination of strategies and regulation. More and more opportunities are arising to make protection and technology innovation mutually compatible through the combination of digital governance and new technologies. Against a rapidly evolving policy and technological background, Sidewalk Labs is informed by an abundance of existing and emerging approaches to enhance privacy, digital rights, participation, and openness, and to advance data and digital innovation. In developing this proposal, Sidewalk Labs envisions digital governance that is responsive to local conditions and informed by best practices around the world.

The success of cities, today and in the future, requires cooperation and coordination across sectors and disciplines to advance an ecosystem of digital governance. There is broad consensus that the decisions, responsibilities, and ongoing management that enable or limit a digital society must evolve. Societal challenges intersect issue areas and cannot be solved by a single sector alone.[77] Multi-sector governance is needed to effectively address the full scope of challenges and achieve scale in implementing solutions. Additionally, there is a mismatch between the pace of technological change and traditional regulation.[78,79] Yet, public well-being requires "continual readiness to rapidly navigate change."[80]

4.5.1 Privacy principles

Within Canada and elsewhere, there are ongoing discussions around existing privacy laws and legal frameworks that aim to address concerns about privacy risks. A discussion of Canada's privacy-related laws and the evolving policy landscape is included in sections 4.3 and 4.4. Complementary to the legal context, discussions are once again highlighting foundational privacy principles, such as the Office for Economic Cooperation & Development (OECD) Privacy Principles and Privacy by Design, alongside emerging policy and technical practices. The ongoing discussion brings together a range of stakeholders all working towards creating an environment that ensures privacy protection.

---

77 "Agile Governance: Reimagining Policy-making in the Fourth Industrial Revolution," *World Economic Forum*, January 2018.

78 "Data Trusts: A new tool for data governance," *Element AI* and *Nesta*, 2019.

79 Silja Baller, Soumitra Dutta, and Bruno Lanvin, "The Global Information Technology Report 2016: Innovating in the Digital Economy," World Economic Forum, 2016.

80 "Agile Governance Reimagining Policy-making in the Fourth Industrial Revolution," *World Economic Forum*, January 2018.

4.5.1.1 Foundational privacy principles

Widely accepted throughout governments and industry globally, the OECD Privacy Principles and Privacy by Design framework provide foundational guidance for current privacy discussions. A brief summary of each is provided as a reference point below.

OECD Privacy Principles

Created in 1980 as part of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Privacy Principles provide a framework about protecting personal data collection. The eight principles are:

1. **Collection limitation**, restricting the collection of personal data and requiring that any data collection is obtained by lawful and fair means with the knowledge or consent of the data subjects.
2. **Data quality,** including relevancy, accuracy, completeness, and timeliness.
3. **Purpose specification,** requiring that the purpose of personal data collection be specified no later than the time of collection and that subsequent use is limited to the fulfilment of those purposes or is not incompatible with those purposes.
4. **Use limitation**, restricting personal data uses.
5. **Security safeguards** that provide protection against risks such as loss, unauthorized access, destruction, use, modification, or disclosure of data.
6. **Openness**, regarding personal data practices and policies including readily providing information about the existence, nature, and use of personal data and the identity of the data controller.
7. **Individual participation** providing individuals with the right to obtain and challenge information and data pertaining to themselves.
8. **Accountability** of the data controller in complying with the principles.[81]

The OECD Privacy Principles inform a range of international and national privacy laws, as well as industry practices. For example, the Generally Accepted Privacy Principles created by Canadian and American professional accountant groups, translates the principles into a tool for privacy compliance, management, and audit.[82,83]

Privacy by Design

Developed in the 1990s by Dr. Ann Cavoukian, former Ontario Information and Privacy Commissioner and former Executive Director of the Privacy and Big Data Institute at Ryerson

---

81 "OECD Privacy Principles," Organisation for Economic Co-operation and Development, accessed September 19, 2019.

82 "Generally accepted privacy principles (GAPP) in privacy policy development," Chartered Professional Accountants Canada, accessed September 19, 2019.

83 "OECD Privacy Principles," Organisation for Economic Co-operation and Development, accessed September 19, 2019.

University, the Privacy by Design framework provides seven principles designed to be integrated into business practices and technology infrastructure and software systems. The framework aims to ensure privacy protection and provide individuals control over information about oneself and recognizes that "privacy cannot be assured solely by compliance within regulatory frameworks."[84]

The Principles of Privacy by Design include:

1. **Proactive not reactive; preventative not remedial.** Anticipate and prevent privacy invasive events before they happen. Action comes before the fact, not afterwards.
2. **Privacy as the default setting**. Ensure automatic protection of personal data in IT systems and business practices, where no action is required on the part of the individual to protect their privacy.
3. **Privacy embedded into design.** Privacy is an essential component of the core functionality being delivered, not an add-on.
4. **Full functionality — positive-sum, not zero-sum.** No trade-offs are necessary to achieve both privacy and security.
5. **End-to-end security — full lifecycle protection**. Secure the retention and destruction of data throughout the information management lifecycle.
6. **Visibility and transparency — keep it open**. Assure stakeholders that business practices and technologies are operating according to the stated objectives and remain subject to independent verification.
7. **Respect for user privacy — keep it user-centric.** Individual privacy requires strong privacy defaults, appropriate notice, and user-friendly options.[85]

Privacy by Design is now offered as a certification for businesses by consulting firm Deloitte in partnership with Ryerson University.

4.5.1.2 Research, advocacy, and industry privacy frameworks

Research, advocacy, and industry groups are contributing to the privacy protection conversation, providing resources for practitioners from a multitude of sectors. Although only a sampling, the examples below provide a sense of the range of frameworks, toolkits, and standards developed to assist organizations in their pursuit of protecting privacy.

Best Practices for Mobile App Developers: Developed by the Future of Privacy Forum and the Center for Democracy and Technology, this guide outlines best practices for the collection, use, and transfer of personal data in the creation

[84] Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," August 2009.

[85] Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," August 2009.

and operations of mobile apps. It provides recommendations largely consistent with Privacy by Design and the OECD Privacy principles, including practice Privacy by Design; communicate openly and effectively; make your privacy policy easily accessible; use enhanced notice; provide users with choices and controls; secure your users' data; and ensure accountability.[86]

Digital Signage Privacy Standards: An industry group, the Digital Signage Federation created voluntary privacy guidelines for data collection and use through digital signage. The standards are largely based in OECD Privacy Principles and expand the concept from personal information to include pseudonymous data as well — data that could be reasonably associated with a particular consumer or property, like a device — and aggregate data.[87]

Anonymisation Decision Making Framework: The Framework offers a practical guide in anonymization — a privacy preserving technique — for any business or organization. Created in 2016 by the UK Anonymisation Network (UKAN), a consortium of universities, government offices, and non-profit research groups, it proposes that anonymization is about risk management and that zero risk is not a realistic possibility when producing useful data.[88] It highlights that data anonymization must consider what happens after data is anonymized, including managing risk arising from data sharing and use.

Anonymisation and Open Data: The Open Data Institute (ODI) created an introduction to managing the risk of re-identification of open data. Targeting the public sector but relevant to any organization the provides free, published data, the report discusses utility risk trade-off; emerging techniques in practice (e.g., differential privacy and synthetic data); and additional anonymization resources (e.g., anonymization case studies, list of industry and public-sector actors).

4.5.1.3 Emerging city-led privacy practices

Initiatives in a handful of cities demonstrate additional possibilities in integrating new approaches to enhance privacy protections for residents.

Open by preference: In 2016 the City of Seattle enacted an "open by preference" policy for their open-data program. Unlike the widely adopted best practice principle "open by

[86] "Best Practices for Mobile Application Developers," *Future of Privacy Forum* and *Center for Democracy & Technology*.
[87] "Digital Signage Privacy Standards," Digital Signage Federation, February 2011.
[88] Mark Elliot, Elaine Mackey, Kieron O'Hara, and Caroline Tudor, "The Anonymisation Decision-Making Framework," *UKAN Publishing*, United Kingdom.

default," Seattle's policy emphasizes privacy protections over openness. The policy requires that potential open-data sets are screened for privacy, security, and quality considerations before they are made public.[89] As part of the policy, the city will conduct an annual risk assessment of the Open Data Program with the Future of Privacy Forum. This evaluates the benefits and risks, the de-identification tools and strategies, data quality, equity and fairness, and transparency and public engagement.[90]

Technical privacy design strategies: Decentralized Citizen-Owned Data Ecosystems (DECODE), in partnership with the cities of Amsterdam and Barcelona, is building a privacy-preserving technical architecture to support multiple pilot projects. DECODE's privacy design strategies for technical architecture include:

- **Minimize.** Limit the processing of personal data as much as possible.
- **Separate.** Prevent the correlation of personal data by separating the processing logically or physically.
- **Abstract.** Limit as much as possible the amount of detail of personal data being processed.
- **Hide**. Protect personal data or make them unlinkable or unobservable. Prevent personal data from becoming public. Prevent exposure of personal data by restricting access, or hiding its very existence.
- **Inform.** Provide data subjects with adequate information about which personal data is processed, how it is processed, and for what purpose.
- **Control.** Provide data subjects mechanisms to control the processing of their personal data.
- **Enforce.** Commit to privacy-friendly way of processing personal data.
- **Demonstrate.** Provide evidence that you process personal data in a privacy-friendly way.[91]

Each strategy includes a description of associated technical tactics or mechanisms to achieve the principle. For example, to minimize personal data, the associate tactics could include "excluding or refraining from processing a data subject's personal data partly or entirely akin; selecting or deciding on a case by case basis on the full or partial usage of personal data; stripping or removing unnecessary personal data fields from the system's representation of each user; or destroying and completely removing a data subject's personal data."[92]

4.5.2 Digital rights, ethics, and tools

Just as cities adopt innovations in computation and technology, they also are rapidly working to implement strategies to protect the digital rights of residents. Ethical

[89] City of Seattle, Executive Order 2016-01: Directing Departments to Comply with the New Open Data Policy, Directing All City Data to Be Open by Preference,2016.
[90] City of Seattle, Executive Order 2016-01.

[91] Shehar Bano, et al., "Privacy Design Strategies for the DECODE Architecture", DECODE, June 2017.
[92] Shehar Bano, et al., Privacy Design Strategies for the DECODE Architecture", DECODE, June 2017.

practices — free from bias, discrimination, and harm — are central to a range of emerging policies and practices seen across the world. Cities are increasingly the stage for concrete action, originating from:

- **Policy-makers —** where city leaders are enacting new standards and practices, such as in Barcelona with Ethical Digital Standards and in New York City with the Automated Decision Systems Task Force and Guidelines for the Internet of Things.
- **Multi-sector collaboration —** where industry, academia, and communities are coming together to create new initiatives, such as in Amsterdam with the TADA manifesto and in Montreal with the Montreal Declaration for the Responsible Development of Artificial Intelligence (see Section 4.6.2.1 for a detailed overview of AI activities in Montreal)
- **Global movements —** led by a coalition of cities and non-governmental organizations like the Cities for Digital Rights.

In the growing recognition that legal compliance is only part of ethical data and information practices, more organizations are expanding ethics codes and tools to address things like non-personal data, the full life cycle of data, and issues beyond privacy and consent.[93] The following principles, research, and tools, while not exhaustive, illustrate some of the emerging best practices.

[93] Ellen Broad, Amanda Smith, and Peter Wells, *Helping Organisations Navigate Ethical Concerns in Their Data Practices*, Open Data Institute, 2017.

4.5.2.1 Principles, declarations, and codes

OECD Principles on AI: The Organisation for Economic Co-operation and Development member countries adopted the Principles on AI in May 2019 and are the first to be signed by governments. In addition to the values-based Principles, the OECD also made recommendations to governments; while these are not legally binding, they are highly influential.

Declaration on Ethics and Data Protection in Artificial Intelligence: In October 2018, at the 40th International Conference of Data Protection and Privacy Commissioners, several privacy and data protection offices, including Canada's Office of the Privacy Commissioner of Canada, endorsed guiding principles to preserve human rights in the development of AI.

National Standard of Canada: Ethical design and use of automated decision systems: The CIO Strategy Council published a national standard of Canada for automated decision systems in October 2019. The Standard is meant to help organizations design and implement responsible AI solutions. The Standard provides a framework and process that is meant to go beyond aspirational principles. The Standard is intended to be used by private organizations, public sector entities, and not-for-profit organizations.

Asilomar AI Principles: The Future of Life Institute's 2017 conference on beneficial artificial intelligence (AI) brought together AI researchers and experts in economics, law, ethics, and philosophy to discuss the opportunities and challenges related to the future of artificial intelligence and to outline steps to make technology beneficial. The group developed 23 principles around three themes:

- **Research issues**, including goals, funding, policy, culture, and safety.
- **Ethics and values**, covering safety, transparency, responsibilities, values, privacy, liberty, shared benefit and prosperity, and human control.
- **Long-term issues** around capabilities, risks, and the common good.[94]

Toronto Declaration Protecting the Right to Equality and Non-discrimination in Machine Learning Systems: Led by international human and digital rights organizations Access Now and Amnesty International, and launched at the May 2018 human rights conference RightsCon, the declaration calls on states and private actors to work together in protecting individuals and groups from discrimination.[95]

The declaration supports states and private actors in promoting the development and use of machine learning and other technologies so long as they enable people to exercise their human rights. To prevent discrimination, protect the rights of all individuals and groups, and promote diversity and inclusion, the framework outlines specific duties for states and for private actors. States must identify risks, ensure transparency and accountability, enforce oversight, promote equality, and hold private sector actors to account. Private-sector actors have the responsibility of human rights due diligence, which includes identifying potential discriminatory outcomes; taking effective action to prevent and mitigate discrimination, and track responses; and being transparent about efforts to identify, prevent, and mitigate against discrimination.[96]

Montreal Declaration for the Responsible Development of Artificial Intelligence: The University of Montreal, in collaboration with the Fonds de recherche du Québec, launched the Montreal Declaration for Responsible Development of Artificial Intelligence in December 2018. Developed with a wide range of stakeholders, the Declaration provides principles and recommendations for the ethical development of AI.[97] Additional information on the Declaration is provided in Section 4.6.2.1.

---

[94] Future of Life Institute, "Asilomar AI Principles," accessed September 19, 2019.

[95] Amnesty International and Access Now, "The Toronto Declaration: Protecting the Right to Equality and Non-discrimination in Machine Learning Systems," 2018.

[96] Amnesty International and Access Now, "The Toronto Declaration."

[97] "The Declaration for responsible AI development," Montréal Declaration Responsible AI website, accessed September 19, 2019.

Universal Guidelines for Artificial Intelligence: The guidelines were developed at an October 2018 conference led by the Public Voice coalition and in partnership with the International Conference of Data Protection and Privacy Commissioners. They are intended to be incorporated into standards, laws, agreements, and technology systems, but emphasize that the primary responsibility in protecting human rights lies with the funders, creators, and users of AI systems.[98] The 12 guidelines aim to maximize benefit and minimize the harm of AI by supporting:

- **Transparency.** All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, logic, and techniques that produced the outcome.
- **Human determination.** All individuals have the right to a final determination made by a person.
- **Public identification.** The institution responsible for an AI system must be made known to the public.
- **Fairness.** Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.
- **Assessment and accountability.** An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.
- **Decision accuracy, reliability, and validity.** Institutions must ensure the accuracy, reliability, and validity of decisions.
- **Data quality assurance.** Institutions must establish data provenance, and assure quality and relevance for the data input into algorithms.
- **Public safety assessment.** Institutions must assess the public safety risks that arise from the deployment of AI systems that direct or control physical devices, and implement safety controls.
- **Cybersecurity protection.** Institutions must secure AI systems against cybersecurity threats.
- **Secret profiling ban.** No institution shall establish or maintain a secret profiling system.
- **Unitary scoring ban.** No national government shall establish or maintain a general-purpose score on its citizens or residents.
- **Termination.** An institution that has established an AI system has an affirmative obligation to terminate the system if human control of the system is no longer possible.[99]

[98] The Public Voice, "Universal Guidelines for Artificial Intelligence," October 23, 2018.

[99] The Public Voice, "Universal Guidelines for Artificial Intelligence," October 23, 2018.

4.5.2.2 Existing tools

Data Ethics Canvas: The Open Data Institute developed the Data Ethics Canvas as a tool to identify potential data ethics issues. Based on tools created by ADAPT Centre and Alex Osterwalder, the Canvas is focused specifically on data collection (completeness, design methods, accuracy, and context); sharing (restricted parties, or parties with access); and use (models, analysis, purpose, and margin for error).

