Sidewalk Labs

October 2018

Digital Governance Proposals for DSAP Consultation

TABLE OF CONTENTS

DRAFT PROPOSALS

DRAFT PROPOSALS

Sidewalk Labs started with a belief...

By integrating forward-thinking urban design and technological solutions we aim to address urban challenges experienced around the world and fundamentally improve quality of life in cities.

We began by speaking with experts from around the world
in fields like mobility, affordable housing, construction, technology, policy, planning, and governance.

From those conversations we envisioned new experiences that could be possible in a new type of city.

Among the new experiences we imagined, we recognized a common theme — that many involved utilizing data in new ways.

We knew that technology could catalyze these solutions, and data would make them better. But we also knew that data for data's sake or tech for tech's sake would not improve quality of life.

From the outset we knew that the monetization of data would not be part of our business model. That is why we committed not to sell personal information or use it for advertising purposes.

The New York Times

TECHNOLOGY

Sidewalk Labs, a Start-Up Created by Google, Has Bold Aims to Improve City Living

June, 2015

The Silicon Valley giant is starting and funding an independent company dedicated to coming up with new technologies to improve urban life. The start-up, Sidewalk Labs, will be headed by Daniel L. Doctoroff, former deputy mayor of New York City for economic development and former chief executive of Bloomberg L.P. Mr. Doctoroff jointly conceived the idea for the company, which will be based in New York, with a team at Google, led by its chief executive, Larry Page.

The founders describe Sidewalk Labs as an "urban innovation company" that will pursue technologies to cut pollution, curb energy use, streamline transportation and reduce the cost of city living. To achieve that goal, Mr. Doctoroff said Sidewalk Labs planned to build technology itself, buy it and invest in partnerships.

A FEW SPECIFIC EXAMPLES

Streets that prioritize safety, pedestrians, and cyclists, because they are designed to anticipate shared, self-driving vehicles that wouldn't need much parking and could communicate with each other and with adaptive traffic lights. This would mean significant amounts of street space given back to pedestrians and cyclists, less congestion, and improved safety.

Buildings with a far more diverse and vibrant mix of uses as a result of "outcome-based code," which doesn't require uniformity of use but rather ensures structural integrity, air quality, and noise levels through conditions-sensing technology.

Significantly reduced carbon emissions achieved by technology that monitors and manages energy demand across the neighbourhood.

...and many more

DRAFT PROPOSALS

We conducted extensive consultations on responsible data use

Over the past year, as Sidewalk Labs prepares a "Master Innovation and Development Plan," we have had extensive consultations with experts, government, regulators, and residents in Toronto and across Canada.

We engaged Dr. Ann Cavoukian, the three-term Information and Privacy Commissioner of Ontario, who created the internationally adopted **Privacy by Design framework**, as an advisor to the project.

We meet regularly with privacy regulators to talk about our plans and seek guidance. Sidewalk Toronto is the first participant in the Office of the Privacy Commissioner of Canada's newly formed Business Advisory Directorate.

We convened a Data Governance Working Group of academics, former regulators, technologists including Canada's leading expert on de-identification, private sector leaders, and community representatives who have advised us on topics ranging from responsible data use in product development to governance and stewardship issues.

We talked to the private sector—early stage startups and large multinationals— about what they see as key opportunities and challenges.

We participated in the public consultations around Canada's National Data Strategy.

We carefully considered feedback from public roundtables, the Residents Reference Panel, and the Sidewalk Toronto Fellows report.

We studied examples from around the world of best practices, policy innovations, and lessons learned.

We welcomed thousands of people from Toronto and around the world to *307* to engage with our team in conversations about every issue we are looking at, including data.

We established a research grant program to explore a range of complex issues, including the intersection of privacy and the collection of non-personal information in the physical environment.

5

We engaged privacy regulators on issues related to digital governance

Excerpt from the Office of the Privacy Commissioner of Canada
(Annual Report to Parliament, September 27, 2018).

"We announced in May 2018 our first advisory project involving Sidewalk Toronto, a smart-city endeavor between Waterfront Toronto and Sidewalk Labs,

owned by Google's parent company Alphabet. The initiative involves building a technology-driven neighbourhood on the city's eastern waterfront that includes sensors aimed at helping city planners find efficiencies.

Understandably, it is raising many questions about data collection, privacy, where the information will be stored and how it might be used.

Along with colleagues from the Office of the Information and Privacy Commissioner of Ontario, members of our Business Advisory Directorate met with those behind the project to learn more about it and how they were addressing some of these privacy concerns.
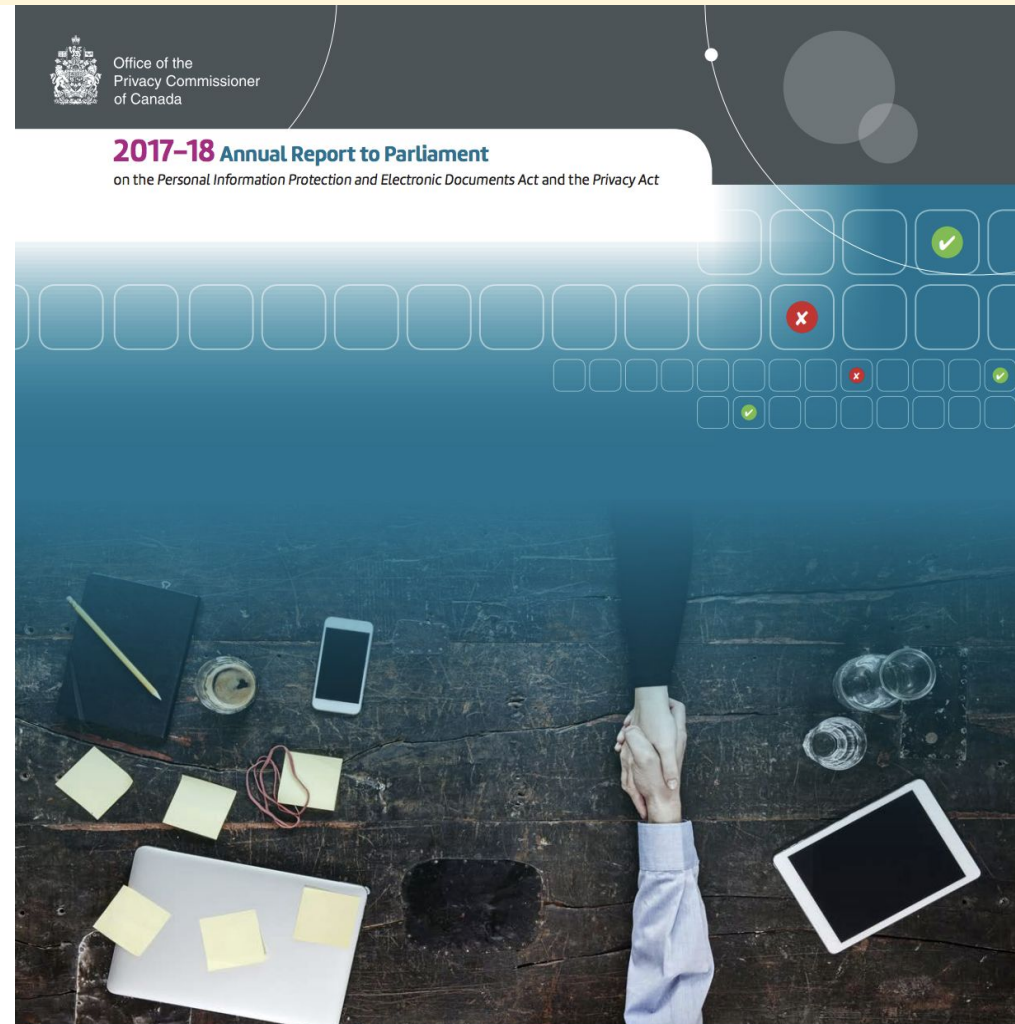
We also reminded officials of key privacy principles, including identifying the purposes for collection, obtaining consent, ensuring individuals could access their own personal information and being accountable for protecting the data and being clear about who owns it.

