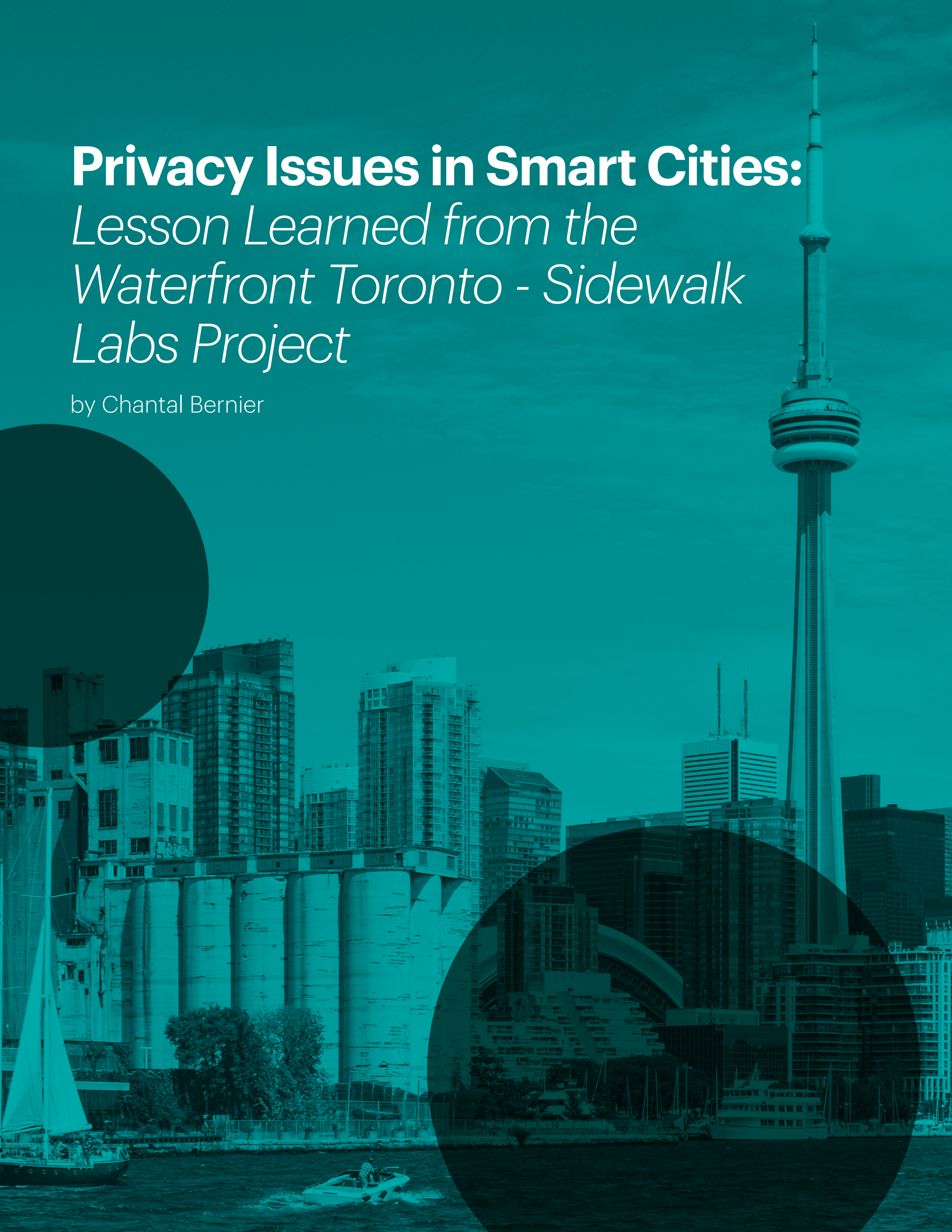
Privacy Issues in Smart Cities: *Lesson Learned from the Waterfront Toronto - Sidewalk Labs Project*

by Chantal Bernier



Dentons has had the privilege to act as privacy counsel to Waterfront Toronto in the development of the smart community Quayside project with Sidewalk Labs. The experience made clear that no smart city can proceed without social license and that there is no social license without addressing privacy risks.

Risk #1: Surveillance both from the State and surveillance capitalism.

Digital solutions generally create the risk of law enforcement access to the data they collect. Risk mitigation includes publicly available guidelines to assess law enforcement agencies' access requests and public transparency reports on how many requests were received, granted or rejected.

Capitalist surveillance particularly arose around the Quayside project because of the link to Alphabet and Google. This must be addressed with procurement contract terms restricting the use of the personal data.

Risk #2: Collection without valid consent.

Smart cities digital solutions often collect data without consent. To respect the right to privacy, this must be restricted to public sector digital solutions that are demonstrably necessary and private sector solutions with a reasonable business purpose and prominent signage. Otherwise, the collection must be optional, for example through an app.

There is no social license without addressing privacy risks.

Risk # 3: Excessive collection of personal data.

The breadth of personal data collection in digital solutions in smart city projects makes it difficult to contain it to what is necessary for specific purposes. To address this risk, Sidewalk Labs had proposed privacy protective technology that "locked" personal data into specific purposes and retention times.

Risk #4: Data breach.

Through intensive public consultations by Waterfront Toronto, we heard the acute concern about data breach. Barcelona, to name one smart city, chose block chain to secure its digital solutions and reassure citizens.

Risk # 5: Data Monetization.

Akin to the issue of surveillance capitalism, the P3 structure generally supporting smart cities creates concerns that the private partner may monetize the personal data collected through the digital solutions. This must be addressed through the procurement contract.