The Canvas articulates key questions across several topics covering data sources, ethical and legal contexts, project purpose and communication, positive and negative effects on people, engagement, openness and transparency, and implementation process and actions. For example, on the topic of communication, it asks, "Do people understand your purpose — especially people who the data is about or who are impacted by its use? How have you been communicating your purpose? Has this communication been clear? How are you ensuring more vulnerable individuals or groups understand?"[100] The Canvas is devised to be used throughout a project life cycle and as a discussion tool. By working through potential risks, the Canvas can help reduce bias and design better products and services.[101]

[100] Open Data Institute, *Data Ethics Canvas*, May 2019.
[101] Open Data Institute, *Helping Organisations Navigate Ethical Concerns in Their Data Practices*, September 2017.

Ethics and Algorithms Toolkit: The Toolkit is a risk management framework intended for city governments developed by the Center for Government Excellence in partnership with the City and County of San Francisco, Harvard's Data-Smart City Solutions, and Data Community DC. Created to help address the gap between ethics research and practice, the toolkit assists users through understanding the potential impacts of using an algorithm, articulating potential risks, and identifying risk mitigation approaches.[102]

The toolkit provides a multistep process, separated into assessing algorithmic risk and managing risk. The algorithmic assessment examines four types of risks:

- **Impact,** evaluating type, degree, scale, and direction.
- **Appropriate use**, including consistency, compatibility, reputation, and perception.
- **Accountability** through automation, explainability, auditability, and accessibility.
- **Bias**, including representativeness, inaccuracy, training data scope, and methodology.[103]

The outcome of this assessment guides the risk mitigation and management.

Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability: Researchers from the AI

[102] GovEx, the City and County of San Francisco, Harvard DataSmart, and Data Community DC, *Ethics & Algorithms Toolkit*, accessed September 29, 2019.
[103] GovEx, et al., "Ethics & Algorithms Toolkit," 2018.

Now Institute at New York University created the Algorithmic Impact Assessments (AIA) framework to support government agencies and the communities they serve to create a process of engagement and accountability around the use of automated decision systems. The framework outlines five key elements of an AIA, which includes:

- **Self-assessment** of existing and proposed automated decision systems and evaluate potential negative impacts.
- **External review** by external researchers and auditors.
- **Public notice and disclosure** of automated decision systems, self-assessments, and review processes.
- **Public comment**.
- **Enhanced due process** for affected individuals or communities.[104]

The researchers also highlight potential challenges with implementing AIA, including difficulty defining automated decision systems, trade secrets of proprietary systems, assessing multiple types of harms (beyond harms of allocation), and funding and resources to implement and maintain the AIA process.[105] Beyond the primary goals of accountability and public participation, potential additional benefits include increased expertise within public agencies, greater ease with public record requests, and more vendors that provide open systems.

4.5.2.3 Emerging research

Annotation and Benchmarking on Understanding and Transparency of Machine Learning Lifecycles (ABOUT ML): The recently launched ABOUT ML project aims to "develop, test, and promulgate documentation best practices for transparency in machine learning."[106] Led by Partnership on AI, with the Tech Policy Lab at the University of Washington and guided by a 30-member steering committee, the project will address the existing gap in industry consensus about disclosure and documentation methods in machine learning (ML).[107]

The multi-year project will include assessing current research and current practices in ML documentation; creating, testing, and iterating on pilots; evaluating best practices based on evidence; and promulgating findings.[108] At the end of July 2019, the project released a summary of existing research on

[104] Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker, "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability," AI Now, April 2018.
[105] Reisman, et al., "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability."
[106] Partnership on AI, "Annotation and Benchmarking on Understanding and Transparency of Machine Learning Lifecycles (ABOUT ML)," 2019.
[107] Partnership on AI, "Annotation and Benchmarking on Understanding and Transparency of Machine Learning Lifecycles (ABOUT ML)," accessed September 19, 2019.
[108] Partnership on AI, "Annotation and Benchmarking on Understanding and Transparency of Machine Learning Lifecycles (ABOUT ML)," accessed September 19, 2019.

documentation for transparency space and the current challenges for public review and comment.

Model Cards for Model Reporting: Researchers from Google and the University of Toronto recently presented a paper and proposed tool to increase transparency about machine learning and artificial intelligence systems. Model cards provide qualitative information about the model as well as quantitative evaluation of the results of the model broken down by demographic characteristics. Model cards provide a framework for a report that contain details on the model's intended use, factors, evaluation metrics, training data, evaluation data, ethical considerations, and caveats and recommendations.

Datasheets for Datasets: A group of academic and industry researchers presented a standardized approach to documenting data sets for machine learning at the Workshop on Fairness, Accountability, and Transparency in Machine Learning, in Stockholm, in July 2018. To reduce the risk of data misuse and increase transparency between the creators and users of datasets, the concept proposes that every dataset be accompanied with a datasheet documenting its creation and management.[109] The datasheet would include questions about the motivation for dataset creation, composition of data; data collection process; data processing, cleaning and labelling; dataset distribution; dataset maintenance; and legal and ethical considerations.

4.5.3 Responsible data sharing

Over the last decade, cities have integrated data into their core operations. Faced with greater expectations from residents as well as new opportunities (and budgetary constraints) to better utilize resources, cities have launched formal efforts to share data and achieve greater impact. This includes leveraging existing data sources, such as the administrative data collected through typical city business processes (property records and business licenses, for example), in new ways, as well as incorporating new data sources from sensors and devices, social media, and corporations (for example, smart water meters, fleet GPS, Yelp reviews, Uber or ride-sharing apps, and imagery) into policy-making and public service delivery.

In addition to greater data use within city governments, there is also growing recognition that the challenges cities face are dynamic and interconnected, requiring cooperation, including the sharing of data, across sectors. This is seen in a number of trends, including the emergence of data-focused offices within government that are often responsible for open-data initiatives and data-driven improvements to public service delivery (such as New York City's Mayor's Office of Data Analytics, London's City Data Analytics Programme, and San Francisco's DataSF); federal and philanthropic funding

[109] Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé III, and Kate Crawford, "Datasheets for Datasets", arXiv:1803.09010v3, July 9, 2018.

supporting the use of technology and data within city government (Canada's Smart Cities Challenge, the U.S. Department of Transportation's Smart City Challenge; and multi-sector data collaborations united around a common cause or interest (such as Waze's Connected Cities Program, Korean telecom KT Corporation's collaboration with the Korean Society of Infectious Disease, multinational bank BBVA's partnership with United Nations Global Pulse to address disaster recovery, and information broker Nielsen's relationship with the University of Chicago to generate consumer purchasing behaviour datasets).

Delivering value from data is tied to how data is used.[110] Research led by the Governance Lab (GovLab) outlines five ways in which sharing data across sectors delivers public value, including:

- **Situational awareness**, meaning a more complete picture and ability to understand conditions on the ground, especially in emergency first response and recovery, which requires coordination across different levels of government, non-profit service providers, and private sector contractors.
- **Public service design and delivery**, in which shared data can enable more accurate and efficient design and delivery of public services.
- **Knowledge creation and transfer,** including bringing different data together to fill knowledge gaps and provide the most useful information to those responsible for solving problems.
- **Prediction and forecasting** to assist in proactive, evidence-based risk mitigation.
- **Impact assessment and evaluation,** where data from other sectors enables monitoring and evaluation of policies.[111]

Similarly, in looking specifically at government-led sharing initiatives, some of the same researchers have outlined a taxonomy of open data impact. In sharing government-held data with the public, open-data initiatives foster:

- **Public problem-solving** through enabling residents and policy-makers to engage in new ways to address public challenges.
- **Opportunity creation** for residents and business to leverage data, innovate, and economically prosper.
- **Government improvement** through increased transparency and accountability.
- **Citizen empowerment,** including more informed decision-making.[112]

---

110 Kurtis McBride, "The Role of a Data Strategy for Canadian Industries: Monetizing Smart Cities: Framing the Debate," Center for International Governance Innovation, March 28, 2018.

111 Stefaan Verhulst, Andrew Young, and Prianka Srinivasan, "An Introduction to Data Collaboratives: Creating Public Value by Exchanging Data," GovLab, Unicef, and Omidyar Network, 2015.

112 Verhulst and Young, "Open Data Impact: When Demand and Supply Meet," GovLab and Omidyar Network, 2016.

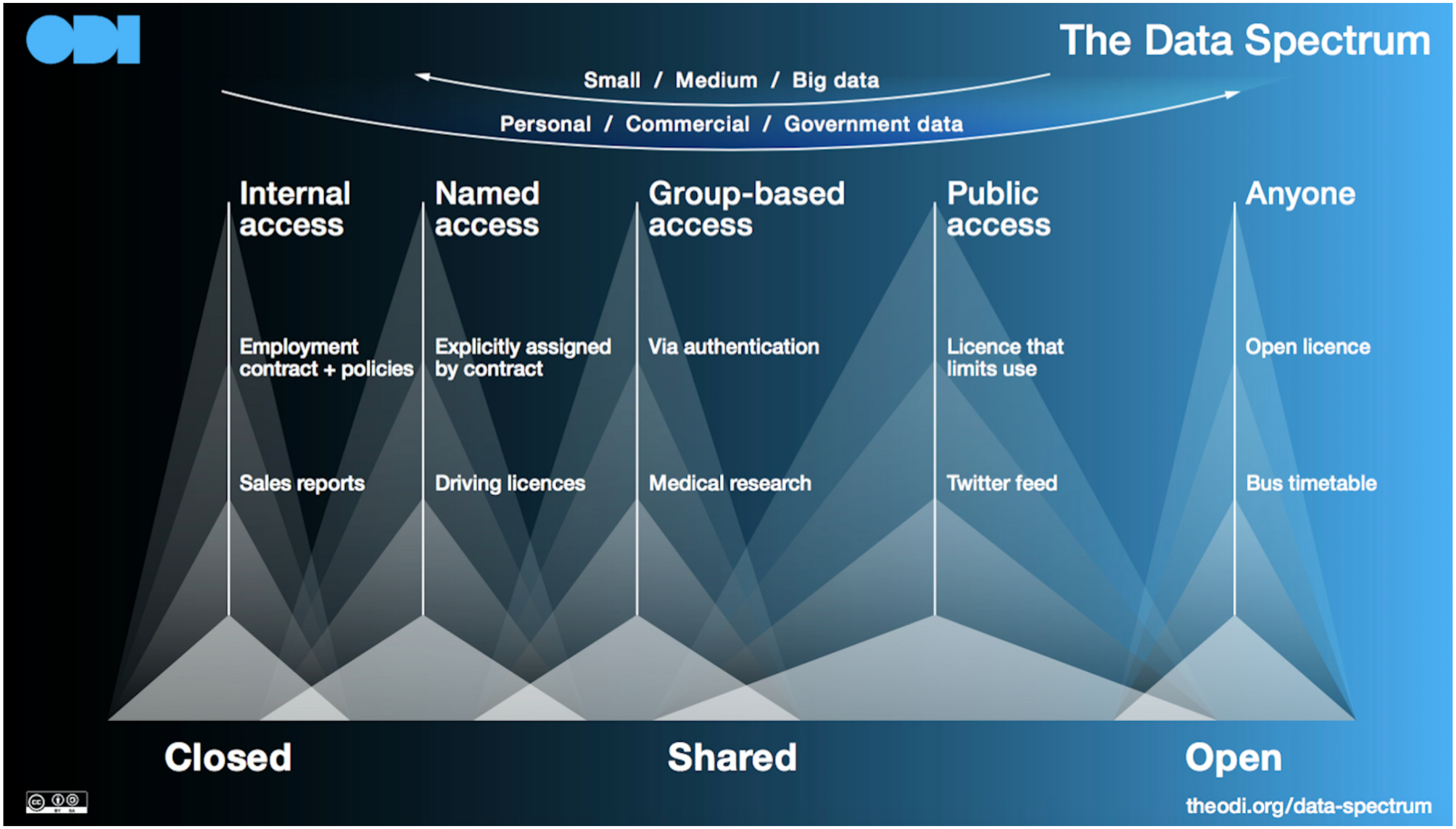
4.5.3.1 Approaches to data sharing

There are several different approaches to sharing data. As the UN Sustainable Development Solution Network's Thematic Research Network on Data and Statistics (TReNDS) acknowledges, there is no one right way of harnessing data and no one perfect system.[113] Similarly, there is no single way to classify and describe data sharing methods; however, some research organizations have developed frameworks to explore different data sharing approaches, create common language and understanding, and build a body of research.

In terms of data access, the Open Data Institute (ODI) created the Data Spectrum (see image below) to illustrate a range of access — from closed to shared to open. The Data Spectrum emphasizes that no matter the size of the data or the source, access is determined by the type of license that enables or limits use.[114]

[113] Sustainable Development Solutions Network Thematic Research Network on Data and Statistics (SDSN TReNDS), "Counting on the World: Building Modern Data Systems for Sustainable Development," September 1, 2017.
[114] "The Data Spectrum," Open Data Institute, accessed September 17, 2019.

Figure: The Data Spectrum (Open Data Institute[115])



115 [Open Data Institute. "The Data Spectrum."](https://theodi.org/data-spectrum) Last modified November 19, 2015. Reproduced and used in accordance with the terms of the Creative Commons Attribution-ShareAlike 2.0 UK: England & Wales License.

In a similar but more expansive effort, the ODI is in the process of creating a classification of different data access "procedures, mechanisms, agreements and structures" through its Data Access Map (formerly the Data Access Archipelago; see image below).[116] Recognizing the difficulty in understanding the "vast and confusing landscape" of different data sharing approaches, the map identifies different models based on distinguishing elements and groups them based on shared attributes.[117] While the map contains 64 different data sharing models located across eleven "islands," the ODI points out that the models include significant overlap and are difficult to compare to one another. Additionally, different models are often used in combination with each other. For example, the "Collaborador Coast" includes 12 models that are primarily focused on collaboration, including data repositories, data platforms, data labs, data pooling, data portals, data trusts, data commons, data clubs, data marketplaces, data exchanges, and data clearinghouses.[118] These collaboration-based models may use models found in the technical-mechanism-centred "Technicaledonia," which includes application programming interfaces (APIs), data warehouses, bulk data transfers, sneakernet, privacy-enhancing technologies, data lakes, data cubes, data observatories, intelligence products, collaboration tools, dashboards, public data visualizations, heat maps, and interactive reporting. While still a work in progress, the Data Access Map is a first step in highlighting the multitude of ways in which data sharing can be accomplished.

[116] "Data Access Archipelago: Mapping the Myriad Ways We Share Data," Open Data Institute, accessed September 19, 2019.
[117] "Mapping the Wide World of Data Sharing," Open Data Institute, accessed September 19, 2019.
[118] "Data Access Archipelago," Open Data Institute website, accessed September 19, 2019.

Figure: The Data Access Map (Open Data Institute[119])

119 Open Data Institute. "Mapping the wide world of data sharing." Last modified July 4, 2019.. Reproduced and used in accordance with the terms of the Creative Commons Attribution-Share-Alike 2.0 UK: England & Wales License.

GovLab focuses specifically on "data collaboratives," which they define as "a new form of multilateral collaboration where participants from different sectors — including private companies, research institutions and governments — can exchange data to help solve public problems."[120] According to GovLab, there are six types of data collaboratives:

1. **Data cooperatives or pooling**, in which corporations and other data holders group together to create data pools with shared data resources.
2. **Prizes and challenges**, where data is available to qualified applicants to develop new apps or discover innovative uses for the data.
3. **Research partnerships**, in which data is shared with universities and other academic organizations, giving researchers access to consumer or client datasets to analyze social trends.
4. **Intelligence products,** where shared data is used to build a tool, dashboard, report, app, or other technical device to support a public or humanitarian objective.
5. **Application programming interfaces,** which give developers access to data for testing product development and for analysis.
6. **Trusted Intermediary**, in which corporations and other data holders share data with a limited number of known partners for a specific purpose or activity.[121]

[120] Verhulst, Young, and Srinivasan, "An Introduction to Data Collaboratives."
[121] Verhulst, Young, and Srinivasan, "An Introduction to Data Collaboratives."