Overall, we are encouraged by Sidewalk Toronto's efforts to proactively address privacy and data security in the design and implementation of the initiative.

Given the project is still in its early stages, we are continuing to monitor developments and proactively engage with Sidewalk Toronto officials as it progresses. We also hope the advice we provide will be helpful as other smart city initiatives pop up across the country."

Office of the Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada

2017–18 Annual Report to Parliament
on the *Personal Information Protection and Electronic Documents Act and the Privacy Act*

TRUST BUT **VERIFY**
Rebuilding trust in the digital economy through effective, independent oversight

DRAFT PROPOSALS

6

A range of concerns and questions surfaced with regard to data and the Quayside project

Confusion about Sidewalk Labs' plans related to data, exacerbated by the time it has taken to work through complicated issues

Concern that data monetization is a key part of Sidewalk Labs' business model

An array of questions:

- **Is Sidewalk Labs**, and this project, intended to be a data source for Google?

- **How will data—particularly data collected in the physical environment**, which some argue should be considered a public asset—be protected and governed?

- **Who will own and control the data** that originates in Quayside's physical environment?

- **How do we address the difficulty of obtaining consent** when collecting data in the physical environment?

- **What are the respective roles of Sidewalk Labs**, other private sector players, and governments when it comes to data and technology?

- **How do we ensure all innovators**, including Sidewalk Labs, will be on equal footing in Quayside?

- **How do we make sure the protections of Canadian law apply to all data** originating in Quayside?

AN ONGOING, COLLABORATIVE PROCESS

This presentation to the Waterfront Toronto Digital Strategy Advisory Panel includes ideas formed in response to what we've heard and learned.

We will use this opportunity and ongoing consultations to further develop these ideas into components of the **Master Innovation and Development Plan, a draft of which will be released in early 2019.**

In the coming months, we will return to the DSAP for discussion of several other topics: intellectual property; charter, governance structure and implementation of the Data Trust; data security, including technological approaches to protecting personal identity and information; and case studies on technologies planned to be implemented by Sidewalk Labs in Quayside. We will also continue conversations on the Responsible Data Use Guidelines and the Responsible Data Impact Assessment.

DRAFT PROPOSALS

Sidewalk Labs determined that Privacy by Design would be embedded into all of our projects, from the beginning

Privacy by Design is an essential component of fundamental privacy protection that served as Sidewalk's first building block as we formulated an approach to Responsible Data Use.

FOUNDATIONAL PRINCIPLES	SIDEWALK LABS' IMPLEMENTATION
Proactive not Reactive *Preventative not Remedial*	Sidewalk Labs is developing and will utilize cutting edge privacy-enhancing technologies including k-anonymity, edge computing, and other de-identification techniques.
Privacy Embedded into Design	Sidewalk Labs conducts Responsible Data Impact Assessments (RDIAs) to enable consistent and transparent decision making. Every project/product starts with a detailed, nuanced discussion of how it is going to interact with data and protect the rights of individuals.
Privacy as the Default Setting	Sidewalk Labs designs projects/products to add value *without* collecting personal information if possible. If personal information is required, Sidewalk destroys the data as close to the source as possible; or de-identifies data using world-class techniques.
Full Functionality *Positive-Sum, not Zero-Sum*	Sidewalk Labs not only embeds privacy into urban development projects, but seeks to develop technologies that benefit the project as well as enhance privacy for the individual.
End-to-End Security *Full Lifecycle Protection*	Sidewalk Labs engages the best and brightest tech and policy thinkers to inform our processes and practices. Sidewalk utilizes (and develops) state of the art technology and processes to protect personal information from loss, theft, and unauthorized access.
Visibility and Transparency *Keep it Open*	Sidewalk Labs proactively communicates the reason we are collecting data and the benefits to individuals when we ask for their personal information, in a clear and easy to understand manner.
Respect for User Privacy *Keep it User-Centric*	Sidewalk Labs is developing ways of providing services which allow user-centric data management and anonymous authorization for access control.

PRIVACY BY DESIGN

In October 2010, regulators at the International Conference of Data Protection Authorities and Privacy Commissioners unanimously passed a resolution recognizing Privacy by Design as an essential component of fundamental privacy protection.

Privacy by Design embeds privacy measures into the design of a project, asking questions such as: *"What is the minimum data you really need to accomplish the goal?"* and *"Do you need personal information, or can you accomplish it with de-identified data?"*

Since then, Privacy by Design has developed Into a global presence and has been translated into 40 languages.

We established and continue to refine Responsible Data Use Guidelines that serve as a foundation for our work

These Responsible Data Use Guidelines guide our work on the development of policies that implement **Privacy by Design** and address data stewardship and access to data.

- **People first.** All projects must apply Canadian values of diversity, inclusion, and privacy as a fundamental human right.

