Privacy Tech-Know Blog: Uniquely You: The identifiers on our phones that are used to track us

This page has been archived on the Web. (#archived)

Christopher Parsons, Guest blogger (/en/blog/?a%5B0%5D=Christopher+Parsons,+Guest+blogger), December 8, 2016 - Data mining (/en/blog/?q[0]=652), Reputation (/en/blog/?q[0]=658), Internet and online (/en/blog/?q[0]=661), Location (/en/blog/?q[0]=663), PIPEDA (/en/blog/?q[0]=667), Privacy Sector Organizations (/en/blog/?q[0]=671), Privacy Tech-Know Blog (/en/blog/?q[0]=677)

Canadians' mobile devices are filled with applications that collect personal information, including identifiers that are engrained into different parts of the devices. But what exactly are these identifiers, and how are they used?

An identifier is a piece of information (usually a sequence of characters) that's used to uniquely identify a device, a user, or a set of behaviours taken on the device. Mobile identifiers constitute privacy-affecting technologies because they can be used to correlate an individual's various activities while using a phone, tablet, or other connected device, and they support the linking of devices with actual persons.

Our mobile devices are filled with identifiers that uniquely label different components and behaviours. The radios and other physical hardware, operating systems, applications, and even web browsers are all rife with identifiers that can uniquely identify the device, the person using the device, or the behaviours of the user. And while these identifiers are typically meant to serve a useful purpose, the user is often unaware that these identifiers exist or how they're collected and used. We will outline several of the most prominent identifiers associated with mobile devices and their significance for privacy.

Hardware Identifiers

All physical devices possess a pair of essential identifier-types: (1) each radio (e.g. Bluetooth, Wi-Fi) has a Media Access Control (MAC) address that uniquely identifies the radio, and (2) devices also have an International Mobile Equipment Identifier (IMEI).

The IMEI reveals where the device was manufactured and a unique serial number. The IMEI remains constant over the lifetime of the device and is used by cellular providers for a variety of purposes, such as checking if a device is 'blacklisted' from a network after being reported stolen. The IMEI number is also sometimes collected by application developers for user-tracking purposes.

The MAC address is used in network communications and can be changed but doing so requires technical sophistication exceeding most users' capabilities. MAC addresses are rarely disclosed to anyone other than the network operator providing cellular or Wi-Fi service.

Network Provider Identifiers

Mobile devices connect to a variety of networks such as those operated by telecommunications service providers (e.g., Bell, Rogers, TELUS) and by smaller organizations (e.g., coffee shops). Telecommunications service providers are responsible for issuing and subsequently monitoring a pair of critical identifiers: the International Mobile Subscriber Identifier (IMSI) and the Mobile Station International Subscriber Directory Number (MSISDN). Both of these numbers are included with the Subscriber Identity Module (SIM) that customers insert into their phones or cellular-connected tablets.

The MSISDN is the phone number that's assigned to the mobile device. The IMSI, in contrast, includes a mobile country code and mobile network code used to identify the mobile network operator, and the identification number of the subscriber. When combined with the IMEI number, a network operator can ascertain when the device was made, the serial number of the device, version of its software, nation of usage-origin, carrier-of-origin, and the subscriber code of the carrier associated with the device.

The SIM also has identifying information: it reveals the telecom operator code (e.g., Rogers, Bell), the network the SIM is associated with, the year and month the SIM was created, as well as the SIM's own number. This latter number is used to confirm the SIM's validity to the mobile carriers the phone connects with. The SIM and the IMSI are typically associated with a particular subscriber in post-paid billing situations.+

Not all of these identifiers are always transmitted. Engineers recognized that the IMSI number, for example, could be used for long-term tracking purposes. Mobile networks are consequently designed to issue a Temporary Mobile Subscriber Identifier (TMSI) after the IMSI has first been received by the network. Since the TMSI is reused across devices it's of limited long-term utility for tracking devices. To capture an IMSI number a third-party would have to actively induce a mobile device to connect to a network and re-issue the IMSI number. One way to do this involves operating a fake telecommunications tower. Such fake towers are sometimes referred to as 'IMSI Catchers', 'Stingrays' or 'Mobile Device Identifiers' and work by inducing mobile devices to divulge their IMSI numbers and, sometimes, the MSISDN and IMEI numbers as well.

In addition, both cellular providers and local network operators, such as cafes, will assign Internet Protocol (IP) addresses when mobile devices are configured to access the Internet. Such operators may also collect the MAC address information associated with either the cellular or Wi-Fi radios. These network operators can potentially monitor the activities that are undertaken on the network. Since they can observe all of the mobile device's network traffic, these operators can correlate such activity with assigned IP addresses or, where login credentials are required, specific identifiers that may be more tightly linked with a specific individual or device owner.

Operating System Identifiers

Google (Android) and Apple (iPhone) also include other identifiers in their operating systems. Google uses the Google Advertising ID and Android Identifier whereas Apple uses the IdentifierForAdvertising (IDFA) Identifier.