There are indications that data collaboratives are increasing. On their website, GovLab has documented over 150 examples of data collaboratives worldwide, created a library for scholarly research, and designed a guide and other resources for forming data collaboratives. Similarly, the World Economic Forum and McKinsey & Company report that the number of companies creating data-related partnerships grew from 21 percent to 40 percent between 2017 and 2019.[122]

4.5.3.2 Barriers to data sharing

While there are various approaches and mechanisms to share data, several researchers highlight the challenges in sharing data. As the ODI Data Access Map begins to illustrate, identifying the "right combination of governance, oversight and enforcement mechanisms, ethical review processes, technical mechanisms, legal structures and stakeholder engagement strategies" is a challenge in creating any data sharing model.[123]

The World Economic Forum's report "Data Collaboration for the Common Good" explores both the benefits and barriers to sharing data across organizations, identifying trust as a critical component in overcoming various types of risks.

[122] World Economic Forum and McKinsey & Company, "*Data Collaboration for the Common Good: Enabling Trust and Innovation Through Public-Private Partnerships,*" 2019.
[123] "Data Access Archipelago," Open Data Institute.

These risks include:

- **Commercial concerns** about data rights, brand reputation, and disclosure of proprietary or commercially sensitive information.
- **Regulatory uncertainty** from fragmented legal and policy frameworks across sectors and sovereign borders.
- **Security vulnerabilities** in data infrastructure, and lack of security expertise and practices across sectors.
- **Privacy and ethical concerns** in the ability to preserve privacy, protect vulnerable populations, and uphold human rights.[124]

To facilitate collaboration and overcome such challenges in sharing data, they propose six dimensions of a trustworthy system, in which stakeholders can focus and align, including:

1. **Security**, including the people, processes, and tools required to ensure confidentiality, integrity, and availability of data.
2. **Accountability** that ensures network stakeholders are held responsible for upholding accepted standards and agreements and for providing oversight that leads to accurate and unbiased outcomes.
3. **Transparency,** including accessible and understandable information on data use, outcomes, and relationship structures.
4. **Auditability,** including externally checking, verifying, and monitoring data flows across stakeholders or jurisdictions.
5. **Equity** through ensuring value is apportioned fairly and outcomes are unbiased.
6. **Ethics**, including principles to guide stakeholders through ambiguous and complex decisions.[125]

Another emerging effort to overcome the challenges and risks to data collaboration is Contracts for Data Collaboration (C4DC). Created by a consortium of research and non-governmental actors, including GovLab, TReNDS, University of Washington, and the World Economic Forum, C4DC seeks to reduce the uncertainty and transaction costs of developing contractual agreements for data sharing. The initiative is developing a toolkit for non-legal experts and creating a repository of contractual clauses taken from existing legal agreements.[126]

4.5.3.3 The data trust model

In looking to advance responsible data use, many organizations are proposing a data trust model for the collection and management of data across organizations and

[124] World Economic Forum and McKinsey & Company, "Data Collaboration for the Common Good."

[125] World Economic Forum and McKinsey & Company, "Data Collaboration for the Common Good."

[126] Verhulst and Young, "Introducing the Contractual Wheel of Data Collaboration," *Medium,* April 24, 2019.

sectors. A data trust, in simple terms, is an approach to data stewardship. The general purpose is to provide a repeatable and trusted framework to responsibly collect, manage, and share data.

The data trust concept is rapidly evolving. While there is no unified consensus around what a data trust is and how it functions, several organizations and researchers are leading conversations about data trusts. This includes research, convenings, advocacy, and pilot projects. Some of the dominant voices in the data trust space include:

The Open Data Institute (ODI): Following the 2017 independent review of artificial intelligence for the UK government, which recommended the development of data trusts to improve trust and increase ease of access to data, and to facilitate the sharing of data between organizations, the ODI has been engaged in developing research on data trusts. This includes:

- Initial research into the multiple interpretations of data trusts found several interpretations of data trusts, including a repeatable framework of terms and mechanisms, a mutual organization, a legal structure, a store of data, and public oversight of data access.
- "Data Trust Summary Report," "Data Trusts: Lessons from Three Pilots," and "Designing Decision Making Processes for Data Trusts." Based on three pilots with city government, private sector food retailers, and non-governmental environmental groups, the ODI issued several reports that more clearly define what a data trust is, the benefits of data trusts, relevant design and decision-making processes, and recommendations for governments, policy-makers, and other stakeholders interested in creating a data trust.[127] The ODI defines a data trust as a "legal structure that provides independent stewardship of data" to balance conflicting views and incentives about data, deliver some of the many benefits that better data access can bring, reduce costs and skills needed to steward and share data, create new opportunities for innovation and business, make control more representative, and ensure data's benefits are distributed widely, ethically, and equitably.[128]
- "Data Trusts: Legal and Governance Considerations." This report commissioned legal experts to explore what a data trust is in legal terms, potential legal structures, data sharing, and governance mechanisms. The ODI does not recommend trust law as an appropriate legal structure for data trusts.

Digital Public (Sean McDonald and Keith Porcaro): The digital governance group Digital Public proposed the creation of a civic trust in 2015 as a "model of public participation in the ownership of intellectual property."[129] Based on a legal trust, the civic trust provides the organizational and legal

[127] Jack Hardinges, Peter Wells, Alex Blandford, Jeni Tennison, and Anna Scott, "Data Trusts: Lessons from Three Pilots," Open Data Institute, 2019.
[128] Open Data Institute, "Data Trusts Summary Report," 2019.
[129] Sean McDonald and Keith Porcaro, "The Civic Trust," *Medium,* August 4, 2015.

mechanisms to protect the public's interest in digital utilities, including data and code bases.[130] McDonald has also written more recently about data trusts with scholars such as Bianca Wylie.[131]

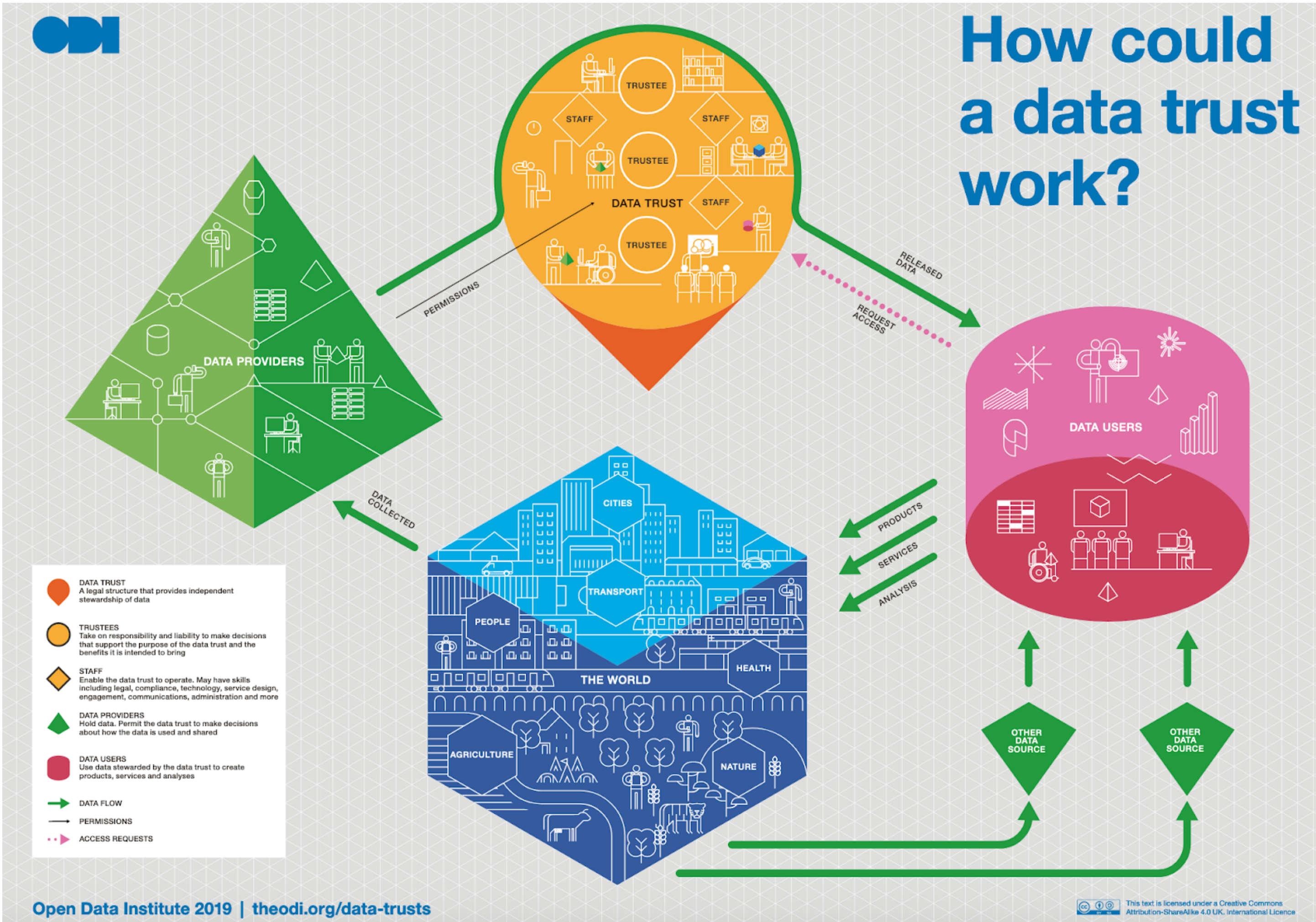
Medical and Related Sciences (MaRS) Discovery District: Based on convenings and research, the MaRS "Primer on Civic Digital Trusts" presents a definition of civic digital trusts, provides examples, and explores design, technical architecture, and business model options for such trusts.

- A civic digital trust extends the concept of a legal trust with fiduciary duties to the management the digital layer of a smart city.[132] MaRS proposes that trustees are responsible for managing digital assets such as physical infrastructure (such as sensors and data warehouses), code bases (such as databases, standards, processing structures, and interfaces), and data on behalf of residents, visitors, businesses, workers, and institutions in a defined urban zone where data is collected (a neighbourhood, district, or city, for example).[133]

---

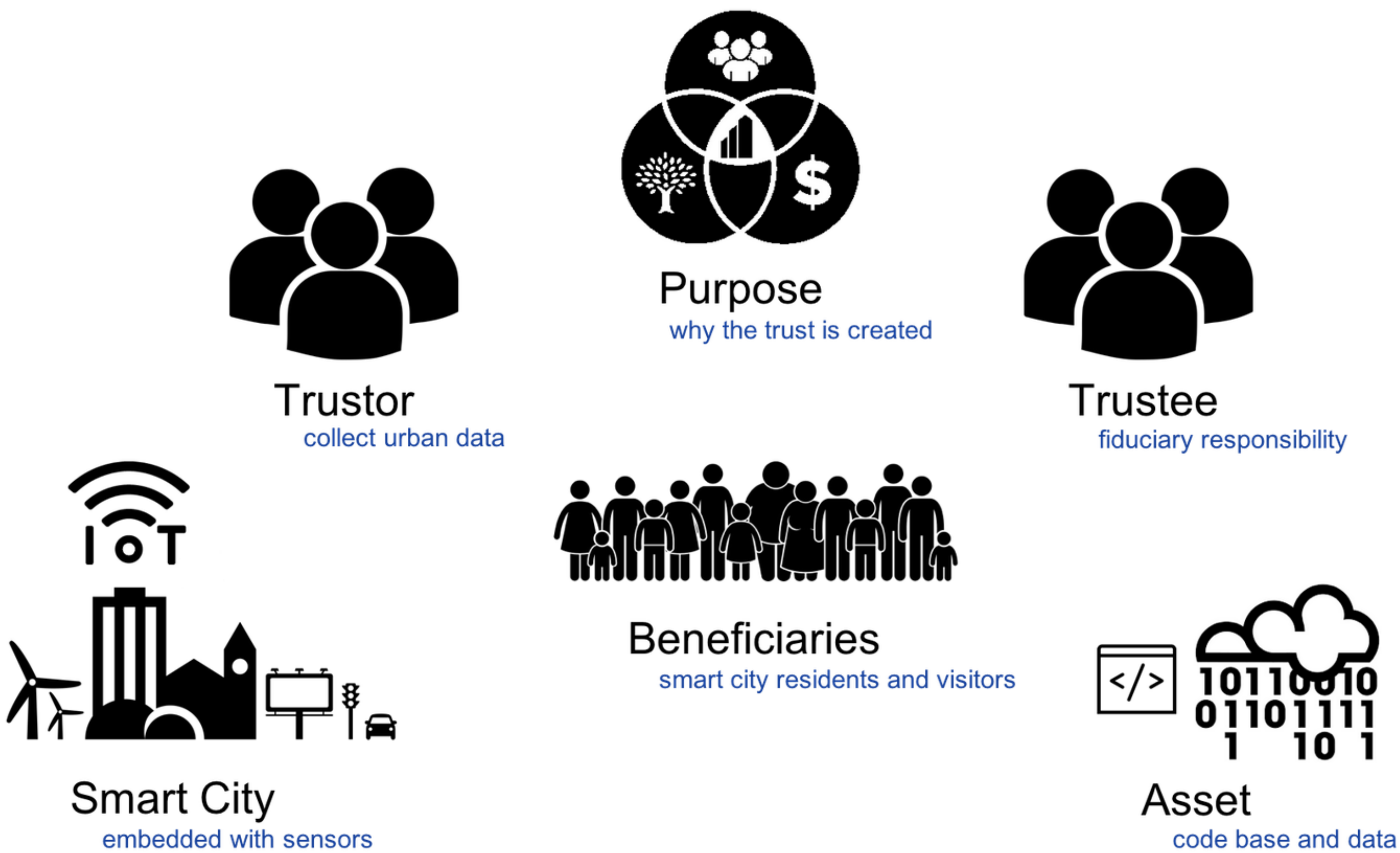
[130] McDonald and Porcaro, "The Civic Trust."
[131] Bianca Wylie and Sean McDonald, "What is a Data Trust?", CIGIOnline, October 9, 2018.
[132] MaRS, "What Is a Civic Digital Trust?," *A Primer on Civic Digital Trusts*, accessed September 19, 2019.
[133] MaRS, "What Is a Civic Digital Trust?."

Figure: Diagram of a Proposed Data Trust (Open Data Institute[134])



[134] Open Data Institute. "How do we unlock the value of data while preventing harmful impacts." Accessed October 9, 2019. Reproduced and used in accordance with the terms of the Creative Commons Attribution-ShareAlike 4.0 UK. International License.

Figure: Essential Elements of a Civic Digital Trust (MaRS Discovery District, [A Primer on Civic Digital Trusts](), 2019)



Essential elements of a civic digital trust.

Nesta: The UK-based foundation focused on innovation examines data governance needs and advocates for the creation of new and different kinds of data trusts, which they call a "new ecosystem of trust." Nesta suggests that the task of creating trust in data governance is different depending on the field or context and that generic solutions will fail.[135] Instead, they propose a variety of types of data trusts ranging from personal data stores to industry data stewardship trusts (such as banking) to public private benefit trusts (such as shared streets) to public data trusts (such as police or health data trusts).

Element AI: The Canadian artificial intelligence products provider Element AI joined with Nesta to lead an international workshop on data trusts in December 2018, which explored data trusts as a new governance model that moves beyond current compliance-based data sharing approaches. The workshop convened experts in data governance, machine learning, law, privacy, and public policy, and created recommendations to encourage policy-makers to explore data trusts through collaborative pilots, data literacy campaigns, and new legislation or policy frameworks.[136] While the group loosely defines data trusts as a "third-party stewardship model based on the common law trust," it also recognized that other legal structures or corporate governance models may be more appropriate.[137] Element AI also recently announced a strategic partnership with Mozilla Foundation to explore data trusts as a way to give both citizens and consumers more control – and greater social return – over the use of their personal information. The partnership will fund and support policy and legal research, along with the technical and design components necessary to make data trusts a practical reality.[138]

In addition, the table on the following page provides a sampling of the diversity of concepts, terms, and structures for data trust models, proposed by a range of sources. While some models propose a legal trust structure, others, particularly the ODI, suggest that a data trust should not focus on any particular legal structure.