- **Beneficial public purpose.** There must be a clear public purpose and value to the proposed use of Urban Data. A proposal cannot collect data for data's sake.

- **Transparency and clarity of usage.** Projects must always inform individuals of how and why their information is being collected and used, and do so in a way that is proactive, clear, and easy to understand. For Urban Data in public spaces, where meaningful consent cannot be reasonably or reliably achieved, clarity of usage can include efforts such as physical signs notifying people of a data device, or informational websites describing a service or program in greater detail.

- **Meaningful consent.** If a person opts into a service that uses individual identification, that person must have meaningful consent or control over how the information is used. Meaningful consent must go beyond current privacy policies, which are typically long and written in legalese, balancing the substance necessary for legal consent with a simplicity that people can understand.

- **De-identify by default.** Urban Data that includes personal information must be "de-identified" by default — designed not to trace back to any individual. For example, if a traffic counter collects an image of three cars that includes license plates, this data can be de-identified by processing a count of "three cars" and deleting the raw image containing the license plate information. Once de-identified, a data set is considered to no longer contain personal information, as the risk of re-identification is extremely low.

- **Open by default.** All de-identified Urban Data gathered in the public realm will be made open, free, and available in the public domain by default to encourage innovation and reflect the role of Urban Data as a collective good.

- **No ads by default.** By default, companies, organizations, or individuals will not sell Urban Data containing personal information to third parties or use it for advertising purpose.

NEED FOR A ROBUST FRAMEWORK

The pace at which the world is changing has underscored the need — and the opportunity — to create a new framework for responsible data use in Quayside:

- **People are more connected now** than ever before, and the proliferation of data raises real concerns about the impact on personal privacy.

- **Recent high-profile examples of data and privacy breaches** or misuse have further evidenced the potential impact of inadequate privacy protection.

DRAFT PROPOSALS

Sidewalk Labs' proposed approach to digital governance aims to serve as a model for cities around the world

Sidewalk's proposed approach to digital governance in Quayside will demonstrate to Toronto, Canada, and the rest of the world that cities do not need to sacrifice their values of inclusion and privacy for opportunity in the digital age.

Our approach to digital governance is based on the position that:

- **Independent governance** is necessary to protect personal and public interests across areas of data stewardship, privacy, access, and, security—in addition to government enforcement of Canadian and Ontario privacy laws and regulations

- **All parties**, including Sidewalk Labs, collecting and/or using data in the physical environment of Quayside will be held to the same high standards of digital governance

- **Information architecture and services** should be open, enabling and promoting innovation by the many, not the few

Based on these positions, we propose four key components of a framework for digital governance in Quayside:

- **Responsible Data Use (RDU) Guidelines**: Application of the guidelines to all parties in Quayside, not just Sidewalk Labs, to put personal privacy and the public good first, while fostering innovation

- **Civic Data Trust**: An independent entity to control, manage, and make publicly accessible all data that could reasonably be considered a public asset, and a set of rules that would apply to all entities operating in Quayside, including Sidewalk Lab. With the Data Trust, we move away from entities, including Sidewalk Labs, solely owning and controlling these assets.

- **Responsible Data Impact Assessment (RDIA)**: Publicly auditable assessment for all public and private digital services required before data is collected and used

- **Open Standards**: Sidewalk will base its technology on open standards, making it easy for others to build and connect new services, offer competitive alternatives, and drive innovation; the Data Trust might consider encouraging or requiring open standards, as well

KEY TAKEAWAYS

No one should own original information collected from Quayside's physical environment—including Sidewalk Labs. Instead, this "Urban Data" should be under the control of an **independent Civic Data Trust.**

To protect privacy, all entities proposing to collect or use Urban Data (including Sidewalk Labs) will have to file a **Responsible Data Impact Assessment** with the Trust that is publicly available and reviewable.

With regard to the use of data, **one set of rules will apply to everyone.** Sidewalk Labs will not receive any special treatment.

Sidewalk Labs will use open standards for any digital infrastructure and services it provides—so anyone can plug in or compete.

DRAFT PROPOSALS

DRAFT PROPOSALS

Data Trusts are beginning to be used to govern data in urban contexts

A Civic Data Trust is a model for stewardship and management of data and digital infrastructure that approves and controls the collection and use of data for the benefit of society and individuals.

A Civic Data Trust is particularly useful where data is being collected and used in an urban environment and there are challenges in obtaining meaningful consent.

It is an independent third party that ensures that value from data goes to the people, communities, government, industry, and society from which it was collected, and that data privacy and security are protected. **A Data Review Board**, assembled of diverse members of the community, would monitor and enforce data collection and use.

Other cities, countries, and organizations around the world, including Canada, Barcelona, Estonia, Guernsey Island, and the Copenhagen-Hitachi City Data Exchange, have implemented variations of data trusts.

GLOBAL EXAMPLES OF DATA TRUSTS

Data trusts come in different forms and structures, two of which are:

Barcelona Model: Trusted Intermediary and a Data Commons

Barcelona's CityOS is the city's internal data lake, which is managed by the city's Chief Data Officer. In this model, all of the data is pooled into one central repository, a "commons", and managed by a trusted intermediary. Some datasets are made publicly available under degrees of openness via APIs. Some data is available through Decidim, Barcelona's digital democracy portal, or BCNow, its data dashboard. 'Sentilo' is Barcelona's main sensor platform for environmental or ambient data. Barcelona's projects are funded by the EU Commission's DECODE.

CITYOS
CITY OPEN SOURCED

Estonia Model: API Framework Management

Estonia's X-Road data exchange platform is based on an approach where each collector of data stores its own data, which are standardized and accessed through APIs that are managed by the Trust. It is a repeatable framework of terms and conditions with APIs that allow developers and others to access data for testing, product development, and data analytics.

X-ROAD

DRAFT PROPOSALS

Proposal: A Civic Data Trust for Quayside

The stewardship, management, and responsibility for data that is collected and used
needs to sit with an independent entity whose sole responsibility is to protect the public interest.

The Trust would be an independent body with the mandate
of being a steward of data collected in the physical environment,
which we call **Urban Data**.

- **Following Responsible Data Use Guidelines, the Trust would
  approve and control** the collection and use of, manage access to,
  and, potentially, store Urban Data originating in Quayside. This would
  be on top of—not in the place of—existing law, regulation, and
  government enforcement.

- **The Trust would, as a default, make de-identified Urban Data
  freely and publicly accessible—and not owned by any private
  entity**. The Trust would consider applications to collect Urban Data that
  involves personal information (e.g. CCTV cameras) or proposals to collect
  Urban Data on a proprietary or commercial basis.

