Explainer: Location Data

Knowing where a person is, has been, or is likely to be has value for a range of private and public sector actors including marketers, telecommunications companies, city planners, policing bodies, and public health officials. This value may be commercial or social, or a mixture of both, depending on how location data is being collected, who wants it, and for what purpose. Increasingly, private sector and public sector distinctions, so important under privacy law, are blurring in the real world as public bodies seek to purchase data collected by the private sector or partner with private sector entities. This creates a range of privacy issues for the individuals whose data is at stake.

Location data is increasingly easy to collect, and is collected, from the cellphones many of us carry about in our pockets or purses. A widening range of applications take advantage of the built-in GPS, WiFi and Bluetooth tools to figure out where we are at any moment. However, precisely because it is readily collectable on an ongoing basis in real time, location data permits comprehensive mapping of our movements through the physical landscape between places that are part of our lives, from home to work, to grandma's house, to the grocery store, to place of worship, to medical clinics and so on. This information can reveal details specific to an individual's behavior, associations, religious faith, and health that are personal and sensitive.

There are many uses of location data that have become commonplace. Examples include:

- Mapping applications use smartphone GPS data to estimate traffic congestion and calculate travel times.
- Fitness applications use smartphone GPS data to help individuals track distance and speed while running, cycling, or walking.
- Social networking sites allow users to "check in" by sharing location data, and provide platforms for application programming interfaces (APIs) so that developers are able to build products to interface with their sites and their users data.
- Bricks and mortar stores may use the signals your phone sends out to detect WiFi and Bluetooth connections around you to track your location via the unique identifier number (the Media Access Control or "MAC" address) of your device. This information may be easily linkable to your name, address, etc. and may be used subsequently to advertise to you online based on stores you have visited or even products you spent a long time looking at in a store.

Often the only notification individuals have for such collection is a vague reference to the possibility of such collection buried in a long terms of use or privacy policy. This is problematic both because consumers rarely read such policies, and when they do, the policies are often written in such a way that it is difficult to determine what information is actually being collected or how it is being used and/or shared. In other words, even when consumers consent to location data collection, the consent is often not meaningful. And the consumer rarely has more than minimal control or bargaining power when dealing with entities that collect, use or disclose data

When it comes to location data, research suggests that there is no evidence to support the claim that effective anonymization is possible. In an often-cited study, MIT researchers, for example, reported that using two large anonymized data sets, one from a mobile network operator and one containing data about personal transportation, they could match 17% of data subjects with a week's worth of data, and more than 55% using a month's worth of data. They estimated that combining these datasets with GPS traces would allow them to match 95% of individual trajectories with less than a week's worth of data.[i] Given this predictable risk, location data should be considered sensitive and treated accordingly.

Public private partnerships and privacy law regarding location data

Private sector: Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to the collection of personal information in the course of commercial activity in all Canadian jurisdictions with the exception of Alberta, British Columbia, and Quebec which have their own private-sector privacy laws which are substantially similar. The Office of the Privacy Commissioner of Canada has an explainer document on PIPEDA on their website.

Public sector: Municipalities, provinces and territories, and federally-regulated bodies are covered under a range of statues. When location data is collected in the course of a public/private partnership agreement, it is imperative to identify the relevant legislation that applies and lines of accountability for compliance with that legislation. For example, the Ontario Information and Privacy Commissioner has described some of the issues inherent in a smart city context in the technology fact sheet "Smart Cities and Your Privacy Rights." When there may be competing proprietary or commercial and public interests in the data, an appropriately designed data stewardship model may assist in resolving those conflicts in the public interest.

Location data and data stewardship models

Data stewardship models are not a silver bullet for the privacy issues raised by location data collection. Best practices for meaningful consent for data collection, use, disclosure and retention are not obviated by a data stewardship model, but rather, such a model may assist in mitigating privacy risks when collecting such data is necessary and proportionate for purposes related to the public good. The question of whether the privacy risks outweigh the potential benefit to allowing location data collection in any given situation will vary and requires careful consideration.It is ultimately an area that may require legislation.

[i] Kondor, Dániel & Hashemian, Behrooz & Montjoye, Yves-Alexandre & Ratti, Carlo. (2017). Towards matching user mobility traces in large-scale datasets. IEEE Transactions on Big Data. PP. 10.1109/TBDATA.2018.2871693.