135 Geoff Mulgan and Vincent Straub, "The New Ecosystem of Trust," Nesta, February 21, 2019.
136 Element AI and Nesta, "Data Trusts:A New Tool for Data Governance," 2018.
137 Element AI and Nesta, "Data Trusts:A New Tool for Data Governance," 2018.
138 Element AI, "Element AI and Mozilla Foundation Partner to Build Data Trusts and Advocate for the Ethical Data Governance of AI," 2019

Table: Summary Overview Comparing Data Trust Models

Concept name	**Data trust**	**Data trust: traditional legal trust model**	**Data trust: contractual framework model**	**Data trust: corporate model**	**Data trust: bottom-up approach**	**Civic digital trust**	**Civic trust**
Author / organization	**Open Data Institute**	**Open Data Institute**			**Element AI with Nesta**	**MaRS Discovery District**	**Sean McDonald and Keith Porcaro**
Publication (source)[139]	*Data Trusts: Lessons from Three Pilots*	*Data Trusts: Legal and Governance Considerations*			*Data Trusts: A new Tool for Data Governance*	"Primer on Civic Data Trusts"	"The Civic Trust"
Publication date	April 2019	April 2019			March 2019	December 2018	August 2015
Link to reference material	https://theodi.org/article/odi-data-trusts-report/	https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf			https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf	https://marsdd.gitbook.io/datatrust/	https://medium.com/@McDapper/the-civic-trust-e674f9aeab43

139 This table was created primarily as a tool for internal discussion at Sidewalk Labs to understand and compare how different organizations and researchers define and characterize a "data trust" across key components. The language in the source documents includes many legal terms that have a very specific meaning. For the purposes of comparison, Sidewalk Labs did not want to interpret the language and therefore pulled the relevant content and present it here unchanged, with the exception of minor formatting edits.

Table: Summary Overview Comparing Data Trust Models

Concept name	Data trust	Data trust: traditional legal trust model	Data trust: contractual framework model	Data trust: corporate model	Data trust: bottom-up approach	Civic digital trust	Civic trust
Description	A legal structure that provides independent stewardship of data, without being a legal trust.	A traditional legal trust in which data assets are provided to a legal trust and managed by the trustees for the benefit of its beneficiaries.	Similar to a standard form of a data-sharing agreement that would, without having a separate organizational structure in place, form a contractual agreement by which the data trust can allow provider data to be used by third parties for purposes within the aims of the trust.	A separate company or partnership set up to manage data and provide access to it. An unincorporated association could be used as an alternative group structure.	Data subjects pool their own data into a legal data trust structure for a social or economic benefit of their choosing.	A trust relating to cities or towns that is established to manage the digital layer of a smart city. The assets the trustees are responsible for managing include the physical infrastructure (sensors and data warehouses), code base (database, standards, processing structures and interface), and data that make up the digital layer. Civic participation is required in the governance of the trust. The civic digital trust may also manage financial assets to ensure the sustainable operation of the trust.	An independent organization that builds public participation into decision-making, and owns and manages underlying code and data resources, including providing limited, revocable access to resources.

Table: Summary Overview Comparing Data Trust Models

Concept name	Data trust	Data trust: traditional legal trust model	Data trust: contractual framework model	Data trust: corporate model	Data trust: bottom-up approach	Civic digital trust	Civic trust
Description	A data trust decides who has access, under what circumstances, and for whose benefit. Where ordinarily an organization that collects and holds data would automatically be the one to steward it, in the data trust model one or more organizations can permit the trust to make decisions about how the data is used and shared. The data trust would make decisions about how the data is used for an agreed-on purpose while taking all relevant stakeholder interests into account.						

Table: Summary Overview Comparing Data Trust Models

Concept name	Data trust	Data trust: traditional legal trust model	Data trust: contractual framework model	Data trust: corporate model	Data trust: bottom-up approach	Civic digital trust	Civic trust
Participants	**Data holders** from the private, public, and social sectors delegate data stewardship to the data trust. **Data trust trustees**, an independent group, take on the responsibility to make decisions about how the data is used and shared and must ensure the decisions support the purpose of the data trust and the benefits it is intended to bring. Trustees have a legally binding responsibility to take the interests of data holders, data users, citizens, and other stakeholders into account.	**Settlor** who gives (data) assets to trustees. **Trustees** own assets and are obliged to use them for the benefit of the beneficiaries.	**Data providers:** An organization that holds data and permits the data trust to make decisions about how the data is used and shared.	**Data providers,** or shareholders, provide or license data to the corporate organization **Directors** are representatives of data providers or independent, externally appointed individuals who make day-to-day decisions on running the trust.	**Data subjects** are both the settlors who place code, data, and technology objects into the trust and the beneficiaries for whom the trust and its term have been established. **Trustees** manage the objects in the beneficiaries' best interests according to the terms of the trust.	**Assets** include the physical infrastructure (sensors and data warehouses), code base (database, standards, processing structures, and interface), and data that make up the digital layer. **Beneficiaries** include the residents, visitors, businesses, workers, and institutions in a defined urban zone where data is collected. This could be a neighbourhood, a district, or an entire city.	**Assets** are anything of value, including code base (databases, standards, processing structures, and interfaces) and data. **Grantors** are the individuals or companies that own an original technology asset. Once the grantor places an asset in trust, the grantor no longer owns the asset. In many cases, the grantor may continue to contribute to the asset or retain a license.

Table: Summary Overview Comparing Data Trust Models

Concept name	Data trust	Data trust: traditional legal trust model	Data trust: contractual framework model	Data trust: corporate model	Data trust: bottom-up approach	Civic digital trust	Civic trust
Participants	**Data users** include "direct beneficiaries," such as startups and researchers, as well as "indirect beneficiaries," such as people, communities, and organizations that might use or benefit from the use of insights, products, and services created by its direct beneficiaries. **Other potential participants** include residents, consumers, or governments that advocate for or require the creation of a data trust to provide more participation and benefit to more people.		**Third parties** are not a main party to the agreement, but may be affected by it by way of data transfers for processing purposes or as beneficiaries, without being a main party in the agreement and providing consideration.			**Trustees** are the group of people with a fiduciary responsibility to protect the interests of the beneficiaries and who would put into place governance structures such as public accountability and participation. **Trustors** are individuals, companies, agencies, and governments who donate digital and financial assets to the trust. A trustor may receive a license from the trust to use the data it donated.	**Beneficiaries** are those who are meant to be served by the use of an asset and could be specific (a single person), general (users of a tool or asset), or very, very general (people). Beneficiaries have a legal right to challenge whether a trustee is doing its job and are the ultimate "owners" of the assets. **Trustees** are the people or organizations responsible for managing assets and fulfilling the trust's purpose in the beneficiary's interests.

Table: Summary Overview Comparing Data Trust Models

Concept name	Data trust	Data trust: traditional legal trust model	Data trust: contractual framework model	Data trust: corporate model	Data trust: bottom-up approach	Civic digital trust	Civic trust
Legal Trust (Y/N)	**N**	**Y**	**N**	**N**	**Y**	**Y**	**Y**
Proposed legal structure	Multiple legal structures can be used, including contractual frameworks, corporate models, charities, a public model with a new regulator, and community interest companies (CICs). Each data trust will need its own individually designed legal structure. It's not possible to recommend any single form of legal structure or even produce a set of templates from which data trusts could choose.	Legal trust.	Signed written agreements relate to each party's obligations, define the purpose of data use and access, and ensure security of personal data.	Limited liability corporation (LLC) or company limited by guarantee (CLG), with each member being an equal partner.	Legal trust.	Legal trust.	Legal trust.

Additionally, the technical architecture, organizational, or business structure, and additional services, are all variable based on the purpose of the trust. For example, the ODI suggests that the data trust should be independent of the technical architecture, such that the technical infrastructure remains flexible to needs and avoids vendor lock-in.[140] MaRS offers similar guidance, stating that different technical architectures can address different legal requirements.[141] Likewise, business models can encompass a wide range of options and may be dependent on funding sources.[142, 143]

4.5.3.4 Technology enabling data sharing

As noted above, there are numerous approaches to sharing data, from limited one-off data sharing agreements to freely licensed open-data portals. Advancements in technology continue to enable and expand the ways in which data can be securely stored, analyzed, and shared. Research from the World Economic Forum, MaRS Discovery District, and the ODI all emphasize that data sharing requires a "fit-for-purpose" technical infrastructure that supports the purpose of that data sharing initiative.[144, 145, 146]
One of the most significant decisions regarding technical infrastructure is the centralization (or decentralization) of data assets.[147] Both the World Economic Forum and Mars Discovery District outline some essential technical infrastructure models, including:

- **Centralized,** in which data is stored in one location with a central point of access.
- **Semi-centralized or federated,** where datasets are stored in a number of different secure locations and access is enabled through a central portal, platform, or secure APIs (application programming interfaces)
- **Decentralized or distributed,** in which data is stored across various secure locations and shared through an index, catalogue, or blockchain[148, 149, 150]

---

140 Hardinges, Wells, Blandford, Tennison, and Scott. 2019. *Data Trusts: Lessons from Three Pilots*. Open Data Institute.
141 MaRS, "Technical Architecture Options," *A Primer on Civic Digital Trusts*, accessed September 19, 2019.
142 MaRS, "Business Model Options," *A Primer on Civic Digital Trusts*, accessed September 19, 2019.
143 Hardinges, Wells, Blandford, Tennison, and Scott. 2019. *Data Trusts: Lessons from Three Pilots*. Open Data Institute.

144 World Economic Forum and McKinsey & Company, *Data Collaboration for the Common Good.*
145 MaRS, "Technical Architecture Options," *A Primer on Civic Digital Trusts*, accessed September 19, 2019.
146 Hardinges, Wells, Blandford, Tennison, and Scott. 2019. *Data Trusts: Lessons from Three Pilots*. Open Data Institute.
147 MaRS, "Technical Architecture Options," *A Primer on Civic Digital Trusts*, accessed September 19, 2019.
148 MaRS, "Technical Architecture Options," *A Primer on Civic Digital Trusts*, accessed September 19, 2019.
149 World Economic Forum and McKinsey & Company. April 2019. *Data Collaboration for the Common Good.*
150 Open Data Institute "Applying Blockchain Technology in Global Data Infrastructure," accessed September 19, 2019.

Technical infrastructure for responsible data use is an active area of research and practice. University of Toronto scholar Lisa Austin's research proposes the development of "safe-sharing sites," which would enable personal and sensitive data sharing through a controlled environment that allows computational activity but does not permit anything but the computational results to leave the site.[151] The safe-sharing-sites approach is an alternative to different anonymization or de-identification techniques to protect the privacy of data subjects. With a similar purpose, Google and other organizations use differential privacy tools to enable researchers to utilize datasets with sensitive data.[152] Differential privacy is a statistical technique from the field of cryptology that adds "noise" to a dataset to prohibit the identification of individuals or sources.[153,154] Google recently released their privacy tools to the public on GitHub to promote broader use and benefit.[155]

[151] Lisa M. Austin and David Lie, "Safe Sharing Sites," *New York University Law Review*, forthcoming, authored February 5, 2019.
[152] Nick Statt, "Google Is Open-Sourcing a Tool for Data Scientists to Help Protect Private Information," *The Verge*, September 5, 2019.
[153] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith, "Calibrating Noise to Sensitivity in Private Data Analysis," 2006.
[154] Joshua Snoke and Claire McKay Bowen, "Differential Privacy: What Is It?," *AMSTATNews*, March 1, 2019.
[155] "Differential Privacy Documentation," GitHub, accessed September 19, 2019.

These are just two examples in a rapidly expanding field of new tools and mechanisms that enable data sharing.

4.5.4 Inclusive and participatory practices

In many places, there is a burgeoning expectation that processes to create new systems, places, and digital tools will be not only consultative but also participatory with transparency and feedback loops built in. Cities are working with a range of stakeholders to go beyond access to digital infrastructure and services to build inclusive digital participation.

4.5.4.1 Digital inclusion

Worldwide, there are efforts to build digital literacy as a foundation to engage whole communities. The U.S.-based National Digital Inclusion Alliance (NDIA) defines digital inclusion as "the activities necessary to ensure that all individuals and communities, including the most disadvantaged, have access to and use of Information and Communication Technologies."[156] It includes:

- Affordable, robust broadband internet service.
- Internet-enabled devices that meet the needs of the user.

[156] "Definitions," National Digital Inclusion Alliance (NDIA) website, accessed September 19, 2019.

- Access to digital literacy training.
- Quality technical support.
- Applications and online content designed to enable and encourage self-sufficiency, participation, and collaboration.[157]

Initiatives to advance digital inclusion exist across all sectors. The Government of Canada recently announced the Digital Literacy Exchange Program, which will provide $29.5 million in funding to local non-profits over five years to teach fundamental computer, mobile, and online skills to individuals currently left out of the digital economy.[158] Other federal initiatives like CanCode and PromoScience offer digital skills through primary education.

The Brookfield Institute for Innovation and Entrepreneurship, a research institute at Ryerson University, is engaged in a multi-year project examining digital literacy in Canada. Their June 2018 report, "Levelling Up," provides extensive analysis of digital education programs across the country, looking at all levels of formal education as well as informal offerings, including boot camps,workshops, community programs, employer-provided courses, online courses, and programs targeting underrepresented and marginalized communities.[159]

[157] "Definitions," National Digital Inclusion Alliance (NDIA) website.Definitions

[158] "Digital Literacy Exchange Program," Government of Canada websiteDefinitions, accessed September 19, 2019.

[159] Annalise Huynh and Nisa Malli, *Levelling Up: The Quest for Digital Literacy*, Brookfield Institute, 2018.

Among their conclusions calling for consistent funding and rigorous evaluation of programs to create best practices, they emphasized the need for collective action from policy-makers, educators, and employers.

The civic tech community plays a unique role in advancing digital inclusion and participation by bridging government and communities.[160] Across the world, civic tech organizations (such as Code for All and Code for America Brigade) partner with government agencies to improve digital public services and tools through better resident engagement. They also support community action through skill building, providing education and trainings (such as Digital Government and Civic Tech), tools (such as "Civic Tech Field Guide" and "Civic Tech Community Organizer Toolkit"), and forums for participation (such as Civic Hall, Civic Hall Toronto, Civic Tech Toronto, NYC School of Data, and City Tech Collaborative).

Emerging from the civic tech community, an encouraging approach to greater access for diverse residents to participate in technology design and mitigate biases is what are known as "Civic User Testing Groups." One of the earliest and most successful of these is the CUTgroup in Chicago. Blue Ridge Labs at the Robinhood Foundation in New York City has also adapted this model to create Design Insight Group (DIG).

[160] Derek Poppert, "Navigating the field of civic tech", Medium, August 16, 2018.

Locally, Code for Canada founded GRIT (Gathering Residents to Improve Technology), a usability testing service connecting technology creators with diverse and underrepresented communities in the city. The GRIT program meets people of all digital skill levels, cultures, ages, and backgrounds where they are — in community spaces outside of working hours, for instance — and incorporates their feedback into the creation of new digital services and products, helping to ensure these tools reflect the needs of the populations they are intended to support.[161] Launched in late 2018 with funding support from Sidewalk Labs, the GRIT Toronto pilot has recruited over 350 residents from Toronto's 25 wards, representing a diversity of backgrounds, lived experiences, and technical skill levels.

4.5.4.2 Emerging participatory approaches

City governments and nonprofits are facilitating participatory processes to bring communities together to develop new policies, programs, and places that are "of" and "by" the community, rather than "for" the community. They are using new engagement methods to create more resident-aligned policies and programs, achieve greater use of public services, and reach a wider spectrum of residents.

The City of Bologna recently launched the Civic Imagination Office, which was designed specifically to build greater participation through regulation, city-wide engagement labs, and digital tools. The city passed a regulation to streamline civic engagement, which allows residents and private organizations to sign collaboration pacts with the city in order to improve public space. Bologna also created labs in the city's six districts that serve as hubs of innovation and collaboration with residents. City officials report a marked increase in citizen engagement — approximately 480 collaboration pacts have been implemented to date, and more than 14,000 people voted in the first year of participatory budgeting.[162]

The Civic Imagination Office is led out of the Fondazione Innovazione Urbana, a joint endeavour between the municipal government and the University of Bologna.

In the London borough of Barking and Dagenham, the local charity Participatory City Foundation started the Every One Every Day initiative, which aims to "create the first large scale fully inclusive, practical participatory ecosystem."[163] Started in November 2017, Every One Every Day is a series of hands-on practical projects designed by residents to directly benefit residents. Projects include things like sharing skills, spaces, and resources; working and playing together; batch cooking and community meals; growing food and planting trees; and

[161] Marisa Bernstein, "GRIT Toronto: Putting the 'Us' in Usability Testing," *Medium,* February 5, 2019.