- **In performing those functions, the Trust would be guided
  by a charter** focused on ensuring that Urban Data is collected and
  used in a way that is beneficial to the community, protects privacy,
  and spurs innovation and investment.

- **The governance of the Trust** would apply to all entities
  operating in Quayside.

BENEFITS OF THE CIVIC DATA TRUST

- **Protects** the public interest

- **Curtails** private ownership of data that might
  reasonably be considered a public asset

- **Ensures** compliance with data protection and privacy laws

- **Upholds** a set of values and processes for the beneficial use of data

- **Organizations** can share their data with other entities across
  different sectors for mutual benefit

- **Access** to different data sources allows us to understand public
  problems from many angles

- **Opportunities for new**, innovative, and data-driven
  solutions to public problems

- **Data collection** and use is made transparent

- **Institutions** can better monitor and evaluate the real-world impacts of policies

DRAFT PROPOSALS

Defining Urban Data

Data collected in the physical environment, particularly in public spaces, will be the domain of the Civic Data Trust.

Urban Data is data collected in a physical space in the city, which includes:

- Public spaces, such as streets, squares, plazas, parks, and open spaces

- Private spaces accessible to the public, such as building lobbies, courtyards, ground-floor markets, and retail stores

- Private spaces not controlled by those who occupy them (e.g. apartment tenants)

Urban Data is different from other data and requires a different approach because:

- It could reasonably be considered a public asset.

- Individual consent is hard to achieve in public or publicly accessible spaces, unlike when individuals provide data in more traditional contexts.

- Existing requirements attached to the collection of Urban Data only apply when it is identifiable, and are often not followed; there are no requirements attached to the collection of Urban Data that is not personal information.

- The community has the right to expect reasonable protection and proper use of data collected in these spaces.

- Such data raises potential community surveillance concerns.

- Urban Data is anchored to geography, unlike data collected through websites and mobile phones, and lends itself to local governance.

HOW OUR FOCUS ON URBAN DATA REFLECTS WHAT WE'VE HEARD

It acknowledges the consent challenge involved with Urban Data and puts in place a mechanism to obtain "community consent" by:

- **Placing** governance and oversight in the hands of an independent entity that represents the community interest

- **Requiring** Privacy by Design

- **Providing** transparency for the community

- **Enlarging** the types of data that deserves protection beyond personal information to data that has the potential to impact people

- **Focusing** on the entire ecosystem in Quayside, enabling responsible data use and across the board privacy protections

DRAFT PROPOSALS

Proposal: Civic Data Trust

The Civic Data Trust will follow a clear and consistent process
that gives it oversight of Urban Data gathered in the public realm.

The Civic Data Trust will sit at the centre of a process established to ensure adherence to Responsible Data Use Guidelines

01	02	03	04	05	06
RDIA Filing	**Approval**	**Registry**	**Managing Access**	**Enforcement**	**Exemptions**
Before any collection and/or use of Urban Data can occur, a Responsible Data Impact Assessment (RDIA) must be conducted and filed with the Civic Data Trust, as part of an application to commence collection and/or use. *(See Section 3 for details)*	Many applications to the Civic Data Trust will be able to be self-certified, submitted, and advanced to the registration step. These will generally be applications for the collection of non-identifiable data that will be made freely and publicly available. Other applications will require substantive review by the Civic Data Trust. These may involve the collection of Urban Data that is identifiable or collection of Urban Data on a more proprietary basis.	Civic Data Trust will approve placement of devices used to collect Urban Data and maintain an online registry of RDIAs and map of device locations, with easily accessible information on what data is being collected, why, how, where, and by whom.	By default, non-personal Urban Data will be open and freely accessible to the public. In cases where Urban Data access is restricted, the Civic Data Trust will manage access to this data. This could be accomplished in a variety of ways, from having the Trust actually hold the data as a repository to having it set rules that require collectors to publish data in real time.	The Civic Data Trust retains the duty to audit all uses and remove digital devices in the event it discovers a violation. If the Civic Data Trust were to serve as a repository for data, it would have the ability to shut down access by bad actors. The question of more traditional enforcement authority needs to be considered as part of ongoing consultation.	The Civic Data Trust will have the authority to exempt from registration specific uses that, in its judgment, do not have implications for personal privacy by virtue of their limited technical capabilities, such as water-pressure sensors on building pipes or weight sensors in freight elevators. (The Trust will have no power to grant exemptions from existing privacy law.)

DRAFT PROPOSALS

Data Typologies

Depending on issues of place, context, and control, different
kinds of Urban Data merit different kinds of oversight.

	Governance Considerations	RDIA & Approval Process	Role of Data Trust
Urban Data Type 1 Collected in the public realm (e.g. pedestrian counters, street-facing cameras)	• Individuals have little control over collection of Urban Data in these spaces • This data could reasonably be considered a public asset and will therefore as a default be made freely and publicly available • Private control or collection of any data that is personally identifiable requires substantive review by Data Trust	• RDIA and applications to Data Trust are mandatory in all cases. • Applications to Data Trust can be self-certified if data is de-identified and freely and publicly available, and applicant does not seek proprietary control • Otherwise Data Trust substantively reviews applications • Existing requirements, including related to signage, in effect and subject to actual enforcement	• Receives applications and RDIAs • Reliably and speedily—potentially, automatically—approves accurate, self-certified applications • Substantively reviews applications that do not meet the requirements for self-certification • Registers placement and maintains a publicly available registry of devices and associated applications and RDIAs • Manages public availability and, where applicable, private access to various data streams
Urban Data Type 2 Collected in privately-owned but publicly accessible spaces Different classes within this type depending on the kind of space (e.g. cameras in large building lobby vs. a small store)	• Individuals have little control over collection of Urban Data in these spaces • Depending on the class (see next column), arguments for data as a public asset may be stronger or weaker • In any circumstance, the public has an interest in a fulsome understanding of data collection mechanisms	• RDIA and applications to Data Trust are mandatory in all cases. • Class A (e.g. camera in a large building lobby): Applications to Data Trust go through same process as Urban Data Type 1 • Class B (e.g. small café camera): All applications to Data Trust can be self-certified • Existing requirements, including related to signage, in effect and subject to actual enforcement	• Class A: Same as Urban Data Type 1. • Class B: 　○ Reliably and speedily—potentially, automatically—approves accurate, self-certified applications 　○ Registers placement and maintains a publicly available registry of devices and associated applications and RDIAs 　○ No substantive review 　○ No access management; data not made publicly available by default
Urban Data Type 3 Collected in fully private spaces, generally homes or offices (e.g. thermostats, home security cameras, sensors for building code compliance)	• Data cannot reasonably be considered a public asset • May be necessary to achieve community goals (e.g. temperature monitoring for energy demand management) • May have particular privacy implications because devices are in private spaces, and devices in tenant spaces raise consent issues	• Devices installed by residents in their private spaces would be entirely exempt from this regime • RDIA and applications to Data Trust are mandatory in all cases of devices installed by a landlord or builder • Parties can self-certify if they abide by Responsible Data Use Guidelines, provide full disclosure, and allow opt-out • Otherwise, Data Trust substantively reviews applications	• Reliably and speedily—potentially, automatically—approves accurate, self-certified applications • Substantively reviews applications that do not meet the requirements for self-certification • Registers placement and maintains a registry of devices and associated applications and RDIAs 　○ Open question regarding whether this registry should be made publicly available. • Audits de-identification and storage.
Traditionally Collected Data Involving Direct Consent (e.g. apps and websites)	• Issue that extends beyond Quayside • Harder to see this data as a public asset • Local, geographically-bound governance regime unworkable given the lack of a relationship between this kind of data collection and geography. • Sidewalk Labs will hold itself and its partners to high standards given the role it will play in this community	• RDIA is not required for third parties • Sidewalk Labs commits to filing RDIAs with the Data Trust so that they are publicly transparent	• Data Trust not involved, other than to receive and publish Sidewalk Labs RDIAs, as well as any voluntarily filed RDIAs; and to manage any voluntarily contributed data

