

DATA GOVERNANCE FOR SHARING SMART CITY DATA: LESSONS FROM SIDEWALK TORONTO

TERESA SCASSA

CANADA RESEARCH CHAIR IN INFORMATION LAW AND POLICY, UNIVERSITY OF
OTTAWA

SEPTEMBER 25, 2019

APPROACH

- Quick overview of Sidewalk Toronto Project (with data emphasis)
- How responding to public/stakeholder feedback shaped data governance framework
- Data 'ownership'
- Urban Data
- Urban Data Trust
- Lessons from Sidewalk Toronto

THE PARTICULAR CHARACTER OF THE PROPOSED SIDEWALK TORONTO DEVELOPMENT

- Vocabulary issues: Quayside/Sidewalk Toronto/IDEA District/Smart City/Innovation Hub
- Distinguishing ST from Montreal, Barcelona, etc.
 - Waterfront Toronto:
 - Non-profit corporation created by 3 levels of government
 - Mandate with respect to development of Toronto port lands
 - “to deliver a connected waterfront that belongs to everyone, serving as a leading example of innovation and excellence in urban design, a magnet for investment and job creation, and a source of pride and inspiration for Canadians.” (Waterfront Toronto, “Note to Reader: Waterfront Toronto’s Guide to reading the draft Master Innovation and Development Plan proposal submitted by Sidewalk Labs”, June 28, 2019, at p. 3, available at: https://quaysideto.ca/wp-content/uploads/2019/06/Note-to-Reader_June-28-2019_Waterfront-Toronto.pdf)

TIMELINE

- RFP – March 17, 2017
- Sidewalk Labs' proposal selected – May 2017
- Plan Development Agreement (SWL) – July 31, 2018
- Master Innovation and Development Plan (MIDP) (SWL) – June 2019 (made public on June 24, 2019)
- Public Consultation (WFT) – Report published September 2019
- Six month extension to PDA (until March 31, 2020), with an early termination date if no agreement can be reached on key issues of October 31, 2019

KEY POINTS OF CONCERN (ABOUT DATA) PRIOR TO THE MIDP THAT SHAPED THE DATA GOVERNANCE MODEL

1. Data sharing and access
2. Participation in data collection
3. Risks to privacy and other values
4. Data localization

DATA SHARING AND ACCESS

- Local tech developers complained of being excluded from opportunities to develop smart city technology in Toronto
- Complex and multi-faceted concerns included issues around access to data
- Sharing smart city data could raise issues of privacy and ethical data use; questions were raised about nature and extent of 'openness' and how it aligned with the public interest
- *Sidewalk Labs initial assurances that data would be open were later modified with the idea of a data trust to oversee data sharing*

PARTICIPATION IN DATA COLLECTION

- Developers did not want to be excluded from creating and deploying the technologies to collect data within the smart city
- *Sidewalk could make commitments about its own practices regarding data sharing, deidentification at source, or privacy by design; it was more difficult for it to do so for other organizations*
- *So compliance with data governance scheme became a precondition for participation in the data ecosystem – including for access to and use of data*

RISKS TO PRIVACY AND OTHER VALUES

- There was considerable opposition to the project due to concerns over privacy risks, as well as concerns about discrimination, profiling and other harmful uses of data
- PbD approach adopted by Sidewalk Labs from outset, including deidentification at source did not satisfy critics
- *Urban Data Trust and Responsible Data Use Framework were proposed as a mechanism to oversee collection and use of data*
- *Note the shifting of these core issues to “independent” governance body*

DATA LOCALIZATION

- There was considerable opposition to the idea that data collected in the Sidewalk Toronto development might be stored outside of Canada
- On one level this is a privacy issue (e.g. PATRIOT Act concerns)
- On another level, it is a data sovereignty/data ownership issue

- *Sidewalk Labs eventually agreed that all data should be stored in Canada; later changed this to indicate it was only to the extent possible*

THE ELEPHANT IN THE ROOM: DATA OWNERSHIP

- The 'owner' (custodian?) of data is primarily responsible for governance
- Who 'owns' the data from the Quayside development?
- Public or private sector data?
- Public/private boundaries in real estate development and the implications for data 'ownership'
- Are there competing claims/interests in some forms of urban data? If so, who mediates these claims and how?