Risk #6: Lack of anonymity for differently abled persons

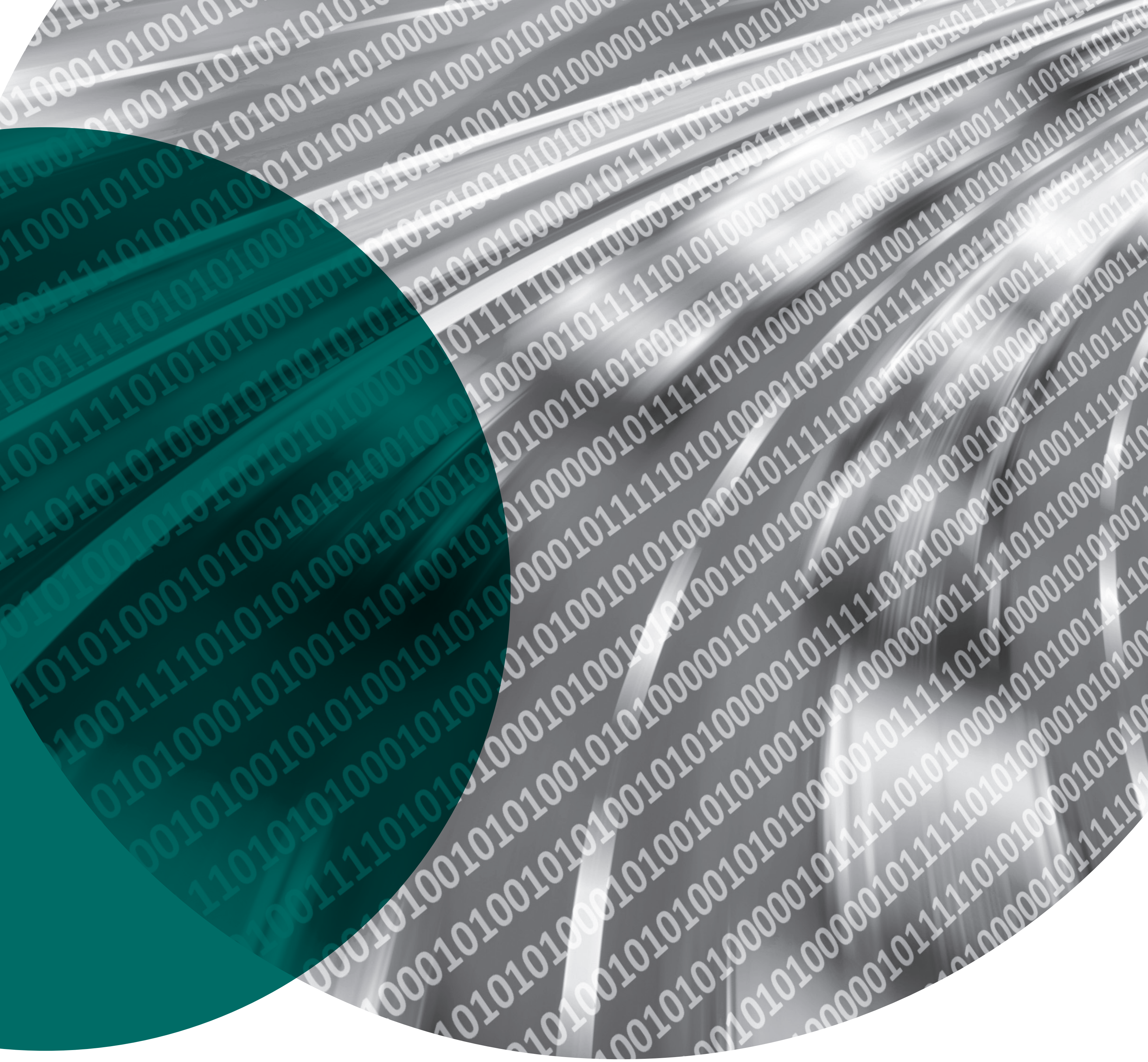
Waterfront Toronto had the wisdom of consulting differently abled persons. In relation to privacy, they made us realise how a solution that may appear anonymous – for example, one that only captures movement in a residential building – may actually be identifying for the one person who moves differently. The privacy lens in a smart community must reflect varied experiences.

Risk #7: Loss of data sovereignty

With some exceptions, Canadian privacy law does not prohibit cross border data transfers. In the Quayside project, however, the idea that a city's data, through a foreign private partner, would be hosted in a foreign jurisdiction under different privacy laws was identified as a significant privacy risk. Mitigation meant requiring storing personal data in Canada.

In short, as privacy counsel, we learned how pivotal privacy is in realizing a smart city project and how integrating privacy to a smart city opens up its extraordinary potential.

This article also appeared on the Dentons Privacy and Cybersecurity Law blog. To view this and other posts and articles, please visit http://www.privacyandcybersecuritylaw.com/privacy-issues-in-smart-cities-lessons-learned-from-the-waterfront-toronto-sidewalks-project/



Chantal Bernier leads Dentons' Canadian Privacy and Cybersecurity practice group, and also is a member of the Firm's Government Affairs and Public Policy group. Before joining Dentons, Chantal spent six years at the helm of the Office of the Privacy Commissioner of Canada (OPC), where she led national and international privacy investigations in the public and private sectors, as well privacy audits, privacy impact assessment reviews, technological analysis, and privacy policy development and research. She advises leading-edge national and international companies as they expand into Canada and Europe, enter the e-commerce space, adopt data analytics and roll out data-based market initiatives. Her clients include ad tech companies, financial institutions, biotech companies, data analytics firms and government institutions.