DRAFT PROPOSALS

DRAFT PROPOSALS

All collection and use of Urban Data will require a Responsible Data Impact Assessment

All entities seeking to collect and/or use Urban Data in Quayside will submit Responsible Data Impact Assessments (RDIAs) as part of applications to the Civic Data Trust. The RDIA process will be a core tool for ensuring adherence to the community's Responsible Data Use Guidelines.

The RDIA is an assessment of the prospective use of data involved in an activity, including an analysis of whether the benefits of the activity outweighs the risks involved. It is a vehicle for assessing alignment with principles, legal requirements, and stakeholder expectations.

Responsible Data Impact Assessments are conducted at the design phase, prior to data collection or use.

The RDIA enables parties to make decisions in a consistent, transparent way— and to do so reasonably quickly.

Outcomes

- ✓ Qualitative + Quantitative evaluation
- ✓ Appropriate stakeholders are involved throughout the project
- ✓ Demonstrable accountability
- ✓ Transparent and proactive
- ✓ Ensures Privacy by Design from the design phase, not an afterthought
- ✓ Enables de-identification by default

RESPONSIBLE DATA IMPACT ASSESSMENT

1. **PURPOSE** of the project/product/service, who is involved and who is accountable

2. **DATA**: a full understanding of the data, sources, data use and parties involved

3. **IMPACT** on parties and, in particular, individuals

4. **ANALYZE** risks and benefits

PRIVACY IMPACT ASSESSMENT (IF APPLICABLE): If the project/product/ service involves the collection or use of Personal Information, a Privacy Impact Assessment is also required.

DECISION: Whether an appropriate balance of benefits and mitigated risks supports the data processing activity

DRAFT PROPOSALS

Responsible Data Impact Assessment Section 1: Purpose

Illustration of what the Assessment form might address.

SAMPLE RESPONSIBLE DATA IMPACT ASSESSMENT

Project Name/Description

Project Objective

What is the ultimate goal of this project?

If a pilot or partnership, what does it seek to demonstrate or achieve?

Does the activity fit within a larger theme of work that is currently being contemplated or undertaken?

Stakeholders

Who is collecting/using the data, and are the other stakeholders involved?

e.g. partners, vendors, customers, government, etc.

Note: This slide has been updated for clarity from the 10/15 version.

DRAFT PROPOSALS

Responsible Data Impact Assessment Section 2: Data

Illustration of what the Assessment form might address.

SIDE WALK LABS

SAMPLE RESPONSIBLE DATA IMPACT ASSESSMENT

Nature of Data

What specific types of data will be collected, tracked, transferred, used, stored or processed?

If project is at the concept stage, what data do you anticipate collecting or using?

Is the data about people, and if so, is it identifiable to a person or is it de-identified?
If Personal Information is collected, a Privacy Impact Assessment is also required

Is the data or anticipated use of the data sensitive?
Sensitive categories of data and/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, information or data that could be used to facilitate identity theft. A sensitive use of data may also be where there is a reasonable expectation the use of the data would be embarrassing or be considered sensitive to the individual whose data it is.

Sources of Data

Will data be provided by third parties?

Will data be collected by sensors? What type, and where are the sensors located?

Note: This slide has been updated for clarity from the 10/15 version.

DRAFT PROPOSALS

Responsible Data Impact Assessment Section 3: Impacts

Illustration of what the Assessment form might address.

SAMPLE RESPONSIBLE DATA IMPACT ASSESSMENT

Impact to Individuals and Groups

Identify all the parties impacted by this data activity, and the impacts it will have.

What are the stated and unstated expectations of individuals, groups of individuals, and society for each use of the data?

Benefits

What are the benefits to the individual or groups of individuals?

What are the benefits to society?

What are the benefits to other stakeholders?

Risks (Inherent)

Considering all the factors relating to the data, the likely data use, the identifiability and sensitivity of the data, what are the risks to the individual, groups of individuals, society?

Is it foreseeable that data use might seem surprising, inappropriate or discriminatory or might be considered offensive causing distress or humiliation?

Could the data be used in a way that may result in a group of individuals being treated differently from other groups of individuals?

Is the accuracy and/or quality of the data appropriate for the data activity? Does the relative accuracy of the data have an impact on individuals/groups?

Note: This slide has been updated for clarity from the 10/15 version.

Responsible Data Impact Assessment Section 4: Analysis

Illustration of what the Assessment form might address.

SAMPLE RESPONSIBLE DATA IMPACT ASSESSMENT

Mitigating Risks

What are the technical and procedural safeguards (mitigating controls) that are being implemented to prevent and mitigate risks described above should they occur (e.g. encryption and delinking of data or increased transparency)?

How have Privacy by Design control standards been applied?