PUBLIC AND PRIVATE SECTOR DATA

- Data governance frameworks in Canada are based on distinctions between public and private sector data
- Different rules apply with respect to access, transparency, privacy
- Also with respect to “ownership”, custody or control

- “Urban data” relies on some form of ‘communal’ ownership
- Urban data trust negates the role of the public sector, although MIDP does suggest that it might eventually be taken over by the public sector

“URBAN DATA”

- MIDP: “information gathered in the city’s physical environment, including *the public realm, publicly accessible spaces, and even some private buildings*”
- Can be person or non-personal data, and can include aggregate and de-identified data
- Definition avoids traditional approach of distinguishing between public and private sector data in order to determine appropriate governance framework
- “Who collects the data” is replaced by “where the data is collected”

“URBAN DATA”

- Urban data is distinguished from transaction data:
- “For clarity, we call the original information collected in a physical place in the city “urban data.” Urban data is different from data created when individuals agree to provide information through a website, mobile phone, or paper document. It presents unique challenges, including that it could reasonably be considered a public asset, and that it raises potential concerns around surveillance and privacy.”

“URBAN DATA”

- “Urban data” has a clear relationship to “a specific geography”, which transaction data lacks
 - But consider Uber sensor data v. Uber transaction data, or smart water meter data v. municipal water transaction data

“URBAN DATA”

1. It is defined based upon where it is collected (i.e. location is a key element in the definition of urban data);
2. The “where” is linked to some concept of shared or communal space;
3. Shared or communal space can cut across the boundaries of publicly and privately-owned spaces;
4. Urban data may include personal information and/or human behavioural data, as well as other types of non-personal data;
5. Urban data is not defined by who is collecting it (i.e. it can be collected by public or private sector actors and possibly even by individuals).

URBAN DATA

- Critique of 'urban data'
 - Much urban data is actually already public sector data; should goal be to ensure that as much as possible remains public sector data?
 - Regulating data collected in public space raises freedom of expression issues
 - Concept of 'urban data' disrupts public/private sector data governance frameworks
 - Urban data is earmarked for management by the trust; which prioritizes data sharing – why is sharing and not privacy the default approach for some forms of urban data?

URBAN DATA AND THE URBAN DATA TRUST

- “No one has a right to own information collected from Quayside’s physical environment – including Sidewalk Labs” (A. Harvey-Dawson)
- Urban data is a “community or collective asset” (MIDP)
- “If no one owns urban data, the question remains: Who manages it in the public interest?” (A. Harvey-Dawson)

THE URBAN DATA TRUST (UDT)

- Vocabulary issues: data trust, civic data trust, urban data trust
- UDT designed to govern urban data by:
 - Controlling who is entitled to collect the data, and under what terms and conditions
 - Determining the terms and conditions for data sharing
- Responsible Data Use Agreement is used as a combined application form and ethics approval request that must be filed prior to collecting data, or when seeking permission to access and use data
- Any sensors would have to be mapped and registered with UDT's public sensor registry

THE UDT

- UDT would be a non-profit independent of Sidewalk Labs and Waterfront Toronto
- Not a 'trust' in true legal sense; not a 'civic trust'
 - 5 members (at least initially)
 - Representatives are:
 - Expert on data governance and legal issues
 - Academic
 - Public sector
 - Private sector
 - community

THE URBAN DATA TRUST (UDT)

- Principles
 - Data open by default, although access conditions may be imposed
 - Data collection and use administration fee part of each RDUA process to offset costs of UDT
- Enforcement
 - UDT has authority to audit (presumably under terms of agreements), to remove sensors in cases of non-compliance, and to seek legal remedies for breach of conditions

THE UDT

- Puts private sector and public sector actors on equal footing with respect to collection and use of data
- No exceptions for particular types or categories of data collectors
- No clear framework for transparency, accountability, governance
- No clear powers of enforcement/oversight

- Raises serious issues about: defining and protecting public interest; representativeness; clash with public sector; civil liberties; legitimacy

LESSONS FROM SIDEWALK TORONTO

- I. What is appropriate nature and source of community consent/acceptance
 - For project
 - For data collection/use
 - For data governance entity
2. The public sector is not irrelevant or passé
 1. For enacting laws and regulations
 2. For setting the normative framework for projects and ensuring transparency and oversight
 3. For taking on data governance in the public interest

THANK YOU!

- tscassa@uottawa.ca
- <http://www.teresascassa.ca>
- @TeresaScassa