The new social contract: What's our privacy worth?

February 07, 2020

As new models of the smart city emerge around the world, established social contracts are being challenged by new concerns around the ownership of data. How do we weigh the worth of an individual citizen's privacy against the collective benefits of open data availability?

The first half of the decade saw major cities establish open data laws and guidelines to promote sharing, yet some smart city projects generated headline-grabbing controversies over data misuse and a lack of transparency. This, in turn, mobilized citizens and civil society organizations around issues of data privacy and cybersecurity.

Governance models and their legal structure are crucial to ensuring accountable, secure and transparent data regimes. In essence, these models will dictate what bodies are directly responsible for managing streams of data, deciding who is permitted access, overseeing dispute resolution mechanisms, and, when applicable, levying a fee for the data's use in commercial contexts.

BLG's Smart Cities round table explored the issue of Canadian municipalities' governance models. Here, we look at how three leading cities around the world are addressing that challenge in different ways.

City of London: Holding it in trust

The Smarter London Together Roadmap, which aims to make the U.K. capital "the smartest city in the world," identifies a new "data deal" as one of its five core priorities. Along with developing a city-wide cybersecurity strategy and establishing a London Office for Data Analytics (LODA) to facilitate increased data sharing and collaboration to improve service delivery, the roadmap underlines the necessity of strengthening citizens' data and privacy rights and decides on the best governance models for how that data is managed.

In collaboration with the Open Data Institute — a non-profit co-founded by Sir Tim Berners-Lee, the computer engineer credited with inventing the World Wide Web — the City of London has been testing the data trust, a model at the forefront of these conversations. Borrowing from the concept of the legal trust, a data trust is a legal

structure that provides an independent stewardship of data, thereby taking it out of the hands of either government or private corporations and empowering its trustees to make decisions about how the data can be used or shared for an agreed purpose. In this case, the trust does not own the data, but rather holds the license to it, and follows or enforces strict guidelines regarding its use established by its own charter.

One of the London case studies, carried out in the Borough of Greenwich, considered the applicability of the data trust in the context of two real-time city infrastructure scenarios — parking use patterns in the borough and heating usage within a council-owned housing block. In each scenario, the collection of data through IoT sensors was oriented toward addressing a challenge the city faces. With parking use patterns it was with an eye toward enhancing infrastructure for electric vehicles; at the housing block it was about improving energy efficiency. But the common goal in both cases was to explore whether a data trust was the best means of administering the collected data and making it available to developers in the tech sector who might be in a position to contribute solutions.

Another of the ODI's pilots considered food waste, and whether a data trust model could support "global food waste reduction efforts by improving the ability of stakeholders to track and measure food waste within supply chains." In this case, the data trust would operate in the context of business-to-business data sharing.

The ODI's report on data trusts, issued in April 2019, confirms many of the model's benefits in facilitating reliable and transparent data sharing among a variety of potential stakeholders, including municipalities, businesses, AI developers and academics. It further argues that the pro-social nature of data trusts can help ensure that the benefits of data sharing are ultimately spread more evenly across society, while also helping to create a more efficient and centralized system for handling data requests.

When it came to the Greenwich pilot projects, the report's findings were inconclusive, saying it wasn't yet clear in the specific "use-cases explored that a data trust would improve the outcomes that the organizations are looking to achieve. The [current] design of the data-sharing arrangements, although they are in many cases still at an early stage, seems sufficient to enable the sharing of the data and gain the insight necessary." As the report advises, creating a data trust requires the infrastructure cost of managing it. Given the relative scale and scope of the data collected and the degree of its impact on privacy issues, it may not be the best model in every instance.

In examining the best legal structure for a data trust in the U.K. context, the ODI report recommends the independent corporation take the form of a Community Interest Company guided by a pro-social mandate.

> *"It will thus have built into it provisions requiring the promotion of the ethical sharing of data for a broadly public benefit… Data would be licensed to the trust, as data is not a physical asset capable of being donated, and the licence can contain terms of how the data should be used. The license could also provide the means by which data providers are paid (if appropriate) for the use of their data. Governance would be conducted by a board managing the day-to-day operation of the data trust, with key shareholding stakeholders meeting less frequently to vote on more significant matters. Any disputes would be resolved by a dispute resolution board and termination of the data trust would be carried out by*

cancelling the licenses and liquidating the company in the normal manner for a CIC."

Amsterdam: Clarifying priorities

To communicate privacy principles more tangibly to the general public, the Amsterdam Economic Board developed the TADA manifesto, an appealingly-branded vision for responsible use of data in digital cities. The manifesto was developed in 2017 by a working group of citizens, government, NGOs and businesses.

