Satellite data: The other type of smartphone data you might not know about

February 21 2023, by Tommy Cooke, Alicia Sabatino, Benjamin Muller and Kirstie Ball

Credit: AI-generated image (disclaimer)

When you think about location data on your mobile phone, tablet or laptop, what comes to mind? Mailing addresses? Postal codes? These data indicate where you live, where you work, and the places you visit.

When combined with other types of data over time, companies and governments use them to analyze your consumption patterns, occupation, education, health and financial status.

Turning location services off only prevents smartphone apps from receiving location data. Smartphones can still be located by cell towers and wireless networks when location services are switched off.

This was highlighted by German politician Malte Spitz over a decade ago when he sued his cellphone provider, Deutsche Telekom, for any personal data they had about him.

When the case was settled and he eventually received the data, Spitz found 35,000 references to his location. He was able to visually reconstruct his movements over the previous six months, demonstrating the relevance of data protection laws to the public.

But there is more. By using critical code and documentary research methods, we found that raw satellite location measurement data are perpetually created in our devices all the time.

Because satellite data are building blocks used by our phones to determine where we are, they don't always get turned off—nor are they collected and treated the same way as location data.

Data outputs

Smartphones determine your location in several ways. The first way involves phones triangulating distances between cell towers or Wi-Fi routers.

The second way involves smartphones interacting with navigation satellites. When satellites pass overhead, they transmit signals to smartphones, which allows smartphones to calculate their own location. This process uses a specialized piece of hardware called the Global Navigation Satellite System (GNSS) chipset. Every smartphone has one.

When these GNSS chipsets calculate navigation satellite signals, they output data in two standardized formats (known as protocols or languages): the GNSS raw measurement protocol and the National Marine Electronics Association protocol (NMEA 0183).

GNSS raw measurements include data such as the distance between satellites and cellphones and measurements of the signal itself.

NMEA 0183 contains similar information to GNSS raw measurements, but also includes additional information such as satellite identification numbers, the number of satellites in a constellation, what country owns a satellite, and the position of a satellite.

NMEA 0183 was created and is governed by the NMEA, a not-for-profit lobby group that is also a marine electronics trade organization. The NMEA was formed at the 1957 New York Boat Show when boating equipment manufacturers decided to build stronger relationships within the electronic manufacturing industry.

In the decades since, the NMEA 0183 data standard has improved marine electronics communications and is now found on a wide variety of non-marine communications devices today, including smartphones.

Who has access to these data?

It is difficult to know who has access to data produced by these protocols. Access to NMEA protocols is only available under license to businesses for a fee.

GNSS raw measurements, on the other hand, are a universal standard and can be read by different devices in the same way without a license. In 2016, Google allowed industries to have open access to it to foster innovation around device tracking accuracy, precision, analytics about how we move in real-time, and predictions about our movements in the future.

While automated processes can quietly harvest location data—like when a French-based company extracted location data from Salaat First, a Muslim prayer app—these data don't need to be taken directly from smartphones to be exploited.

Data can be modeled, experimented with, or emulated in licensed devices in labs for innovation and algorithmic development.

Satellite-driven raw measurements from our devices were used to power global surveillance networks like STRIKE3, a now defunct European-led initiative that monitored and reported perceived threats to navigation satellites.

Data and citizen rights

Our research raises questions about how rights are protected in the midst of these practices. Citizens have little to no access to the data output from NMEA 0183 and GNSS raw measurements. Because of this, people are unable to negotiate the visibility of their data in these datasets.

The data output from NMEA 0183 and GNSS raw measurements flow unrestricted from every smartphone on the planet. Smartphones have unique identifiers—IMEI numbers—that are known to the tech ecosystem. They can be connected to a user's personal details.

The flow of NMEA 0183 and GNSS data is invisible to the average person, meaning citizens are unsure of how these data are used, or with whom they are shared. Because of this, it's impossible for people to challenge how their personal data are used.

As interest in the supposed security, entertainment and surveillance value of these protocols continue to grow, these protocols are increasingly susceptible to misuse by third-party developers.

But there is another layer to this: NMEA 0183 and GNSS raw measurements are standards in industries that offer products and services that many of us benefit from. The NMEA has foundations in safe passage at sea, making their data an important part of emergency services operations. GNSS raw measurements are also utilized for safety purposes.

Could solutions restrict the use of these data for life-critical situations only? Is there an oversight body that could assess what impacts industrial usage of these data might have upon smartphone owner rights and liberties? What about an audit led by civil society, who would be appropriately positioned to objectively inspect these issues to determine whether they might harm the public? For example, consider the way the federal privacy commissioner reviews app data activities.

Location data now flows constantly from GNSS chipsets. There is uncertainty about who is using these data, and for what purposes. Until industry and government reassure citizens that personal data are not being exploited and that rights are protected, these remain open questions.

Provided by The Conversation

Citation: Satellite data: The other type of smartphone data you might not know about (2023, February 21) retrieved 23 April 2024 from https://techxplore.com/news/2023-02-satellite-smartphone.html