Are you using analytical driven models, insights or algorithmic decision making, that could impact individuals?

Is there a less data intensive way to achieve the goals of the data activity (including potential insights)?

Decision Analysis

Is there a net benefit?

Are there any other factors that should be considered?

Does the data activity comply with all laws, cross-border, policy, contractual, industry or other obligations organizational policies and self-regulatory commitments?

Does the purpose of the activity fit within the values of society?

Have all the stakeholder concerns identified in the Governance of Data section been appropriately addressed?

Is their appropriate Notice, Consent and Control as part of the data collection and use?

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?

Note: This slide has been updated for clarity from the 10/15 version.

DRAFT PROPOSALS

DRAFT PROPOSALS

Hypothetical Case Study 01: Traffic Management System

Traffic management system in Quayside by Sidewalk Labs

Future hypothetical: Sidewalk Labs is working to implement a plan approved as part of the Master Innovation and Development Plan for a traffic management system in Quayside, which involves pedestrian counters and adaptive traffic lights.

APPLICATION 1
Pedestrian Counters

Sidewalk Labs submits an application and RDIA for pedestrian counters to the Data Trust. Because the data is non-identifiable and will be made freely and publicly available, it can be self-certified.

- **The Data Trust publishes the RDIA** and adds the locations where the pedestrian counters will be installed to its public registry.

- **The pedestrian counters are installed,** and the data from the counters is made freely and publicly available, and not owned by Sidewalk Labs.

- **Pedestrian count data is used** as part of the traffic management system.

- **The data is also accessed by a community group** to make the case for the need for a street redesign.

APPLICATION 2
Adaptive Traffic Lights

Sidewalk Labs submits an application and RDIA to deploy devices developed by a partner that use computer vision to compute de-identified paths and speeds of cars, cyclists, and pedestrians.

- **Depending on the policies of the Data Trust**, this application may:
  (1) be allowed to self-certify because the data is de-identified in real time; or
  (2) be subject to substantive review and, if real-time de-identification is confirmed, approved.

- **The Data Trust publishes the RDIA** and adds the locations where the adaptive traffic lights will be installed to its public registry.

- **The adaptive traffic lights are installed**, and the de-identified data feeds are made freely and publicly available, not owned by Sidewalk Labs.

- **That data is used** as part of the traffic management system.

- **The data is also accessed by another company** that believes it can process this data more effectively and produce better results.

DRAFT PROPOSALS

Hypothetical Case Study 02: Parks Improvement Study

Parks improvement study by a new third-party startup

SIDE WALK LABS

Future hypothetical: Startup A is working on a project to make recommendations about improving environmental conditions and usage patterns at several parks throughout the City, including one in Quayside. This hypothetical scenario involves both air quality sensors and video cameras in the park.

APPLICATION 1
Air Quality Sensors

Startup A submits an application and RDIA for air quality sensors to the Data Trust. Though the data is non-identifiable, Startup A will incur a substantial financial burden in installing the sensors and seeks to recoup its investment by selling the data to companies trying to reduce their negative environmental impacts. Startup A asserts that it will not move forward with this project if the data is made freely and publicly available from the start.

- **This application may not be self-certified** because Startup A seeks to maintain proprietary control of the data.

- **The Data Trust reviews the application, judges it to provide a net benefit to the public, and approves on the condition** that proceeds from the sale of the data will be shared between Startup A, the City, and the Data Trust.

- **The Data Trust publishes the RDIA** and adds the locations where the air quality sensors will be installed to its public registry.

- **The air quality sensors are easily installed** using open standards-based mounts, and access to the data is limited to Startup A.

- **After a time, the data is made freely and publicly available.** It is then accessed by a weather app providing air quality alerts that decides to start funding the ongoing operations and maintenance of the technology.

APPLICATION 2
Video Cameras

Startup A submits an application and RDIA for video cameras to capture usage patterns at the park in Quayside.

- **This application may not be self-certified** because it involves the collection of personal information.

- **The Data Trust reviews the application and approves on the condition** that the video footage will be used only for the purposes of the park improvement project, and will be destroyed on a rolling basis after seven days. Startup A must also, in accordance with existing requirements, prominently post signage around the cameras.

- **The Data Trust publishes the RDIA** and adds the locations of the cameras to its public registry.

- **The cameras are easily installed using open standards-based mounts**, and the footage is reviewed and then destroyed on a rolling basis, meeting the seven-day requirement.

DRAFT PROPOSALS

SIDE WALK LABS

DRAFT PROPOSALS

Quality of life comes first—no tech for tech's sake

This neighbourhood is not about technology for technology's sake.
We are focused on technological and urban design solutions to real problems.

RECAP

From the start of this project, we imagined a set of new experiences that could be possible in a new type of city.

Streets that prioritized safety, pedestrians, and cyclists, because they are designed to anticipate shared, self-driving vehicles that wouldn't need much parking and could communicate with each other and with traffic lights. This would mean significant amounts of street space given back to pedestrians and cyclists, less congestion, and far fewer accidents.

Buildings with a far more diverse and vibrant mix of uses as a result of "outcome-based code," which doesn't require uniformity of use but rather ensures structural integrity, air quality, and noise levels through conditions-sensing technology.

Significantly reduced carbon emissions achieved by technology that monitors and manages energy demand across the neighbourhood.

We have identified a set of innovations that could help improve urban life in Quayside. A non-exhaustive list:

Mobility	Traffic management technology and adaptive traffic lights to reduce congestion and increase safety.
Public Realm	Structural innovations to create active weather mitigation tools that can be deployed based on real-time hyperlocal measurements of rain and wind.
Sustainability	Energy demand management technology, thermal heating and cooling, and other innovations to push toward climate positivity.
Community	Engagement tools to provide informed input into neighbourhood decision making.
Buildings	Construction innovation to enable a mix of affordability levels and real-time monitoring of building conditions to enable a mix of uses.
Access + Equity	Truly ubiquitous connectivity and focused efforts to improve digital literacy to bridge the digital divide.
Accessibility	Tools to make the community more accessible, such as spoken information about the physical environment and sensors to detect snow in curb cuts.

DRAFT PROPOSALS

Sidewalk Labs will build solutions—but not exclusively

We have identified solutions we believe will help make this a great place for people to live, and we are committed to bringing those to life. But we will also encourage others to create better solutions—because we will never have all the best ideas.

