WeirFoulds LLP

WeirFoulds Technology Insights: "Is Someone Following Me?" A Primer on Data Tracking

June 14, 2022

By James G. Kosa and Kristen Robertson

Companies collect more data than ever before, allowing them to make informed decisions about how to better their business and serve their customers – whether that be by improving their website experience, or tailoring advertising efforts based on a potential customer's preferences.

This article provides an overview of the ways that user data can be tracked by companies, and the potential privacy implications surrounding the collection and use of such data.

How can user data be tracked?

- IP address: a unique numerical identifier assigned to devices connected to the internet that can reveal the geolocation of the device (i.e., city, postal code, area code). Advertisers looking to target potential customers with relevant products may be particularly interested in tracking IP addresses.
- MAC addresses: a distinct serial number given to every device connected to a network interface. Hackers can use a MAC address to bypass authentication checks and copy all the data passed on to the default gateway.
- IMEI numbers: a unique number exclusive to a mobile device, like a cell phone or an Internet of things (IoT) device, that can be used to spoof a SIM card. "Spoofing" allows someone to pretend to be your cellphone and to bypass two factor authentication protections.
- Cookies: a small piece of text placed on your computer while visiting a website that collects information based on your browsing patterns.
    - Third party Cookies: when visiting a website with an ad, a cookie can be passed from a third party ad company to your computer, and is saved on your computer as a small text file, which informed the website about your preferences and browsing history, so that ads can be targeted to you.
    - Super Cookies: HTML 5 (the most current form of the language used to display web pages, and most modern browsers, allow the creation and storage of information about you on your computer in a number of new ways that go beyond a simple text file.
- Beacon: a tiny image file on web pages or in email messages (1 pixel by 1 pixel in size). When you visit the web page or open the email, the image is downloaded and information about you (i.e., IP address, location data) becomes trackable.
- Third party access to online accounts (via SDKs): a package of tools that help apps function (i.e., if a developer wants to let users sign in via Facebook, they'd want Facebook's Login Software Development Kit (SDK)). SDKs for many of the common social media platforms and devices include features that allow for the collection of personal information. Such SDKs collect and send data back to the third party that provides them.
- Location data: SDKs for mobile devices make it easy for developers to include location-tracking features on an app while providing no real service.
    - GPS sensors: location is derived by comparing timestamps against the position of GPS satellites when the signal is

received.

- Cell towers: as the strength of the signal changes between towers, the location of a device can be approximated using the device's SIM card.
- WiFi networks: using crowdsourced WiFi data of surrounding networks.
- Bluetooth beacons: transmit information packets through Bluetooth signals that can be "seen" by other devices

Artificial intelligence (AI) and data tracking

While tracking methods provide an avenue to collect significant amounts of data, companies are sometimes unable to benefit from the data they collect without expending a lot of energy extracting insight into customer behaviour. AI, and specifically machine learning tools, bridge this gap by allowing the company to process a large amount of data. As part of processing such data for machine learning purposes, data is unified across many platforms and sources, pulling all the data into one view, and then the AI tool can identify patterns in such aggregate sets of data. These patterns can then be used to make predictions about preferences and assist companies in their business development.

Intersection with privacy laws

In Canada, the *Personal Information Protection and Electronic Documents Act (**"PIPEDA"**)*[1] governs the private sector's collection, use, and disclosure of personal information, or information about an "identifiable individual." Although data tracked online is often anonymous, it can be reidentified with relative ease, especially if AI software is used to unify data or the data is aggregated from multiple sources.

Combining datasets from anonymous profiles from multiple sources increases the risk of profiles being tied to offline identities, and the data becoming personal information. If the data is capable of identifying a person, even if it was originally rendered "anonymous", it is still personal information. If data becomes personal information, companies should be aware of their additional obligations including regarding consent to collection, how the information is stored, and notification if a security breach was to occur.

What's next?

As governments in Canada and around the world are updating their privacy legislation, with a focus on data protection and consent, it is likely that companies will soon be subject to greater privacy requirements when tracking data. For example, the GDPR and Quebec's new Privacy Act both have updated definitions of "personal information" that will likely encompass more of the data that is collected through the various methods discussed above.

WeirFoulds Technology Insights is a monthly issued newsletter that discusses the meaning of cybersecurity, the privacy frameworks that mark the boundaries of the cyber domain, the basic of technology contracting and the types of contracts to consider, security compliance, security reporting obligations and mechanisms, and the dark web. To receive the email newsletter, click here and subscribe to our "Intellectual Property and Technology" list.

[1] The provinces of British Columbia, Alberta and Quebec each have their own private sector privacy law legislation that is "substantially similar" to PIPEDA.

For more information or inquiries:

James G. Kosa

Toronto
416.947.5043

Email:
jkosa@weirfoulds.com

James Kosa is a partner at WeirFoulds with a practice focused on information technology and intellectual property law. He is the Co-Chair of the firm's Technology & Intellectual Property and Privacy & Access to Information Practice Groups, and Co-Chair of the Blockchain and Digital Assets Practice Group.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035