[162] Cities of Service and City of Bologna, Italy, "Co-creating Urban Commons," 2018.

[163] Participatory City Foundation, *Made to Measure: Building a Participatory Ecosystem in Barking and Dagenham Through the Every One Every Day Initiative*, October 24, 2018.

trading, making, and repairing goods.[164] The program operates four "high street", which are known as the primary streets for business, shops and a warehouse, which are used as core spaces to gather and program events and projects.

The program uses design principles to encourage inclusive participation. The principles lead to projects that are welcoming and inclusive; low commitment; open to beginners and experts; 100 percent free of stigma; close to home; easy and practical; zero or low cost; many and varied in their activities; built with everyone in mind; and have immediate and accumulative benefits.[165] Over the first 18 months, over 5,000 people worked on more than 100 projects.[166]

There are many different ways that civic participation is unlocked. One promising approach involves leveraging technology to bring transparency into processes and decision points, which could allow community members to better understand the issues at hand, provide input, and feel satisfied that their voices have been heard. While digital tools hold great potential, they also risk engaging only those people who are already engaged and have the time and skills to participate.

The following digital tools provide a small sample of the many available tools for participation:

- The City of Barcelona is at the forefront of the digital participation trend, having created Decidim, a free, open-source digital tool inspired by social media that keeps residents up-to-date on processes and garners their input. The digital tool supports activities like strategic planning, participatory budgeting, and public consultations through allowing users to create proposals, vote, view results, convene and organize, and receive notifications.

  Decidim goes beyond providing a digital platform: it's an infrastructure involving code, documentation, design, training courses, a legal framework, collaborative interfaces, user and facilitation communities, and a common vision, including a social contract centred on transparency, sharing, and participation.[167] Today more than 35 cities use Decidim, as do dozens of regions and organizations.[168]

- Some community-based efforts have started creating their own tools, such as YouthScore, which allows youth to rate their neighborhoods based on their youth

[164] "About," Every One Every Day Project website, accessed September 19, 2019.
[165] "Everyday Projects," Participatory City Foundation website, accessed September 19, 2019.
[166] "Everyday Projects," Participatory City Foundation website, accessed September 19, 2019.

[167] "Decidim: A Brief Overview," *Decidim: Political and Technopolitical Networks for Participatory Democracy*, Decidim Docs, accessed September 19, 2019.
[168] "These Cities, Regions and Organizations Are Already Using Decidim," Decidim website, accessed September 19, 2019.

friendliness. The tool was developed by youth for youth and promotes the voice of a population not typically involved in public decision-making. It also builds skills in civic participation. The tool has been used in neighbourhoods in Toronto and in Frankfurt, Germany.[169]

- Startups are creating digital participation tools. For example, Neighborland offers a customizable platform for engagement between city planners and communities. It enables organizations to publish proposals, collect and publish stakeholder feedback, and provide discussion forums and moderate stakeholder engagement. Supporting a range of urban, strategic, and capital planning projects, the tool aims to empower residents to shape the development of their communities. Neighborland reports that organizations using the tool reach participation levels 10 to 100 times greater than conventional outreach methods.[170]

4.5.5 Digital identity to improve protection and control

As governments are increasingly using digital methods to expand access to public services and reach all members of society, they are exploring promising new approaches that provide residents greater privacy protection and control over their personal data. Digital IDs are electronic-based verified identities, akin to physical IDs like drivers licences or passports, that allow individuals to identify themselves to access services. With the rise of digital options, there is also a rise in the number of accounts, cards, and passwords people must manage. Digital IDs have the potential to be used across institutional boundaries, providing users the ease of a single verified identity across social services, transit, dining, and recreation.

Digital IDs could provide users control over their information. Currently, personal data is sprinkled across all the digital services one accesses. Digital IDs could make it possible for personal data to be in the possession and control of individual users, providing transparency into and management over how one's personal information is collected, used, and shared across different digital service providers. Traditionally, sharing one's identity has been an all-or-nothing system. Digital IDs could give users selective disclosure to share only what they want with whom they trust. While a Digital ID system with all these features doesn't yet exist, there are coalitions in place advancing the partnerships and technology to make it a reality in the coming years.

---

[169] "Youthscore," Maximum City website, accessed September 19, 2019.
[170] Neighborland, "The Neighborland Handbook," *Medium,* accessed September 19, 2019.

Identity is a human rights issue. Article 6 of the UN's 1948 Universal Declaration of Human Rights stipulates that, "Everyone has the right to recognition everywhere before the law."[171] And increasingly, governments are seeing identity as foundational for "political, economic and social opportunity."[172] Digital IDs are being advanced by governments around the world.

The ID2020 Alliance is a leading voice in advancing digital identity with governments and their partners. It is a public-private partnership that not only advocates for digital IDs, but also funds implementations, convenes stakeholders, and defines technical requirements for development.[173] ID2020 outlines four requirements for digital identity:

1. **Private:** Only you control your identity, what data is shared, and with whom.
2. **Portable:** Accessible anywhere you happen to be through multiple methods.
3. **Persistent:** From birth to death.
4. **Personal:** Unique to you.[174]

171 "The Need for Good Digital ID Is Universal," ID2020 website, accessed September 19, 2019.
172 ID2020, "ID2020: At a Glance," accessed September 19, 2019.
173 "We Need to Get Digital ID Right," ID2020 website, accessed September 19, 2019.
174 "The Need for Good Digital ID Is Universal," ID2020 website.

4.5.5.1 Global precedents

Countries like Estonia and India have instituted national digital IDs. In 2002, Estonia became a pioneer of digital ID, creating a full ecosystem of digital government (see case study for greater detail). India created a digital ID system, Aadhaar, in 2009.[175] In both these cases, government action was critical to digital ID creation and widespread adoption. Specifically, government provided legislation to legitimize and regulate IDs, a framework to unite cross-sector actors implementing IDs, and digital infrastructure as a foundation for the ID systems.[176] Each country had its own technical approach to digital IDs and related digital infrastructure, leading to different risks and results.

Cities are an emerging site for advancing individual control over digital identity. Both Amsterdam and Barcelona are working with DECODE (Decentralized Citizen Owned Data Ecosystems), a UN-funded project, to create and pilot new technologies and tools that facilitate user control over storing, managing, and use of personal data.

- In Amsterdam, DECODE is piloting two projects — one a digital registry and the other a neighbourhood-based social network. The digital registry project will provide

175 Alfred Ng, "UN Wants a Universal Digital ID for Your Data," *Cnet*, June 20, 2017.
176 "Canada's Digital ID Future: A Federated Approach" (white paper, Canadian Bankers Association, May 30, 2018).

the digital infrastructure to give residents access to data stored in municipal databases and allow them to select pieces of that information to share in other contexts.[177] The GebiedOnline social network pilot will test new verifications for logging into the platform, providing more security and privacy that the current email and password or Facebook verification methods.[178]

- In Barcelona, one pilot project will modify Barcelona's digital participation tool Decidim to allow users to use the tool and sign bills anonymously, while still having a verified identity. It will also give Decidim users more control over their data and allow them to share select information on the city's public dashboard BCNow (BarcelonaNow). The second pilot will enable residents to share environmental data (such as noise levels and air quality) collected from sensors in their homes anonymously with the city.[179]

4.5.5.2 Multi-sector collaboration across Canada

There is growing momentum for digital identity across Canada. The 2010–12 Task Force for the Payments System Review, set up by the Canadian minister of finance to explore

[177] "Pilots," DECODE website, accessed September 19, 2019.
[178] "Pilots," DECODE website.
[179] "Pilots," DECODE website.

digital payments and the digital economy, paved the way for multi-sector collaboration. The subsequent Digital ID & Authentication Council of Canada (DIACC), a non-profit member-based coalition of public- and private-sector organizations working on digital identity and authentication, is a driver of the development of digital ID today.

DIACC is responsible for setting the strategic direction for digital identity for all sectors in Canada. Through the Pan-Canadian Trust Framework, DIACC aims to bring together the standardized technologies and policy processes required to enable trustworthy digital transactions and support an inclusive digital economy. The guiding principles propose to create a digital identity ecosystem that:

1. Is robust, secure, and scalable.
2. Implements, protects, and enhances privacy by design.
3. Is inclusive, open, and meets broad stakeholder needs.
4. Is transparent in governance and operation.
5. Provides Canadians choice, control, and convenience.
6. Is built on open, standards-based protocols
7. Is interoperable with international standards
8. Is cost effective and open to competitive market forces.
9. Is able to be independently assessed, audited, and subject to enforcement.
10. Minimizes data transfer between authoritative sources and will not create new identity databases.[180]

[180] Digital ID & Authentication Council of Canada Trust Framework Expert Committee, "Pan-Canadian Trust

The draft framework was publicly released in February 2019. Supporting documents regarding components like notice, consent, and privacy continue to be developed and released.

Several other initiatives are tied to the Pan-Canadian Trust Framework. The Framework is the foundation to ensure that all organizations and jurisdictions in Canada agree to common rules of trust and is spurring initiatives at the national and provincial levels. For example:

- SignIn Canada is the federal government initiative leveraging digital identity to achieve a "tell us once" policy for government services.[181] It is scheduled to launch in fall 2019.
- The Ontario Ministry of Government and Consumer Services' ServiceOntario is working with Bluink, an identity management platform, to develop a digital ID as an alternative to the Ontario driver's license and health card.[182]
- Alberta Credential Ecosystems is a newly announced digital identity initiative set to pilot new solutions. It is led by ATB Financial, a crown corporation owned by the province, in partnership with the cities of Calgary and Edmonton, local universities, telecoms, health providers, and decentralized ID services providers.
- In a parallel effort, the Verifiable Organizations Network creates open source platforms that enable businesses to partner with government more quickly through providing verification of business identity and credentials. Both Ontario and British Columbia use the technology in their Verifiable Businesses and OrgBook BC, respectively.

There is also strong leadership for digital identity across industry. Banking and finance organizations (such as the Canadian Bankers Association) have long been key drivers of policy conversations and are continuing to advance the industry with technology partners. Verified.Me from SecureKey Technologies provides customers of several banks, including CIBC, Desjardins, RBC, Scotiabank, and TD, with a new way to verify their identity and enhance privacy and control.[183] Interac is providing digital identity services for individuals interacting with the health industry, facilitating ease and protection with prescriptions, payments, and medical records.[184]

Framework Model 3 Draft Recommendation V1.0,", June 3, 2019.

[181] Ken McMillan, *Canadian Digital Identity* (Treasury Board of Canada, prepared for the 2018 International Identity Summit, Seattle, Washington), 2018.

[182] Rose Behar, "Ontario Is Developing a Mobile ID Card Solution with Ottawa-Based Bluink," *mobilesyrup,* November 14, 2017.

[183] Verified.Me website homepage, accessed September 19, 2019.

[184] "Digital Identity in Health Insights from Interac Corp.," (white paper, Interac Corp., September 2018).

4.5.6 Agile and open-technology practices

Cities are looking to create flexible, interoperable digital systems that enable collaboration and continuous improvement. This aspiration has propelled the adoption of open source policies, which require the use of open source software and standards in public digital infrastructure, across governments worldwide.[185] By implementing open source software, cities gain flexibility and savings as they are able to address their changing needs without additional costs or reliance on vendors. Cities like Barcelona and Amsterdam also position open source software as a tool for participation and community involvement — a way to enhance digital sovereignty.

4.5.6.1 Open standards

With the growth of digital infrastructure and data, open standards are essential to data sharing and generating public benefit from digital technologies. Open standards increase interoperability, improve the quality and comparability of data, and enable better aggregation of data and linkability of data, all of which are important to cities and organizations providing public services.[186] To assist governments and organizations in adopting, using, and creating open standards, the Open Data Institute (ODI), in partnership with W3C, OpenNorth, Porism, and Open Data Services, developed the "Open Standards for Data" guidebook.[187] The guidebook highlights a wide range of economic, social, and technological benefits made possible through the use of open standards. For example, new commercial ecosystems are encouraged by the reduced barrier to entry in combining data within a sector (Generalized Transit Feed Specification and Google Maps), or new tools and services are developed because of the consistently formatted and published data (such as the Building and Land Development Specification; the Boulder County Land Use information platform, in Colorado; Accela; and the Socrata data platform).[188, 189] Furthermore, the Open North report "Identifying Recommended Standards and Best Practices for Open Data" highlights that domain-specific data standards are important in generating widespread adoption of open data use.[190]

---

185 James Andrew Lewis, "Government Open Source Policies," Center for Strategic & International Studies (CSIS), April 16, 2010.

186 Open Data Institute, "Introduction," Open Standards for Data online guide, accessed September 19, 2019.
187 "Documenting the Development of Open Standards for Data," Open Data Institute, accessed September 19, 2019.
188 Open Data Institute, "Introduction," Open Standards for Data online guide.
189 Open Data Institute, "Economic impacts of open standards," Open Standards for Data online guide, accessed September 19, 2019.
190 Stéphane Guidoin, Paulina Marczak, Juan Pane, and James McKinney, *Identifying Recommended Standards and Best Practices for Open Data*, OpenNorth, 2015.

Data standards for urban digital infrastructures are not centralized through any single standards body, like W3C for the World Wide Web or the Institute of Electrical and Electronics Engineers (IEEE) for physical connectivity. Instead Sidewalk Labs sees several efforts to create directories to help find and identify relevant standards for cities and their partners. A few examples include:

- "Civic Open Data Standards," published by Azavea, an open source geospatial data services and products firm, includes open standards that are location based and focused on cities.
- The Open Data Standards Directory created by GovEx and GeoThink covers a wide range of topics related to government and civic society.
- "Tools to Find Open Standards" in the ODI guidebook acts as a sort of metadirectory for other resources.
- The World Council on City Data implements ISO 37120 Sustainable Development of Communities: Indicators for City Services and Quality of Life – a new international standard for urban metrics.

Additionally, the Open Group is a member organization that brings together stakeholders to create standards, establish requirements and policies, and share best practices for open, vendor-neutral technology standards and certifications.[191] It also provides a library of standards, guides, and published research on data standards.

[191] "The Open Group: Making Standards Work," Open Group website, accessed September 19, 2019.

Cities are also creating their own open standards and standards bodies. Last year, the Los Angeles Department of Transportation created the Mobility Data Specification to actively manage dockless scooters, bikes, taxis, and buses and public right-of-way. Through APIs, mobility service providers share real-time information about vehicles, and the city shares parking information. Building from this, 15 cities joined together to form their own standards body for urban mobility.[192] Established in June of this year, the Open Mobility Foundation creates a governance structure for open urban mobility software and tools.

4.5.6.2 Procurement innovation

This movement towards open source technologies and standards encourages an emerging shift in procurement strategies within governments. Organizations are increasingly recognizing that current practices in scoping and awarding technology projects do not support adaptable digital infrastructure and technology. As New America outlines, typical technology procurement practices result in huge scopes with lengthy requirements that only a few companies have the scale and experience, and qualifications to handle.[193]

[192] Seleta Reynolds, "What the Open Mobility Foundation Says About Cities, Software, and Standards," *Forbes*, July 18, 2019.
[193] Sara Hudson and Hana Schank, *Getting the Work Done: What Government Innovation Really Looks Like* (Washington, D.C.: New America, 2018).

This can lead to a lack of diversity among technology vendors — or worse, a sort of monopoly — as well as increased risk for creating outdated technologies. Modular procurement is a strategy to address such issues. By creating shorter, more tightly scoped contracts for interoperable technologies, modular procurement increases the diversity of vendors and their ability to adapt to emerging technologies while reducing the risk of contract failure.[194]

Organizations like 18F, the U.S. government's digital service, and Code for America, a non-profit partner for state and city governments, are leading voices in the movement towards modular contracts for open technologies. One early example is from the State of California, in which the state, in partnership with 18F and Code for America, took a 1,500-page request for proposal (RFP) three years in the making and broke it into multiple, separate modules described by a 10-page scope of work. As a result, the project ended up with more and new vendors bidding.[195] 18F has also introduced similar agile and modular approaches to technology procurement in the states of Alaska, Mississippi, and Ohio.[196, 197, 198]

[194] Robin Carnahan, Randy Hart, and Waldo Jaquith, *De-risking Custom Technology Projects*, 18F, Technology Transformation Service, General Services Administration, August 5, 2019.
[195] Andre Francisco and V. David Zvenyach, "From 1,500 pages to 10: Helping California Buy a New Child Welfare System," 18F blog, March 22, 2016.
[196] Alaska Department of Health and Social Services (DHSS), "EIS Modernization Project," GitHub, last updated August 7, 2019.