AN EXAMPLE: ENERGY USE

One key approach to creating a climate-positive neighbourhood is to measure how energy is used and optimize it using machine learning. Sidewalk Labs will work with partners to develop technology to measure aggregated and de-identified energy use by systems including heating and cooling, apply algorithms to propose optimizations, and build control systems to implement those optimizations. Aggregated and de-identified energy use measurements would be considered Urban Data and will be made freely and publicly available by the Civic Data Trust in order to stimulate research and development of even better techniques by others.

To accomplish this, Sidewalk Labs will:

- Identify and deploy **devices from the market that measure energy use and environmental conditions**
- With local partners, develop and deploy a **ubiquitous network** to allow those measurements to be communicated in real time
- Design **standardized mounts** for light poles and buildings to reduce the cost of deploying network access points and devices
- Build a **digital map** of the neighbourhood—with an unprecedented level of accuracy
- Create an **open data hub** that will provide real-time access to data in standard formats through well-documented interfaces in order to make measurement data that goes to the Data Trust easily accessible

This will not be done to the exclusion of others. To the contrary, this place will be more successful when alternatives are encouraged:

- When better devices are developed, it should be **easy to replace Sidewalk Labs-developed technology**
- We expect and encourage **many network providers** to provide service in this neighbourhood
- Better approaches to deploying network access points and devices will be able to supplant ours
- The digital map will be created by broad collaboration and be made freely and publicly available to all by a Civic Data Trust
- There will likely be several data hubs, making it easy to understand and work with publicly available data

The same open approach will apply to solutions for **mobility**, **public realm**, **community**, **buildings**, **accessibility**, etc.

DRAFT PROPOSALS

Enabling innovation by a wide range of players

Designing technology to support our quality of life goals has revealed patterns: common pieces of infrastructure and specific services that are required to bootstrap digital innovation in the neighbourhood for Sidewalk Labs and others.

WHAT SIDEWALK LABS WILL BUILD

Taking the same approach to designing solutions for **sustainability**, **flexible public realm**, **community**, **buildings**, **accessibility**, etc. leads us to believe that we should create a new standard for digital infrastructure and services in cities, including:

- Ubiquitous connectivity
- Standardized mounts and power
- A high-resolution 3D map of the neighbourhood
- An open data hub which will provide real-time access to data in standard formats through well-documented interfaces

The fact that Sidewalk Labs is committing to build these components does not preclude others from deploying technology that improves on, competes with, or replaces them.

WHAT OTHERS WILL BUILD

The lion's share of technologies that make Quayside unique will be developed and deployed by an ecosystem of many innovators:

- Just as in the World Wide Web, multiple providers can coexist, and technological solutions can integrate, as long as they agree on standards

- Others should be welcome to provide better, different, cheaper infrastructure and services

- We hope that this will enable a wide range of Canadian startups to innovate more quickly, and use Quayside as a springboard to success

- All systems collecting or using Urban Data —whether created by Sidewalk or third parties—will be subject to Civic Data Trust governance

DRAFT PROPOSALS

Open architecture makes this possible

Sidewalk Labs will not create a centralized, monolithic platform. Rather, we will work with partners to create an open architecture—one that enables and encourages collaboration and experimentation.

In order for anyone to innovate, and have the opportunity to replace components that Sidewalk Labs and others build, there must be no proprietary lock-in. This requires:

- **Well-documented, standardized formats and interfaces**
    - Any party will have the information required to build a replacement component for any urban system, or to create an entirely new application.
- **Easy access to public-domain data**
    - Standards are worthless if it's not possible to get access to data. For example, devising a new optimization algorithm for traffic requires training and test data, so traffic volume data should be made broadly available.
- **Data portability**
    - An existing system will likely have access to historical data provided to it by neighbourhood systems. This data should be able to be exported from the existing system so that new systems are not at a disadvantage for training and bootstrapping.
    - This is similar to email systems that allow the user to export all of their historical email messages so that they can move to a new provider, eliminating lock-in.

DRAFT PROPOSALS

Urban Digital Architecture Sketch

Each function within the urban technology stack will be served by Sidewalk Labs and also by others. Interchangeability requires standardized interfaces and formats.

SIDEWALK LABS

Legend:
- Third Parties (blue)
- Sidewalk Labs (yellow)

Applications
- [Third Parties]
- [Third Parties]
- Energy Optimization
- [Third Parties]

STANDARDS

Data Sharing Portals
- [Third Parties]
- Open Data Hub
- [Third Parties]
- [Third Parties]

STANDARDS

Measurements and other data
- [Third Parties]
- High-Resolution Map
- Traffic Volume Sensors
- [Third Parties]

STANDARDS

Connectivity
- [Third Parties]
- [Third Parties]
- Ubiquitous Wi-Fi
- [Third Parties]

STANDARDS

Physical Mounts
- Standardized Mounts and Power
- [Third Parties]
- [Third Parties]
- [Third Parties]

DRAFT PROPOSALS

31

Example of an Open System: The World Wide Web

If urban technology used open standards in the same way that the World Wide Web does, innovation would explode, and the risk of vendor lock-in would be dramatically reduced.

You can use any browser...

to visit any web page...
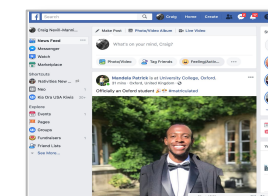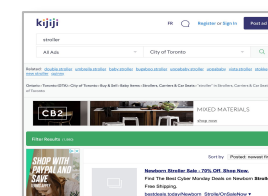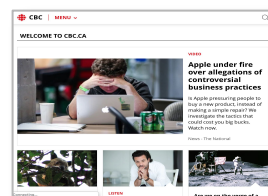
served by any web server.

Apache

NGINX

Microsoft IIS

LITESPEED

Example: World Wide Web Standards

Standards enable innovation and competition.

Formatting

Hypertext Markup Language (HTML),
Cascading Style Sheets (CSS)

Images

Portable Network Graphics (PNG),
Joint Photographic Experts Group (JPG)

Interactivity

JavaScript

Communication

HyperText Transfer Protocol (HTTP)

Security

Secure Sockets Layer (SSL)

Anyone can build a web browser as long as it implements standards like HTML, CSS, JavaScript, HTML and SSL. The most popular browsers are free, and their cores are open source.

Likewise, anyone can build a web server as long as they implement HTTP, SSL, etc. The most popular servers are free and open source.

With partners, we hope to significantly advance a competitive, innovative urban technology ecosystem by using, developing, and promulgating standards.