The TADA manifesto outlines six abstract principles that cover aspects such as the right to be forgotten and who maintains decision-making control over data use. As well as the city's own Smart City working groups and stakeholders, other government authorities, organizations, entrepreneurs and citizens have been encouraged to sign on to the manifesto. The manifesto is not binding in any way, though the "TADA!" label can be applied to initiatives that adhere to the manifesto.

1. **Inclusive.** "Our digital city is inclusive. We take into account the differences between individuals and groups, without losing sight of equality."
2. **Control.** "Data and technology should contribute to the freedom of people. Data are meant to serve the people. To be used as seen fit by people to benefit their lives, to gather information, develop knowledge, find room to organise themselves. People stay in control over their data."
3. **Tailored 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. **Legitimate and monitored.** "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 process and the resulting social consequences."
5. **Open and transparent.** "What types of data are collected? For what purpose? And what are the outcomes and results? We are always transparent about those aspects."
6. **From everyone - for everyone.** "Data that government authorities, companies and other organizations generate from the city and collect about the city are held in common. Everyone can use them. Everyone can benefit from them. We make mutual agreements about this."

A manifesto, however, is not a binding policy—it is a framework of beliefs. Many other cities, particularly in the first half of the decade, developed manifestos and statements of principles that promise to develop data and privacy policies at a later date. Mark Crooymans, Amsterdam's Director of Urban Services and Information, wrote in August 2019 that the key to TADA's success is that the principles are backed by implementation methodologies.

"That approach is very inviting, making it easy to transpose it into your own day-to-day operations," he wrote. "It's allowed to be a process that you're figuring out as you go along, not something that's either right or wrong."

In the city's first formal Agenda for the Digital City, released in April 2019, the TADA principles lay at the foundation of a roadmap for digital governance with privacy at its core. "The City of Amsterdam stands for the digital freedoms and rights of the people of Amsterdam," the agenda reads. "If these rights are not protected, there can be no free city. This means that we have to make technology human again."

The Agenda promises the near-future addition of data ownership clauses in procurement terms and conditions. It also looks to examples such as Estonia's ambitious but already implemented X-Road, a blockchain-backed platform which sits as a transparent interoperability layer behind public and private sector information services across the country, transparently encrypting data and ensuring granular citizen-level control over ownership of the data itself. Concurrent with this agenda, Amsterdam launched the Cities Coalition for Digital Rights in conjunction with Barcelona and New York City.

New York: An exercise in algorithmic accountability

A significant concern amongst North American constituencies has been the reliance on data-driven algorithms using historic and open data to make predictive decisions on future behaviours. This has led to problematic planning outcomes and potential algorithmic bias in policing or welfare policy.

In 2018, New York City passed an "algorithmic accountability bill," of which the chair of the committee driving it said, "If we're going to be governed by machines and algorithms and data, well, they better be transparent." In announcing the establishment of the Automated Decision Systems Task Force mandated by this legislation, Mayor Bill de Blasio said, "As data and technology become more central to the work of city government, the algorithms we use to aid decision making must be aligned with our goals and values."

This work added to the previous establishment by the city in 2016 of agreed guidelines for deployment of Internet of Things devices. Thirty-five cities in 11 countries have subsequently signed on to use these guidelines as a framework for their own deployments.

Though the bill initially required that public and private organizations disclose the source code of any software used by the city to the public for open scrutiny, resistance from both technology companies and the NYPD have seen this mandate somewhat softened.

The Automated Decision Systems Task Force convened two public meetings during 2019 on the themes of Transparency, and Fairness and Accountability. Experts are skeptical as to what it may realistically deliver, but as Julia Powles wrote in The New Yorker:

> *Whatever the new law's inadequacies, many of the people I spoke with saw it as an opportunity for greater engagement on important questions. "Think of this bill as an experiment in the world of algorithmic accountability, sent out much like Captain Picard, from 'Star Trek,' would send out a probe to explore a wormhole," Cathy O'Neil, the author of "Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy," told me. "What we're finding is*

that the world of algorithms is one ugly wormhole." In insulating algorithms and their creators from public scrutiny, rather than responding to civic concerns about bias and discrimination, the existing system "propagates the myth that those algorithms are objective and fair," O'Neil said. "There's no reason to believe either."

Expertise

Cybersecurity, Privacy & Data Protection, Compliance with Privacy & Data Protection, Municipal & Land Use Planning, Government & Public Sector, Online Retail & E-commerce

---

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.