In Ontario, the multi-city joint effort Municipal Innovation Exchange (MIX) is using procurement as a tool to build innovation capacity and explore complex municipal challenges. MIX is led by the City of Guelph, in partnership with the City of London, City of Barrie, and the MaRS Discovery District. The effort is structured such that each city will run an innovation procurement challenge, explore the potential for multi-city challenges, and enable the sharing of best practices between municipalities.

4.5.7 The need for cross-sector collaboration

There are many practices in Canada and from around the world that show promising paths for addressing critical issues in smart cities. What is striking is how nearly all initiatives require cross-sector collaboration, bringing together the public sector, the private sector, academia, and civil society. There is no single solution out there, but rather diverse approaches that can be taken for inspiration.

In recognition of the need for coordination among the multitude of global smart city digital governance initiatives

[197] Greg Boone and Zac Cohn, "Mississippi Brings Agile and Modular Techniques to Child Welfare System Contract," 18F blog, September 20, 2016.
[198] Eyragon Eidam, "Ohio Takes Page from 18F to Launch Inclusive Procurement, Attract New Bidders," *Government Technology,* December 9, 2016.

and stakeholders, the G20 Global Smart Cities Alliance was created to provide a platform for city leaders to share best practices and establish global standards, identify governance gaps, and develop new policies for the responsible and ethical use of smart city technologies through multi-sector collaboration. The Alliance seeks to advance a policy framework that aims to accelerate best practices, mitigate potential risks, and foster greater openness and public trust.

4.6 Digital innovation precedents from Canada and around the world

The following case studies demonstrate approaches to opportunities and challenges common in integrating digital technologies and city building, providing inspiring precedents for responsible smart city development. The studies include examples from Europe, including Estonia, considered to be the "most advanced digital society in the world";[199] Amsterdam, a leader in responsible sharing and use of data; and Barcelona, with a robust participatory, open approach to governing and technology. Chicago and New York City present examples of data-driven city governments in the United States, both of which have invested in digital infrastructure and developed digital policies. And in Canada, we look at Montreal, a winner of the 2019 Canadian Smart Cities Challenge and a leader in responsible use of artificial intelligence.

[199] Ben Hammersley, "Concerned About Brexit? Why Not Become an e-Resident of Estonia," *Wired,* March 27, 2017.

4.6.1 Estonia

The Baltic country of Estonia is a global leader in digital government. Estonia provides 99 percent of public services online.[200] In 2005, it became the first country in the world to hold national elections online.[201] It was also the first country to use blockchain technology nationally.[202] And in 2017, the World Economic Forum ranked Estonia as the most entrepreneurial country in Europe.[203]

Started as a government initiative after the country regained its independence in the 1990s, "e-Estonia" is the digital government ecosystem Estonia built through a digital infrastructure called X-Road (more recently called X-tee) and a national digital ID. Together, these two features have enabled Estonia to provide nearly all government services online, ranging from health (such as prescriptions and medical records) and education (such as report cards) to business and finance (such as tax filings, banking, and business licences).[204] Estonia estimates that the digital

[200] *e-Estonia guide*, e-Estonia, accessed September 29, 2019.
[201] *e-Estonia guide*.
[202] *e-Estonia guide*.
[203] Alex Gray, "Europe's Most Entrepreneurial Country? It's Not the One You Might Expect," *World Economic Forum,* March 16, 2017.
[204] Rainer Kattel and Ines Mergel, "Is Estonia the Silicon Valley of Digital Government?," *Medium,* September 28, 2018.

infrastructure delivers annual savings of 2 percent of the GDP by delivering time savings to the public and private sector.[205]

4.6.1.1 X-Road

X-Road is a data exchange platform that facilitates secure access to and sharing of data from different distributed databases to provide government services. Designed as a distributed system in part because the government did not have the financial resources to build a unified system, the approach allows for each government agency to build IT systems and databases to fit its needs.[206] X-Road is the software that Estonia designed to connect these independent systems regardless of software or architecture.[207] It allows data to be stored where it is created and does not duplicate data while providing secure access or information sharing.[208]

Estonia publishes real-time stats on X-Road data use and requests for data (over 2,700 services use X-Road and there have been over 5 billion requests to date), lists security technologies (XAdES, ASiC, and more), and tracks time savings attributed to X-Road (1,407 working hours last year) on a public website. It also provides a visualization of data exchange networks.

X-Road is used by governments as well as by the private sector, such as banking, which provides direct services to consumers and needs to verify identity and information. Currently 150 public-sector institutions and nearly 500 institutions and enterprises use X-Road in Estonia.[209] Other governments, including Finland, Kyrgyzstan, the Faroe Islands, Iceland, and Japan have adopted this approach to digital services and are using X-Road technology.[210]

4.6.1.2 Digital ID (or e-Identity)

Estonia requires residents to hold state-issued digital IDs. The digital ID is critical in the e-governance ecosystem because it is what authenticates an individual's identity, issues a digital signature, and allows access to government services like submitting tax claims or paying a parking ticket. It can also be used to verify identity when logging into bank accounts or medical records, filling prescriptions, travelling (as a legal ID), and collecting customer loyalty rewards with different

[205] *e-Estonia guide*.
[206] Kattel and Mergel, "Estonia's Digital Transformation: Mission Mystique and the Hiding Hand" (UCL Institute for Innovation and Public Purpose Working Paper Series, 2018).
[207] "Data Exchange Layer X-tee," Republic of Estonia: Information System Authority website, accessed September 19, 2019.
[208] "Interoperability Services," e-Estonia website, accessed September 19, 2019.
[209] "Requests This Month," X-tee website, accessed September 19, 2019.
[210] "Interoperability Services," e-Estonia website.

businesses.[211] Digital ID holders can also see a record of all of their authentication and digital signatures online.[212]

The digital IDs are issued in two forms — an ID-card or a mobile-ID. The ID-card is a physical photo ID with an embedded chip. Individuals have two pin codes: one that is part of the encryption process and one that issues a digital signature.[213] Nearly all Estonians – 98 percent — have ID-cards, and 67 percent use them regularly.[214] The government estimates that five days per year are saved through the use of digital signatures.[215] The mobile-ID functions the same as the ID-card, but replaces the physical card with a mobile phone (with sim card technology) and serves as a secure digital ID.

X-Road and e-identity, like the rest of e-Estonia initiatives, are based on the following design and governance principles:

- **Decentralization**, which allows every government department, service provider, and business to use its own IT system.
- **Interconnectivity** using secure interoperability across systems.

[211] "Areas of Use," ID website, accessed September 19, 2019.
[212] "My ID-card Activities," ID website, accessed September 19, 2019.
[213] Nathan Heller, "Estonia, The Digital Republic," *New Yorker,* December 18 & 25, 2017.
[214] "e-Identity," e-Estonia website, accessed September 19, 2019.
[215] "e-Identity," e-Estonia website.

- **Integrity** in data storage and exchange.
- **Open platform** and open source.
- **No legacy** through continuous improvement.
- **Only once,** where residents and businesses provide information only once to government.
- **Transparency** for residents into the use of their personal information.[216]

These principles, along with strong government leadership and a partnership with technologists in Estonia and Scandinavia, have created a strong culture for digital transformation. Several years into Estonia's digital governance movement, these remain principles, not laws or regulations.[217]

4.6.1.3 Continuous innovation

Estonia continues to grow and evolve its digital offerings. In 2014, Estonia launched e-Residency, which allows anyone in the world to apply for digital identity in Estonia and gain access to the Estonia digital services, like creating and managing a business. The government believes that providing easy access to digital services — a business can be incorporated in only three hours — will attract innovation and grow the economy.[218] Currently, over 50,000 people from

[216] *e-Estonia guide*.
[217] Kattel and Mergel, "Estonia's Digital Transformation: Mission Mystique and the Hiding Hand."
[218] "Business and Finance," e-Estonia website, accessed September 19, 2019.

more than 165 countries have applied and started 6,000 new business.[219]

Estonia recently launched a data embassy. The data embassy is an emerging concept for a data centre located outside of Estonia's territorial boundaries but that is under the control and ownership of the Estonian state.[220] It is one approach to security and safety, which Estonia has developed rapidly since a 2007 distributed denial of service cyberattack that shut down digital service delivery for four weeks.[221] Using the Estonian government's cloud and blockchain technologies, the data embassy would serve as a backup data record and could provide operations for critical services in a crisis.[222] Estonia signed an agreement for the first data embassy with Luxembourg in 2017.

4.6.2 Montreal

Like Toronto, Montreal has a strong technology sector spanning academia and industry. Montreal is a key location in the Government of Canada's Pan-Canadian Artificial Intelligence Strategy, is one of five of Canada's innovation superclusters, and was a winner of the 2019 national Smart Cities Challenge. Propelled by these government investments, Montreal continues to advance technological innovations as well as address their impact.

4.6.2.1 Artificial intelligence

Montreal is a hub for artificial intelligence (AI). It is one of three cities that have newly created AI institutes funded through the Canadian Institute for Advanced Research's $125 million Pan-Canadian Artificial Intelligence Strategy to support and expand research and thought leadership on AI. These include the Alberta Machine Intelligence Institute in Edmonton, the Vector Institute in Toronto, and the Montreal Institute for Learning Algorithms, which are all rooted in strong research universities.

Montreal is also one of five innovation superclusters in Canada, receiving $230 million in funding from the Government of Canada, $53 million from the Government of Quebec, and matching funds from the private sector to create the AI-powered supply chain supercluster (SCALE.AI), foster faster adoption of AI, and boost economic development. Montréal International, the greater Montreal economic development agency, reports that over $2 billion

---

[219] Kaspar Korjus, "Estonian President Kersti Kaljulaid Reveals the Future Direction of e-Residency," *Medium,* December 18, 2018.
[220] "Data Embassy," e-Estonia website, accessed September 19, 2019.
[221] Kattel and Mergel, "Is Estonia the Silicon Valley of Digital Government?" *Medium,* September 28, 2018.
[222] "Data Embassy," e-Estonia website.

has been invested in AI in Montreal since 2016.[223] While these examples do not provide a comprehensive list of AI initiatives or actors in Montreal, it suggests the strength of the technology ecosystem and scale of investment into AI in Montreal.

While advancing the development and deployment of technology, Montreal is also leading action in the ethics of AI. The city is home to the Montreal AI Ethics Institute, whose mission is to help define humanity's place in a world increasingly characterized and driven by algorithms, through creating tangible and applied technical and policy research on the ethical, safe, and inclusive development of AI. The institute takes a practical and applied approach to AI ethics. The institute also offers two global fellowship programs: a short-term summer fellowship and a longer-term one-year fellowship.

Led by the University of Montreal, and developed with a wide range of stakeholders, the 2018 Montreal Declaration for the Responsible Development of Artificial Intelligence offers ethical principles for the development of AI. The declaration has three main objectives:

- Propose a framework for ethical development and deployment of AI;
- Guide the field of digital innovation towards inclusive, public benefit; and
- Create a forum for national and international discussion.[224]

It calls on anyone, but especially political representatives, to contribute to the evolving conversation.

The framework includes the following 10 principles to advance the interests of individuals and groups, regarding the development of digital technologies, including AI:

1. **Well-being:** The development and use of artificial-intelligence systems (AIS) must permit the growth of the well-being of all sentient beings.
2. **Respect for autonomy:** AIS must be developed and used with respect for people's autonomy, and with the goal of increasing people's control over their lives and their surroundings.
3. **Protection of privacy and intimacy:** Privacy and intimacy must be protected from intrusion by AIS and by data-acquisition and archiving systems.
4. **Solidarity:** The development of AIS must be compatible with maintaining the bonds of solidarity among people and generations.
5. **Democratic participation:** AIS must meet intelligibility, justifiability, and accessibility criteria, and must be subjected to democratic scrutiny, debate, and control.

223 "Montréal: Artificial intelligence Serving the Common Good," Montréal International website, accessed September 19, 2019.

224 "The Declaration for responsible AI development," Montréal Declaration Responsible AI website, accessed September 19, 2019.

6. **Equity:** The development and use of AIS must contribute to the creation of a just and equitable society.
7. **Diversity inclusion:** The development and use of AIS must be compatible with maintaining social and cultural diversity, and must not restrict the scope of lifestyle choices and personal experience.
8. **Prudence:** Every person involved in AIS development must exercise caution by anticipating, as far as possible, the potential adverse consequences of AIS use and by taking appropriate measures to avoid them.
9. **Responsibility:** The development and use of AIS must not contribute to diminishing the responsibility of human beings when decisions must be made.
10. **Sustainable development:** The development and use of AIS must be carried out so as to ensure the strong environmental sustainability of the planet.[225]

The declaration reflects a year of consultation and research with a wide range of stakeholders, including residents, experts, policy-makers, industry, civil society, and professional organizations, much of which is also documented in the reports of the Montreal declaration. One report outlines the following eight recommendations for integrating the ethical principles into digital innovation:

1. **Establish an organization for independent citizen scrutiny and consultation** dedicated to the examination of and research into the uses and social impacts of digital technology and AI.
2. **Institute a coherent AIS audit and certification policy** that promotes responsible deployment should be instituted.
3. **Support the empowerment of citizens** in the face of digital technologies, in the form of access to education that enables understanding, critical thinking, respect, and accountability, so as to promote active participation in a sustainable digital society.
4. **Invest in education, ethics, and multidisciplinarity** to benefit stakeholders concerned with the design, development, and use of AIS.
5. **Promote the inclusive development of AI** with a coherent strategy that makes use of various existing institutional resources and preventing potential biases and discrimination related to the development and deployment of AIS.
6. **Protect democracy** by using a containment strategy to prevent the manipulation of information for political ends and the deception and political manipulation of citizens via malicious social platforms and websites, along with a strategy to combat political profiling, so as to maintain the conditions for healthy functioning democratic institutions and informed citizens.
7. **Adopt a non-predatory model of international development** that aims to include the various regions of the globe without abusing low- and middle-income countries.

[225] "The Declaration for responsible AI development," Montréal Declaration Responsible AI website.

8. **Protect the environment** by implementing a public-private strategy to ensure that development and deployment of AIS and other digital technologies are compatible with robust environmental sustainability and conducive to the advancement of solutions to the environmental crisis.[226]

4.6.2.2 Smart cities winner

The City of Montreal was the $50 million winner of the Government of Canada's Smart Cities Challenge, which asked communities to "adopt a smart cities approach to improve the lives of their residents through innovation, data and connected technology."[227] The city proposed a range of related initiatives to enhance neighbourhood life and promote collective action, including an integrated mobility project, a food infrastructure project, and a civic innovation lab.

Focusing specifically on the integrated mobility project, Montreal proposes to combine multiple modes of currently available travel with a single mobility account and simplified fare integration, and expand short-distance travel options with the addition of a neighbourhood fleet of self-driving vehicles.[228] To accomplish this, Montreal proposes to create a metropolitan integrated mobility centre, an open platform that incorporates:

- A customer mobility account that includes a digital ID and allows for invoicing, payment, and loyalty programs;
- A service portal, including a trip-planning tool and a digital ticketing program;
- A mobility data hub and applications, with bidirectional sharing of data between all greater Montreal transit operators; and,
- A new governance and partnership model.[229]

The concept for a customer mobility account, or digital ID, dovetails with broader initiatives on digital identification in which the city is involved. These include work like the Pan-Canadian Trust Framework, which addresses compatibility between national and local IDs, and the digital services and identity committee of the Quebec municipal computer network, which focuses on data architecture for

226 "The Montreal Declaration for the Responsible Development of Artificial Intelligence Launched," Canada-ASEAN Business Council website, accessed September 19, 2019. See also, Montreal Declaration Responsible AI, "Part 6: Priority Projects and Their Recommendations for Responsible AI Development", accessed September 19, 2019.
227 "Smart Cities Challenge," Infrastructure Canada, Government of Canada website, accessed September 19, 2019.
228 "Smart Cities Challenge," Making MTL website, accessed September 19, 2019.
229 "Smart Cities Challenge: Documents," Making MTL website.

citizen identification and piloted the Citizen API with the City of Longueuil.[230]

Additionally, in support of the mobility project and Montreal more broadly, the city proposed creating the Civic Innovation Lab for Regulatory Testing, which would be specifically dedicated to municipal regulation and governance.[231] The concept recognizes that new technologies require new models of participation, governance, and regulations — an area of growing research (see for example the Network of Regulatory Experimentation and Legitimacities). The lab would bring together a range of municipal stakeholders with the objective of evolving governance and regulation to "better meet the needs and realities of communities and foster innovation."[232] This includes:

- Creating a new public body on data and technology to oversee the use of data and technology at the municipal level;
- Establishing a governance framework for a common data trust;
- Creating a space and prototyping mechanisms for co-creation; and,
- Removing barriers to innovation.