DRAFT PROPOSALS

DRAFT PROPOSALS

Ensuring the protection of data in accordance with Canadian Law does not require data localization

Canada and other places with leading data protection regimes have recognized the ineffectiveness of one-size-fits-all and/or technology-specific requirements, and the importance of context—that the best way to achieve data protection in any given context depends on the types of data, entities, and jurisdictions involved.

With specific exceptions, data localization is not presently a requirement of Canadian or Ontario law. In addition, data localization:

- Is not necessary to ensure that data that originates in Canada is handled in accordance with Canadian law with regard to privacy protections, which can be achieved through contractual and technical mechanisms

- Presents technical and operational obstacles, including access to redundant storage locations to ensure security and availability

- Increases costs, which may raise barriers to entry for less mature companies

- Runs counter to the way information travels across the internet, without regard to geographic boundaries

For these reasons, Sidewalk Labs does not believe that it is sensible to impose a data localization requirement for innovators in Quayside.

Sidewalk agrees with the position of the Business Council of Canada, as expressed in its September 2018 Report on the Data Economy

" *Individuals and businesses should be free to transfer data across provincial and international borders, provided appropriate safeguards are in place.* "

" *There should be a general presumption against local data storage and processing requirements. Governments may need to exercise sovereignty over data flows in rare cases when it is necessary to protect the public interest.* "

DRAFT PROPOSALS

DRAFT PROPOSALS

In summary: our proposed approach

Robust governance, an open system, and protection of data.

Establishment of a Data Trust: Sidewalk proposes the establishment of an independent Civic Data Trust, which would approve and control the collection of, manage access to, and potentially store data collected in the physical environment, known as "Urban Data."

Data Trust to Make Urban Data Freely and Publicly Available: As a default, the Data Trust would make de-identified Urban Data freely and publicly accessible, eliminating the concept of data ownership. Specific approval by the Data Trust would be required for entities to collect Urban Data with personally identifying information (such as CCTV cameras) or Urban Data collected on a more proprietary basis.

Responsible Data Impact Assessments: Responsible Data Impact Assessments (RDIAs) would be used to ensure Privacy By Design and adherence to Responsible Data Use Guidelines in every part of the project and all collection of Urban Data, whether by Sidewalk or other parties. RDIAs would be filed with the Data Trust before the collection and/or use of any Urban Data within the project geography by any entity.

RDIAs and Registry of Devices Maintained by the Data Trust: RDIAs, along with a registry of devices collecting Urban Data, would be maintained and made publicly available by the Data Trust.

An Ecosystem of Technologies by Many Innovators: Sidewalk anticipates providing specific pieces of critical digital infrastructure and specific, use-case-driven technologies to achieve quality-of-life goals. All technologies provided by Sidewalk will be based on open standards, making it easy for the lion's share of technology in the neighbourhood to be provided by others.

Data Always Handled in Accordance with Canadian Law: To ensure that Canadian law and values are applied to data, Sidewalk Labs will use a toolbox of mechanisms, including contractual protections, technical protections, and edge computing, where data is processed on-device and not transferred to a central server. Sidewalk does not propose a data localization requirement specific to Quayside.

How our thinking addresses key questions.

Confusion about Sidewalk Labs' plans related to data, exacerbated by the time it's taken to work through complicated issues

We hope that these proposals have provided some clarity on how we are approaching a range of critical issues—all subject to your feedback and ongoing consultation.

Concern that data monetization is a key part of Sidewalk Labs' business model

It is not, and the governance of the Civic Data Trust is intended to ensure that no private entity can gain unfettered access to and ownership of data collected in Quayside.

Is Sidewalk Labs, and this project, intended to be a data source for Google?	No (see p. 4)
How will data—particularly data collected in the physical environment, which some argue should be considered a public asset—be protected and governed?	By an Independent Civic Data Trust, using Responsible Data Impact Assessments to promote the beneficial use of data and transparency (see p. 13)
Who will own and control the data that originates in Quayside's physical environment?	The concept of ownership will not apply to Urban Data in most cases, with the Data Trust making de-identified data freely and publicly available as a default matter and/or controlling access. Data will be under the control of another entity only in select cases, which will be determined once an RDIA has been submitted and the Trust has examined the public benefits involved. (see p. 13)
How do we address the difficulty of obtaining consent when collecting data in the physical environment?	By implementing a robust form of community consent represented by the Civic Data Trust (see p. 14)
What are the respective roles of Sidewalk Labs, other private sector players, and governments, when it comes to data and technology?	• Sidewalk provides some critical infrastructure and core services (see pp. 27-29) • Other players provide the lion's share of technology (see pp. 29-33) • Governments enforce privacy laws (see pp. 10, 13) • Data governance provided independently by the Data Trust, which may involve government in its establishment or ongoing work (see p. 13)
How do we ensure all innovators, including Sidewalk Labs, will be on equal footing in Quayside?	Through open standards; a limited, catalyzing role for Sidewalk Labs; and a governance model that applies equally to all players (see p. 30)
How do we make sure the protections of Canadian law apply to all data originating in Quayside?	We can ensure that data will always be handled in accordance with the laws of Canada without a data localization requirement (see p. 35)

DRAFT PROPOSALS

DRAFT PROPOSALS

Some of our open questions

In addition to seeking general feedback on this presentation
from the DSAP, a number of specific questions are on our minds.

1. **What needs to be added** to the Responsible Data Use Guidelines to avoid vendor lock-in?
   Are there other additions or edits to consider for the Guidelines?

2. **How should a Civic Data Trust** with the broad authority we propose be established? Can it be established by contract?
   Can it be achieved through standards imposed by Waterfront Toronto? Or does it require legislation?

3. **What should the structure**, staffing, and, if pertinent, board composition of the Civic Data Trust look like?

4. **Should the Civic Data Trust** act as a repository for data? Is this necessary,
   and what are the upsides and challenges attendant to that responsibility?

5. **What will be involved** in getting the Civic Data Trust up and running, and how will this be funded? How will ongoing operations of the Civic Data Trust be
   funded? Should the Civic Data Trust have the authority to charge for access to certain kinds of data? How would that relate to the goal of making data freely
   and publicly accessible?

6. **Should the Trust** carry liability related to the improper collection or use of data under its jurisdiction?

7. **Are the typologies of Urban Data** well-crafted and have we drawn the lines between self-certification and substantive review in the right places?

8. **What are the mechanisms** and who will be responsible for enforcement?

9. **How can we best encourage** use of open standards?

DRAFT PROPOSALS