Google's Advertising ID enables in-application targeted advertising and can be reset. Google and advertisers correlate activities with this ID in order to serve targeted advertising, and Google has a cross-device conversion system so advertisers can determine if a user viewed an ad on one device and then completed a sale on another. The Android Identifier, in contrast, is permanently associated with a device. It's no longer

supposed to be used by developers for advertising-related user tracking, though it can be used for non-advertising purposes to track user profiles.

Apple's IDFA is used to track users of applications in order to serve targeted advertisements and determine if the advertisement leads to a 'conversion', such as a sale or download of an advertised application. The IDFA can be reset and even disabled if users opt-out of ad-tracking.

Android and iPhone devices also rely on credential sets that let users access the same applications across multiple devices. While these sets are not necessarily baked into the companies' operating systems, they're required for users to access the majority of the services linked to the devices, including application stores, cloud-based photo backup services, contact books, and so on.

Application Developer Identifiers

Application developers can create their own identifiers and also access the identifiers provided by operating systems and manufacturers, including the IMEI, IDFA, Android identifier, and the phone number. Such unique identifiers can be used to provide them with requested services (such as letting them log into a fitness tracking application), and they can also be shared with third parties or sold to data brokers. Application developers may also collect users' social media credentials or they can compel users to generate an application-specific credential set (e.g., a username and password), and correlate these with identifiers.

Web Browser Identifiers

Websites and advertisers can set cookies in mobile devices' Internet browsers (e.g., Safari, Chrome) and applications, and track persons as they use the Internet. Cookies can often be deleted from the mobile device, although the interfaces for controlling cookies can often be difficult to use.

Consent, Collection, Confusion

Not all identifiers are the same: some are permanent and others are transitory; some are revealing of personal information and others less so. The IMEI, as an example, reveals relatively little personal information in isolation. However, when the IMEI is combined with other identifiers or activities, it can be used to link what might otherwise be disparate activities to a common, permanent, device identifier. The result is that, despite some identifiers being clearly personal information (such as social media credentials, phone numbers, or perhaps geolocation information) others *become* personal information depending on how developers or other parties assign and use the identifiers.

Identifiers are often unknown to users and collected without device owners' explicit knowledge. While privacy policies may indicate that users are tracked or monitored, not all applications contain privacy policies. Additionally, such policies may be challenging for users to understand: even if all the captured identifiers are listed, users may not know what kinds of information are integrated into the identifiers in question, or the implications of capturing the identifiers denoted in the policy.

The uploading of identifiers to servers can sometimes happen without warning and, short of reading a privacy policy (which may not list each specific kind of identifier collected) or monitoring data traffic between the device and the Internet (which may sometimes be challenging if data transmissions are encrypted), a user may never fully know which data are collected from their device. A lack of knowledge of the data transmissions raises questions concerning the extent to which an individual can consent to the collection and use of their personal information.

In addition to questions of whether mobile identifiers constitute a reasonable collection of personal information, there's also the potential for companies that collect the information to subsequently use it for different purposes or sell that data to other parties (e.g., collecting a mobile phone number and selling it to other organizations, or collecting GPS information and selling location data to data brokers). As a result, mobile device identifiers could be circulated more widely than expected by users.

Finally, mobile identifiers are usually meant to be accessed by particular commercial parties for ostensibly legitimate reasons. But they can also be accessed by other parties, including parties who design applications to collect information in excess of what's required for the application to operate. They might also be accessed by parties (including government agencies) that establish and operate cellular telephony equipment designed to capture mobile identifiers that are typically only transmitted to cellular providers.

Christopher Parsons is a Research Associate at the Citizen Lab in the Munk School of Global Affairs at the University of Toronto.

Suggested Reading

- The Many Identifiers In Our Pockets: A Primer on Mobile Privacy and Security (https://citizenlab.org/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/)
- Location-Based Services and Privacy (https://ojs.library.dal.ca/CJLT/article/download/4848/4367)
- We're Watching: Malls Track Shopper's Cell Phone Signals to Gather Marketing Data (http://arstechnica.com/business/2011/11/were-watchin)
- A Marketer's Guide to Cross-Device Identity (https://adexchanger.com/data-exchanges/2016-edition-marketers-guide-cross-device-identity)
- A Chatty Squirrel: Privacy and Security Issues with UC Browser (https://citizenlab.org/2015/05/a-chatty-squir)

Previous (/en/blog/20161109/)

Next (/en/blog/20170105/)

About the blog

The Office of the Privacy Commissioner of Canada's blog serves as an informal platform for writing about trends that are of interest to our office, our stakeholders and the Canadian public.

Sign up for updates

RSS (/en/rss-feeds/)

Recent Posts

Privacy Tech-Know blog: When what is old is new again – The reality of synthetic data (/en/blog/20221012/)

Blog Post - October 12, 2022

Making privacy protection a basic skill for students (/en/blog/20220303/)

Blog Post - March 3, 2022

Having a Data Privacy Week 'family tech talk' (/en/blog/20220124/)

Blog Post - January 24, 2022

Remote access: Opening the door to your personal information (/en/blog/20211209/)

Blog Post - December 9, 2021

Making playtime safer in the Internet of Toys (/en/blog/20211202/)

Blog Post - December 2, 2021

Date modified:

2016-12-08