By Emily McClendon and Adrienne Atherton
Civic Legal, LLP

CASE of INTEREST

Smart Cities – They're Watching You

Smart Cities use integrated data collection and management to track and analyze the patterns of a community to drive and power services. Some examples include pedestrian traffic sensors, mobile apps for buses and expedited handling of requests for city services. However, innovation inevitably comes with uncertainties and risks. While there is a public appetite for the convenience that technology provides, enthusiasm is tempered by the public's concerns about privacy and cybersecurity risks, as is demonstrated by the recent news reports of the privacy controversy surrounding Toronto's new Alphabet Company (aka Google) operated Waterfront development.

At first blush, one could believe that there is no expectation of privacy in relation to data collected from public spaces. However, in *R. v. Jarvis*, 2019 SCC 10, the Supreme Court of Canada affirmed that there is a reasonable expectation of privacy in relation to the recording of data from a public place. In the *Jarvis* case, a school teacher recorded the chests of female students in public areas of the school with a hidden camera. In defense to the criminal charge of voyeurism, Jarvis argued that, because the students were already under the school system's surveillance, they had no reasonable expectation of privacy. The Supreme Court of Canada disagreed and held that "being in a public or semi-public space does not automatically negate all expectations of privacy with respect to observation and recording." This ruling clarified that privacy expectations of casual observance may be much different than focused and permanent visual recordings.

In addition to common law principles, local governments must comply with the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA). The *Personal Information Protection and Electronic Documents Act* (PIPEDA) plays a corresponding role in the private sector. Depending on the Smart City data collected and how it is used (e.g. if the private sector is using data collected by local government), either or both FIPP and PIPEDA could apply to protect personal information. For Smart Cities, there are certain key issues that should be considered.

1. **Purpose of Collection**: Information collected must relate directly to and be necessary for a program or activity of the public body (s. 26 of FIPPA). This means that a local government should avoid collecting more personal information than is needed for the intended purpose.
2. **Consent**: Public bodies must obtain informed consent to access websites or applications that track the user's data, and provide notice of surveillance or tracking. In a public area that is being surveilled, effective notice should include large signs around the perimeter of the area being surveilled advising:
   a. that accessing the area implies consent to data collection;
   b. to whom the collected information may be disclosed; and
   c. that collection is authorized under FIPPA.
3. **Use of Data**: The use of personal information by a public body is limited to the purpose for which a) it was collected and b) the individual affected has consented (s. 32 of FIPPA). Having a policy that sets out appropriate retention times for data collected could reduce the risk that data may be misused.
4. **Third Party Use of Data**: If collected information is supplied to a third party, the identifying information should be stripped out to the extent possible, including blurring out third parties' faces or blacking out areas not intended to be included in the surveillance.
5. **Unintentional Disclosure of Data**: A disclosure of information contrary to FIPPA is an offence, which can result in fines or imprisonment. In the event of an unintentional disclosure or cybersecurity event, section 30.5 of FIPPA requires the 'head' (which for local governments is the Council or Board, or their delegates) to be immediately notified. Pursuant to sections 73.1 and 73.2 of FIPAA, the 'head' can take steps to recover personal information that was improperly disclosed.

The privacy issues and risks surrounding Smart Cities are complex. With facial recognition systems and pattern recognition software that can manipulate vast streams of images, the collection and actual uses of data are increasing over previously human-only collection and use.

There is much opportunity in the development of Smart City technology. However, local governments would be 'smart' to ensure that progress is achieved in a way that properly protects privacy.