[230] "Smart Cities Challenge: Documents," Making MTL website.
[231] "Smart Cities Challenge: Documents," Making MTL website.
[232] "Smart Cities Challenge: Documents," Making MTL website.

4.6.3 New York City

As one of the founding members of the Cities for Digital Rights coalition, New York is leading the call to "protect and uphold human rights on the internet at the local and global level."[233] At the local level, the City of New York continues to build digital and data strategies that promote transparency and public collaboration.

4.6.3.1 Digital strategies

Building on the foundation of the 2011 Roadmap for the Digital City, the 2016 Digital Playbook provides six principles and 12 strategies aimed at transforming government digital services to create better resident experiences and a more equitable city. The principles, which largely promote resident inclusion and participation in public digital service design and operations, seek to:

1. **Welcome all** by serving a diversity of needs and backgrounds.
2. **Make government simple** through proactively identifying resident needs and designing to resident preferences and requirements.
3. **Listen and respond** in collaborative service design.

[233] "Declaration of Cities Coalition for Digital Rights," Cities for Digital Rights website, accessed September 19, 2019.

4. **Reach people where they are,** including through existing service and information channels.
5. **Protect trust** by keeping personal data secure and being transparent about data collection and use.
6. **Build collaboration** including sharing data and platforms to improve all resident services.

One of the ways New York City is building capacity to deliver on these principles is through the Service Design Studio at the Mayor's Office for Economic Opportunity, which publishes Civic Service Design Tools + Tactics, workshops, hosts events, and completes design projects that put those who use and deliver services at the centre of creating and improving them.

4.6.3.2 Smart City Guidelines

Led by the City of New York, the Guidelines for Internet of Things (IoT) is a framework for the responsible deployment of connected technologies. It is now adopted by 35 cities (including Chicago) and endorsed by the Council of Global City Chief Information Officers.[234]

The IoT guidelines were created in 2016 by the New York City Mayor's Office with the purpose of providing a common framework through government, maximizing transparency and openness about IoT systems, providing clarity on technical and operational requirements, and advancing public dialogue on multi-sector innovation partnerships. Through a combination of research, stakeholder engagement, and expert review, the city identified global best practices, which they used to inform the guidelines as they were being developed.[235] The guidelines recommend:

1. **Privacy and transparency** about the "who, what, where, when, why and how" of data collection, transmission, processing, and use.
2. **Data management** that ensures that data is captured, stored, verified, and made accessible in ways that maximize public benefit.
3. **Infrastructure**, including devices and networks, that is deployed, used, maintained, and disposed of in an efficient, responsible, and secure manner.
4. **Security** in design and operations to protect the public, ensure the integrity of services, and maximize resilience.
5. **Operations and sustainability** structured to ensure financial, operational, and environmental benefit.[236]

The guidelines are expected to evolve as needs change.

[234] "Partners," Guidelines for the Internet of Things, City of New York website, accessed September 19, 2019.

[235] "About the IoT Guidelines," Guidelines for the Internet of Things, City of New York website, accessed September 19, 2019.

[236] "Guidelines for the Internet of Things," City of New York website, accessed September 19, 2019.

4.6.3.3 Automated Decisions Task Force

Established in January 2018 through The New York City Council as "a local law in relation to automated decision systems used by agencies," the Automated Decision Systems Task Force is the first of its kind in the United States. The task force is required to recommend a process for reviewing the use of automated decision systems (or algorithms) within city government and for ensuring any systems or algorithms are fair and equitable.[237] The 20 task-force members are from multiple sectors and include representatives from city agencies, industry, research organizations, and non-profit and advocacy groups.

To date, the task force has led two public forums — one on the topic of fairness and accountability and one on transparency.[238] The discussion on fairness and accountability focused on:

- Developing criteria for deciding which systems are within the scope of the Task Force and subject to its recommendations.
- Creating processes to determine if a system has disproportionate impact on an individual or group and to address instances of such harm.[239]

In response to developing criteria, the task force created a checklist to assist city agencies in determining whether a tool or system is an automated decision system and subject to the task force recommendations.

The transparency forum discussed a number of processes to ensure or support openness and disclosure, including:

- Information requests about automated decision systems by impacted people;
- Public disclosure strategies about automated decision systems; and,
- Feasibility analyses of archiving agency systems.

The forum also solicited feedback about which systems or technologies should or should not be used by the city, which information about systems is desired by residents, and which organizations are trusted in making decisions about systems.[240]

4.6.3.4 Open Data program

The City of New York's Open Data program is one of the largest and most comprehensive municipal data strategies. Officially launched and codified into law in 2012[241], the

[237] New York City Automated Decision Systems Task Force, City of New York website, accessed September 19, 2019.
[238] New York City Automated Decision Systems Task Force.
[239] New York City Automated Decision Systems Task Force.
[240] New York City Automated Decision Systems Task Force.
[241] The New York City Council, "A Local Law to amend the administrative code of the city of New York, in relation to publishing open data.", March 7, 2012.

strategy goes beyond transparency and accountability and envisions "Open Data for All," where "Open Data is an opportunity to engage New Yorkers in the information that is produced and used by City government. Every New Yorker can benefit from Open Data, and Open Data can benefit from every New Yorker."[242]

To deliver on this vision, the city has partnered with community and industry organizations to create a number of resources to engage residents in participating in the creation, use, and benefit of open data. These include tutorials and guides to increase skills and literacy; Open Data Week to raise the profile of and propagate knowledge about open data through exhibits, panels, and workshops; and public community events and programs like NYC School of Data and the Open Data Borough Ambassadors pilot.

Currently, there are over 2,500 datasets available on the OpenData portal. Progress in publishing data sets and providing data dictionaries and geospatial standards is tracked on the OpenData Dataset Compliance Dashboard.

[242] "Laws and Reports," NYC Open Data website, accessed September 19, 2019.

4.6.4 Chicago

The City of Chicago aims to leverage technology assets for the social and economic benefit of its residents through cross-sector collaboration.[243] This strategy is detailed in the Chicago Tech Plan and demonstrated through the Array of Things project.

4.6.4.1 Tech Plan

Released in 2013, the Chicago Tech Plan outlines 28 initiatives to transform Chicago into a city where "technology fuels opportunity, inclusion, engagement, and innovation."[244] Specifically, the plan aims to deliver impact through:

- Public cost savings;
- Improved public services;
- Increased engagement in problem solving;
- Better access and support to the internet and other digital resources;
- Enhanced computer and digital skills;

[243] Sean Thornton, "The Chicago Tech Plan: Building a Model for Cities and Technology," Data-Smart City Solutions website, Harvard Kennedy School, Ash Center for Democratic Governance and Innovation, September 25, 2013.
[244] City of Chicago, *The City of Chicago Technology Plan,* Chicago Tech Plan, September 25, 2013, accessed September 19, 2019.

- New jobs; and,
- Support for STEM (Science, Technology, Engineering, Math and Medicine) professions.[245]

To accomplish this, the plan outlines five strategies. The first two strategies — establishing next generation infrastructure and encouraging full participation of all Chicago residents and businesses — create the foundation for and enable growth through the following three cross-sector approaches:[246] leveraging new data and technology for government, engaging with civic innovators on public solutions, and encouraging research and technology industry.[247]

4.6.4.2 Array of Things

The Array of Things project in Chicago is one of the largest Internet of Things (IoT) installations to date. Announced in 2014 and launched in 2016, the Array of Things creates a network of 500 sensors that collect real-time environmental measurements for policy, city operations, and research, including development, education, prototyping, and demonstration.[248] It is regularly described as a "fitness tracker for the city"[249] and, similar to a fitness tracker, it can provide residents with information to manage their lives and communities.

Funded by Argonne National Labs ($1 million) and the National Sciences Foundation ($3.1 million), the Array of Things is a partnership between the City of Chicago and the Urban Center for Computation and Data (UrbanCCD) at the Computation Institute, a joint initiative of the University of Chicago and Argonne National Labs. The project requires ongoing cooperation and engagement across multiple organizations and the community.

The Array of Things sensors, called "nodes," include up to 15 sensors, a computer, two cameras, a microphone, and a fan encased in a protective shield.[250] They are attached to City of Chicago streetlights (managed by the Department of Transportation) and collect a range of measurements related to air quality (such as carbon dioxide, sulfur dioxide, and particulate matter), weather conditions (including temperature, barometric pressure, and humidity), street conditions, and sound and light conditions (such as sound levels, visible light, and ultraviolet intensity). The nodes use cellular data to communicate but do not measure the

[245] City of Chicago, *"Impact," The City of Chicago Technology Plan*.
[246] City of Chicago, *"Foundational Strategies," The City of Chicago Technology Plan*.
[247] City of Chicago, *"Growth Strategies," The City of Chicago Technology Plan*.

[248] *Array of Things Operating Policies,* GitHub, August 15, 2016, accessed September 19, 2019.
[249] "Node Location Map," *Array of Things Operating Policies*, GitHub, August 15, 2016.
[250] Sean Thornton, "A Guide to Chicago's Array of Things Initiative," Data-Smart City Initiative website, January 2, 2018.

presence of Bluetooth or Wi-Fi devices.[251] Three examples of potential uses of such data include identifying healthy and unhealthy walk times and routes; detecting flooding in real time; and better estimating where to apply salt before snowstorms.[252, 253]

Designed as an open and scalable project, the technology infrastructure uses an open, modular platform developed at Argonne National Labs called Waggle; data collected by sensors (or nodes) is maintained under the stewardship of the University of Chicago and published to the city's open data portal and on the Array of Things project website through a project API. Sensor instruments and platform technology are designed to evolve with technology and time.

The "Array of Things Operating Policies" presents privacy and governance practices and processes that promote privacy, transparency, and openness. In addition to the governance roles and responsibilities, it also outlines sensor location selection criteria and public engagement and notification requirements before sensor deployment. Policies are expected to be reviewed regularly.

[251] "FAQ," *Array of Things Operating Policies*.
[252] "Current AoT Node Architecture," *Array of Things Operating Policies*.
[253] "Array of Things Operating Policies," *Array of Things Operating Policies*, GitHub, August 15, 2016.

4.6.5 Amsterdam

For close to a decade, Amsterdam has pursued cross-sector collaboration in advancing urban innovation. Starting in 2009 with Amsterdam Smart City, an online collaboration platform for innovation projects and partnerships bringing together 11 core partners across industry, academia, civil society, and city government, Amsterdam continues to build a multi-sector approach to smart cities rooted in trust and sharing. In 2015, Amsterdam was recognized as Europe's first "Sharing City,"[254] and in 2016 it was named the European Capital of Innovation.[255] Currently, the city maintains several ongoing data sharing initiatives as well as a strong commitment to ethics and privacy protection.

4.6.5.1 Data sharing initiatives

The City of Amsterdam is engaged in several cross-sector data sharing initiatives, including the Internet of Things (IoT) sensor registry, a holiday rental registry, and the Amsterdam Data Exchange. The approaches in these initiatives align with the city's digital agenda, released through the 2018 municipal

[254] Theo Bass, Emma Sutherland, and Tom Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons,* DECODE and European Commission, July 3, 2018.
[255] Michael Fitzgerald, "Data-Driven City Management: A Close Look at Amsterdam's Smart City Initiative," *MIT Sloan Management Review*, May 19, 2016.

coalition agreement, which emphasizes an open and democratic digital city.[256]

IoT registry

Amsterdam is creating a voluntary registry of all IoT devices in the city, including those from the private sector. The registry provides residents with information about the presence of a device, the deployer of the device, and the parties who have access to data collected from the device.[257] In addition to creating transparency about data collection and use, the initiative also sees opportunity in building a collective resource with economic benefit.[258] The city envisions that the registry could eliminate duplication of data collection and provide a door to data sharing among entrepreneurs. Amsterdam's chief technology officer has shared some of the challenges associated with implementing the initiative, including that companies sometimes do not know where all of their assets, like sensors, are located, or fear that the disclosure of such information could be used by competitors.[259] Additionally, it can be difficult to enforce reporting.

The registry lists the type of IoT device, such as a camera, sensor, or beacon; the device's location; and the type of data it collects. The devices are currently displayed on an interactive map, and the city is in the process of building open source tools for device registration and measurement of connected devices.

Holiday rental registry

Amsterdam city regulations limit the number of days a year that a landlord in Amsterdam can let a property for short-term accommodation. As of 2017, Amsterdam requires accommodation providers to register holiday rentals on an online registry.[260] While needing to collect information for compliance and enforcement measures, the city aims to protect privacy and provide individuals control over personal information.

To create a holiday rental registry, the city partnered with DEcentralized Citizen Owned Data Ecosystems (DECODE), which is funded by the EU's Horizon 2020 Program, on a pilot project to create a technical platform that enables accommodation providers to share only essential information about their property and holiday-rental occupants to the city. By using attribute-based credential technology, the platform allows a resident who rents out their property to choose selected attributes about their occupants to share with the registry, limiting identifying information to as little as "person is a resident of the City of Amsterdam" or "person is over the

256 Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

257 "The IoT Registry," Interreg North Sea Region SCORE European Regional Development Fund website, accessed September 19, 2019.

258 Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

259 Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

260 Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

age of 18."[261] While demonstrating the privacy-preserving capacity of the technology, the pilot project also highlighted the need to provide more information to users about data sharing and what personal data control entails.

Amsterdam Data Exchange

The Amsterdam Data Exchange (AMdEX) is a data sharing initiative developed by the Amsterdam Economic Board, a cross-sector economic advocacy partnership, and Science Park Amsterdam, an innovation and research campus, with the support of the City of Amsterdam. Currently a concept in development, AMdEX is designed to promote data privacy and sovereignty while fostering cooperation across sectors and national boundaries.

AMdEX is a transparent "open-data market" where data producers, such as organizations and communities, would retain control over their data and would be able to share selected data or attributes with others.[262] It would also allow users of the open-data market to shop, compare, and agree to data-service provision.[263] AMdEX aims to create a trusted data market for data sharing that offers opportunities for cooperation that would not be achieved from separate, independent sharing transactions.[264]

AMdEX fosters data exchange by serving as an intermediary between data providers, their data ("product"), and data-storage hubs by providing:

- **Technical infrastructure**, including secure data transfer and processing;
- **Services**, such as quality assurance, tools for compliance assessment and auditability, interoperability, scalability, software-based enforcement, and conflict resolution;
- **Common rules** including contract models and legal interoperability.[265]

4.6.5.2 TADA manifesto

In 2017, a wide range of actors in Amsterdam, including those representing government, business, civil society, and residents, came together to address the opportunities and challenges of digital tech. They proactively created guidelines for the responsible use of data in smart cities, producing a manifesto called "TADA: Data Disclosed."[266] The six principles listed in their original form are as follows:

[261] Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*
[262] Amsterdam Data Exchange, *Towards an Internationally Trusted Exchange of Data: The Data Hypermarket* (Amsterdam: City of Amsterdam, University of Amsterdam and Free University of Amsterdam, 2018).
[263] Amsterdam Data Exchange, *Towards an Internationally Trusted Exchange of Data: The Data Hypermarket*.
[264] "About," About AMdEX, Amsterdam Economic Board website, accessed September 19, 2019.
[265] Amsterdam Data Exchange, *Towards an Internationally Trusted Exchange of Data: The Data Hypermarket*.
[266] Tada website, accessed September 19, 2019.

1. **Inclusivity.** Our digital city is inclusive. We account for the differences between individuals and groups, without losing sight of equality.
2. **Control.** Data and technology should contribute to the freedom of citizens. Data is meant to serve the people; to be used as seen fit by people to benefit their lives; to gather information, develop knowledge, and organize. People stay in control over their data.
3. **Tailoring to the people.** Data and algorithms do not have the final say. Humanity always comes first. We leave room for unpredictability. People have the right to be digitally forgotten, so that there is always an opportunity for a fresh start.
4. **Legitimacy and monitoring.** Citizens and users have control over the design of our digital city. The government, civil society organizations and companies facilitate this. They monitor the development and the social consequences.
5. **Openness and transparency.** What types of data is collected? For what purpose? And what are the outcomes and results? We are transparent about this.
6. **From everyone — for everyone.** Data that the city, companies and other organizations generate from the city are held in common. Everyone can use them. Everyone can benefit from them. Together we make agreements about this.[267]

[267] Tada website.

In addition to this framework, one of the manifesto creators, the Amsterdam Economic Board, created TADA — branded labels to increase visibility of the principles and visually communicate that a piece of technology, organization, or event supports and adheres to the manifesto.[268] Branding and labels such as these serve as a sort of ethical certification of products, services, and organizations.

4.6.6 Barcelona

The City of Barcelona leverages digital innovation for resident-driven data-informed policy. After significant investments in digital infrastructure over the first half of the decade, the city shifted its smart city approach to leverage its investments and develop technologies as an "instrument to empower people and transform the city."[269] Through this lens, the City of Barcelona is creating a new model for participation and innovation.

[268] Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*
[269] "Barcelona Digital City: About Us," Ajuntament de Barcelona website, accessed September 19, 2019.

4.6.6.1 Digital strategies

Sensors and Internet of Things

In 2012, the city released its Smart City Strategy, which focused heavily on Internet of Things investments.[270] A network of sensors for different public services — transportation and streets, waste management, and energy — was built on the city's extensive fibre network and enabled more efficient and effective delivery of public services. For example, the city:

- Installed smart meters and sensors for energy consumption, including LED lamp posts that automatically dim (and provide free internet access), leading to annual savings of 30 percent in energy use and $37 million in costs.
- Introduced park irrigation sensors with remote controls creating a 25 percent increase in water conservation.
- Optimized residential waste collection through municipal smart bins.
- Provided more accurate information for transportation, including multimodal transit and smart street-parking spaces.[271]

Real-time sensor data is collected on Barcelona's open-source platform Sentilo. Currently, the city is in the process of opening up this platform, in which residents could choose to share personal data with the city as a way to help the city better understand their needs.[272]

Ethical Digital Standards and Barcelona Digital City 2017

The 2015 mayoral change propelled the city's development of resident-centred and democratic approaches to technology. While acknowledging the value of data in public policy and service delivery, Barcelona seeks to address the political and ethical challenges accelerated by technology through advancing "data as commons."[273] This concept envisions data as a public infrastructure that is created by and serves residents and positions the city as the custodian for the residents' data rights.[274]

To realize this vision, the city created a manifesto and related policy toolkit for ethical digital standards, along with a new digital strategy, Barcelona Digital City. Together they look to transform how innovation policy and projects are created and implemented. The manifesto details core values and goals for technological sovereignty and digital rights for cities, including:

---

[270] Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

[271] Laura Adler, "How Smart City Barcelona Brought the Internet of Things to Life," *Data-Smart City Solutions,* February 18, 2016.

[272] Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

[273] Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

[274] Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

1. **Technological and data sovereignty,** including full control and autonomy of information and communications technologies such as service infrastructures, websites, applications, and data.
2. **Digital rights for citizens,** including privacy, security, information self-determination, and neutrality, placed at the centre of digital policies and protected through the implementation of technological sovereignty and digital democracy policies.
3. **Interoperability and accessibility** though free software, open data and open standards, document and data formats, and communication protocols.
4. **Collaborative development** through sharing and pooling of resources.
5. **Citizen and industry participation in technology design and governance** empowered by open city data.
6. **Transparency, auditability, security and privacy** through mandatory adoption of open standards, document and data formats and communication protocols.[275]

To aid the integration of these principles into municipal policies and practices and to support the city's digital agenda, the ethical digital standards policy toolkit translates these principles into the following eight guides. They include:

[275] Francesca Bria and Malcolm Bain, Ethical Digital Standards, Ajuntament de Barcelona website, accessed September 19, 2019.

- **Digital service standards,** outlining digital principles;
- **Technology code of practice** for municipal leaders managing technology and innovation projects;
- **Technology sovereignty** best-practices guide for implementing free software, standards, formats, and interoperability best practices;
- **Free software management** covering development, technical infrastructure, management, legal, and documentation;
- **Agile methodologies**, including general principles;
- **ICT procurement** overview for increasing knowledge on strategic measures;
- **Innovative public procurement,** providing case studies and procedures; and
- **Ethical data management,** including policies for the governance, planning, procurement, management, analysis, use, protection, access, preservation, and reuse of municipal data, to add value to municipal digital information throughout its life cycle.[276]

[276] Francesca Bria and Malcolm Bain, Ethical Digital Standards, Ajuntament de Barcelona website, accessed September 19, 2019.

4.6.6.2 Digital tools for participation

The city's priorities of sovereignty and free and open infrastructure allow for greater participation, and call for tools for digital engagement. Decidim is a free, open source digital participation platform developed for Barcelona's residents. Launched in February 2016, it is a mobile tool that allows residents to vote and comment on city council budgets and proposals, and analyze their viability.[277] It also allows users to track the progress of the selected projects.

With the adoption of the tool by over 30,000 users, the city is looking to enhance data sovereignty features within the tool.[278] The city is partnering with DECODE to create an application in which residents can set specific permissions over what types of data they share. This would let residents decide how their data can be used by the city council or any other third party.

---

[277] "Decidim.barcelona," Euro Cities website, accessed September 19, 2019.
[278] Bass, Sutherland, and Symons, *Reclaiming the Smart City: Personal Data, Trust and the New Commons.*

Attachment A

Quayside Digitally Enabled Services List

Disclaimer: Due to the complex nature of this table it may be challenging to navigate for some users. If you require additional support to navigate this table please contact us at accessibility@sidewalklabs.com.

	Proposed Service	Waterfront Toronto Priority Outcomes	Subsystem	Subsystem Objective(s)
2	Dynamic Streets - Mobility Management	New Mobility	Real-Time Traffic Operational System	More efficient flow of traffic. Faster travel times for vehicles, pedestrians, and cyclists.
3	Dynamic Streets - Mobility Management	New Mobility	Bicycle Green Wave	Enhanced safety for cyclists and decreased travel time.
4	Dynamic Streets - Mobility Management	New Mobility	Adaptive Traffic Signals	Coordination of all travel modes. Enhanced safety for cyclists and decreased travel time. Safer intersections for pedestrians and reduced traffic.
5	Dynamic Streets - Mobility Management	New Mobility	Real-Time Crosswalks	Safer and more efficient movement of people and public transportation.
6	Dynamic Streets - Mobility Management	New Mobility	Dynamic Curb	More efficient movement of vehicles: fewer parking spaces, more reclaimed land for the public realm, and reduced overall traffic congestion
7	Dynamic Streets - Mobility Management	New Mobility	Autonomous Vehicle Traffic Management (Future Case)	Freeing up additional space for pedestrians by enabling sharing of rights of way between AVs and public transit.
8	Dynamic Streets - Streetscape	New Mobility, Sustainability and Climate-Positive Development	Weather-Responsive Heated Pavement	Increased ability to use non-GHG emitting modes of transportation (e.g., walking, cycling) year-round.
9	Dynamic Streets - Streetscape	Sustainability and Climate-Positive Development	Responsive Street Lighting	More efficient use of energy for streetlights.
10	Dynamic Streets - Streetscape	Urban Innovation - Inclusive Communities	Public Realm Enhanced Accessibility	More inclusive street design and improved mobility for people who are visually impaired.
11	District Parking Management	New Mobility	Managed Satellite Parking with Valet Service	Fewer unnecessary cars on the roads, safer and more enjoyable for pedestrians.
12	District Parking Management	New Mobility	Enhanced Electric Vehicle Charging	More convenient charging for EVs.
13	Mobility as a Service	New Mobility, Sustainability and Climate-Positive Development	Mobility as a Service (MaaS)	MaaS enables a Unified Mobility Subscription, which would make public transit, ride-sharing, and active modes of transport less expensive and more convenient than owning a car; more residents choose not to own private automobiles; fewer employees choose to drive to work; lower household expenditures on mobility. More people choosing active transportation in an organized fashion or as part of a multi-modal trip.
14	Public Realm Management	Urban Innovation - Inclusive Communities	Public Realm Geographic Information System Database ("Maintenance Map")	Reduce cost of maintenance with more accurate information and reduce interruptions to public space use. Increase the overall quality of public space. Enable higher quality maintenance and/or more targeted maintenance. Community booking of spaces
15	Public Realm Management	Urban Innovation - Inclusive Communities	Outdoor Comfort System - Outdoor Weather-Mitigation	Increase time people can comfortably spend outdoors.
16	Public Realm Management	Urban Innovation - Inclusive Communities	Multi-Purpose Sports Courts	Maximize the diversity of uses within the park
17	Public Realm Management	Urban Innovation - Inclusive Communities	Commonspace - Community Tool for Management of Public Space	Evidence-based improvements to the use of public space.
18	Ground Floor/Flexible retail platform - "Seed Space"	Job creation and Economic Development	Flexible retail platform - "Seed Space"	Increase ground floor activity by making it far easier for businesses to launch and operate in brick and mortar. Support businesses by identifying co-tenancy, co-programming, and co-merchandising.
19	Outcome Based Code - Building Systems	Job creation and Economic Development	Outcome-Based Building Code Monitoring	Allow for a more diverse mix of tenants in a given building. Provide for greater long-term flexibility with less disruption for continuous repurposing of building units. Increase the building performance by monitoring and measuring energy usage, equipment performance, indoor air quality, etc.
20	Outcome Based Code - Building Systems	Job creation and Economic Development	Building Monitoring	Continuous monitoring of building nuisance and environmental noise conditions.
21	Building - Energy Management	Sustainability and Climate-Positive Development, Housing Affordability	Building Management System (BMS) / Building Information Model for Facilities Management	BMS provides automated controls for HVAC equipment using industry standard sensors and protocols. Increase ease of building operations and life-cycle management by monitoring and maintaining the built environment using a digital model to inform and document facilities management. Notify Building Maintenance and Emergency Service Providers of maintenance issues from various systems.
22	Building - Energy Management	Sustainability and Climate-Positive Development, Housing Affordability	Building Operator Scheduler	Manage energy use to enable the transition from natural gas to electricity for all thermal loads while maintaining energy bills within 10% of Business-As-Usual. More customer control over utility costs.
23	Building - Energy Management	Sustainability and Climate-Positive Development, Housing Affordability	Office Scheduler	Manage energy use to enable the transition from natural gas to electricity for all thermal loads while maintaining energy bills within 10% of Business-As-Usual. More customer control over utility costs.
24	Building - Energy Management	Sustainability and Climate-Positive Development, Housing Affordability	Home Scheduler	Manage energy use to enable the transition from natural gas to electricity for all thermal loads while maintaining energy bills within 10% of Business-As-Usual. More customer control over utility costs.
25	Building - Energy Management	Sustainability and Climate-Positive Development	HVAC Performance Monitoring	Monitor building HVAC system performance to optimize thermal energy use and lower peak demand.
26	Building - Energy Management	Sustainability and Climate-Positive Development	Efficient Building Lighting	Lower energy consumption and cost by monitoring building lighting use and efficiency.
27	Building - Energy Management	Sustainability and Climate-Positive Development	Building Electricity Monitoring	Lower peak energy demand by monitoring electricity use.
28	Building - Energy Management	Sustainability and Climate-Positive Development, Urban Innovation	Digital Electricity	Improved metering capability, increased electrical control of devices and enables automated fault detection of plugged in devices.
29	Building Performance Monitoring Platform - "Perform"	Sustainability and Climate-Positive Development	Building Performance Monitoring Platform ("Perform")	Enable building operator to validate that buildings meet performance objectives in operation and not just design, and provide reporting to regulators.
30	Logistics - Freight Management System	New Mobility	Logistics - Freight Operational System	Reduced traffic on the roads and more efficient housing units. Ease of personal storage, retail inventory storage, the sharing of goods, and discarding of non-pneumatic waste for both commercial and residential users.
31	Logistics - Freight Management System	New Mobility	Urban Consolidation Centre & Delivery System	Reduced traffic on the roads, simplified shipping, safe and timely delivery of mail and parcels.
32	Logistics - Freight Management System	New Mobility	Storage and Borrow System	Increases free space in apartments and businesses, simplified storage.
33	Logistics - Freight Management System	Sustainability and Climate-Positive Development	Specialized Waste System	Keep waste not managed by the pneumatic system separated as it was at the source point.
34	Waste Management System	Sustainability and Climate-Positive Development	Waste Sorting, Processing, and Monitoring	Improve diversion of waste from landfill by providing users with feedback on recycling stream to improve sorting effectiveness.
35	Waste Management System	Sustainability and Climate-Positive Development	Building Waste System	Enable Toronto's pay-as-you-throw waste system to be utilized within multi-family buildings
36	Waste Management System	Sustainability and Climate-Positive Development	Pneumatic Waste Collection System	Keep trash separated as it was at the source point.
37	Waste Management System	Sustainability and Climate-Positive Development	Self-Driving Trash Bins	Prevent litter conditions that reduce quality of the public realm and increase maintenance costs
38	Active Stormwater Management (SWM)	Sustainability and Climate-Positive Development	Active Stormwater Operational System	Maximize the use of green infrastructure to manage stormwater instead of concrete tanks, mechanical and electrically powered filtration systems. Actively manage stormwater controls based on the prediction of rain events in order to maximize beneficial greywater reuse and minimize the volume of stormwater entering the municipal system in heavy rain events.
39	Active Stormwater Management (SWM)	Sustainability and Climate-Positive Development	Stormwater Monitoring System	Optimize the management of stormwater within the district to minimize grey water infrastructure, and use water as a resource to its highest and best use.
40	Active Stormwater Management (SWM)	Sustainability and Climate-Positive Development	Green Infrastructure Performance Monitoring	Diagnosis and maintenance of the health of green infrastructure components of the stormwater system.
41	Active Stormwater Management (SWM)	Sustainability and Climate-Positive Development	Grey Water Infrastructure Monitoring	Diagnosis and maintenance of the grey water infrastructure components of the stormwater system
42	District Energy System	Sustainability and Climate-Positive Development, Housing Affordability	Advanced Power Grid (APG)	Flatten neighborhood peak electricity demand to avoid infrastructure expansion, which increases costs for all consumers, and reduce use of most expensive and most GHG-intensive grid power.
43	District Energy System	Sustainability and Climate-Positive Development, Housing Affordability	Thermal Grid	Electrification of all thermal loads to eliminate natural gas consumption, to support Climate Positive Development, and to maintain affordability.
44	District Energy System	Sustainability and Climate-Positive Development, Housing Affordability	Distributed Energy Resource Management System (DERMS)	Reduce spending on electricity and reduce GHG emissions.
45	District Energy System	Sustainability and Climate-Positive Development, Housing Affordability	Dynamic Rate Engine	Lower electricity use during peak hours. More customer control over utility costs.
46	Digital Infrastructure	Urban Innovation	Koala	Create a new urban device innovation ecosystem by greatly reducing the cost and complexity of device installation. Enables the ability to authenticate and enable specific, approved devices in the public realm. Enables the ability to audit / monitor / remove devices as needed via software.
47	Digital Infrastructure	Urban Innovation - Inclusive Communities	Ubiquitous internet connectivity	Increase availability and ease of connectivity to the Internet, and enables better community broadband access via public Wi-Fi. In addition, increase security, decrease technical overhead, and decrease hardware required to connect to high-speed, secure internet.
48	Digital Infrastructure	Urban Innovation	Distributed digital identity credentials	Provide individuals with the ability to control and minimize the personal information they provide.
49	Digital Infrastructure	Urban Innovation	Device Registry	Greater transparency for the public about data collection and use.
50	Digital housing application system	Housing Affordability; Urban Innovation - Inclusive Communities	Digital housing application system	Increased access for eligible low- and moderate-income households. Simplified and transparent process for affordable applicants. Reduced vacancy rates for developer(s) by accelerating lease-up timelines.
51	Civic Engagement - "Collab"	Urban Innovation - Inclusive Communities	Civic Engagement - "Collab"	Community engagement and influence in decision-making
52	Infrastructure that enables personal assistive tech	Urban Innovation - Inclusive Communities	Infrastructure that enables personal assistive tech	Making it possible for existing navigation tools to make trips and mobility accessible, safe and convenient.
53	Real-time digital map of the municipal utility network	Urban Innovation	Real-time digital map of the municipal utility network	Reduce cost of maintenance and enable predictive maintenance.