National Security Agency | Cybersecurity Information

# Limiting Location Data Exposure

Mobile devices store and share device geolocation data by design. This data is essential to device communications and provides features—such as mapping applications—that users consider indispensable. Mobile devices determine location through any combination of Global Positioning System (GPS) and wireless signals (e.g., cellular, wireless (Wi-Fi®[1]), or Bluetooth®[2] (BT)). Location data can be extremely valuable and must be protected. It can reveal details about the number of users in a location, user and supply movements, daily routines (user and organizational), and can expose otherwise unknown associations between users and locations.

Mitigations reduce, but do not eliminate, location tracking risks in mobile devices. Most users rely on features disabled by such mitigations, making such safeguards impractical. Users should be aware of these risks and take action based on their specific situation and risk tolerance. When location exposure could be detrimental to a mission, users should prioritize mission risk and apply location tracking mitigations to the greatest extent possible. While the guidance in this document may be useful to a wide range of users, it is intended primarily for NSS/DoD system users.[3]

## Mobile devices expose location data

Using a mobile device—even powering it on—exposes location data. Mobile devices inherently trust cellular networks and providers, and the cellular provider receives real-time location information for a mobile device every time it connects to the network. This means a provider can track users across a wide area. In some scenarios, such as 911 calls, this capability saves lives, whereas for personnel with location sensitivities, it may incur risks. If an adversary can influence or control the provider in some way, this location data may be compromised. Public news articles have reported that providers have been known to sell data, including near-real time location data, to third-parties [1].

Location data from a mobile device can be obtained even without provider cooperation. These devices transmit identifying information when connecting to cellular networks. Commercially available rogue base stations allow anyone in the local area to inexpensively and easily obtain real-time location data and track targets. This equipment is difficult to distinguish from legitimate equipment, and devices will automatically try to connect to it, if it is the strongest signal present [2].

Additionally, location data is stored on the mobile device. Past location information can be used to forecast future locations [3]. Other examples of risk exist: websites use browser fingerprinting to harvest location information [4], and Wi-Fi access points and Bluetooth sensors can reveal location information [5].

## Location services ≠ GPS

A mobile device provides geolocation data as a service to apps. This is known as location services, and users can disable them in the settings of a device. Perhaps the most important thing to remember is that disabling location services on a mobile device does **not** turn off GPS, and does **not** significantly reduce the risk of location exposure. Disabling location services only limits access to GPS and location data by apps. It does **not** prevent the operating system from using location data or communicating that data to the network.

Also important to remember is that GPS is **not** the same as location services. Even if GPS and cellular data are unavailable, a mobile device calculates location using Wi-Fi and/or BT. Apps and websites can also use other sensor data (that does **not** require user permission) and web browser information to obtain or infer location information [6].

[1] Wi-Fi is a registered trademark of Wi-Fi Alliance.

[2] Bluetooth is a registered trademark of Bluetooth SIG, Inc.

[3] The information contained in this document was developed in the course of NSA's Cybersecurity mission, including its responsibilities to assist Executive departments and agencies with operations security programs.

## Location can often be determined even if cellular is turned off

Even if cellular service is turned off on a mobile device, Wi-Fi and BT can be used to determine a user's location. Inconspicuous equipment (e.g., wireless sniffers) can determine signal strength and calculate location, even when the user is not actively using the wireless services. Even if all wireless radios are disabled, numerous sensors on the device provide sufficient data to calculate location. Disabling BT completely may not be possible on some devices, even when a setting to disable BT exists. When communication is restored, saved information may be transmitted.

If a mobile device has been compromised, the user may no longer be able to trust the setting indicators. Detecting compromised mobile devices can be difficult or impossible; such devices may store or transmit location data even when location settings or all wireless capabilities have been disabled.

## The risk isn't limited to mobile devices

Anything that sends and receives wireless signals has location risks similar to mobile devices. This includes, but is not limited to, fitness trackers, smart watches, smart medical devices, Internet of Things (IoT) devices, and built-in vehicle communications. Personal and household smart devices (e.g., light bulbs, cookware, thermostats, home security, etc.) often contain wireless capabilities of which the user is unaware. Such IoT devices can be difficult to secure, most have no way to turn off wireless features, and little, if any, security built in. These security and privacy issues could result in these devices collecting and exposing sensitive location information about all devices that have come into range of the IoT devices [7]. Geolocation information contained in data automatically synced to cloud accounts could also present a risk of location data exposure if the accounts or the servers where the accounts are located are compromised.

## Apps and social media

Apps, even when installed using the approved app store, may collect, aggregate, and transmit information that exposes a user's location. Many apps request permission for location and other resources that are not needed for the function of the app.

Users with location concerns should be extremely careful about sharing information on social media. If errors occur in the privacy settings on social media sites, information may be exposed to a wider audience than intended. Pictures posted on social media may have location data stored in hidden metadata. Even without explicit location data, pictures may reveal location information through picture content [8].

## Mitigations

Different users accept different levels of risk regarding location tracking, but most users have some level of concern. The following general mitigations can be used for those with location sensitivities:

- Disable location services settings on the device.
- Disable radios when they are not actively in use: disable BT and turn off Wi-Fi if these capabilities are not needed. Use Airplane Mode when the device is not in use. Ensure BT and Wi-Fi are disabled when Airplane Mode is engaged.[4]
- Apps should be given as few permissions as possible:
  - Set privacy settings to ensure apps are not using or sharing location data.
  - Avoid using apps related to location if possible, since these apps inherently expose user location data. If used, location privacy/permission settings for such apps should be set to either **not** allow location data usage or, at most, allow location data usage only while using the app. Examples of apps that relate to location are maps, compasses, traffic apps, fitness apps, apps for finding local restaurants, and shopping apps.
- Disable advertising permissions to the greatest extent possible:
  - Set privacy settings to limit ad tracking, noting that these restrictions are at the vendor's discretion.
  - Reset the advertising ID for the device on a regular basis. At a minimum, this should be on a weekly basis.

[4] For iOS devices: Only use the Settings app to disable Wi-Fi/BT. Settings for these features in the control center may not work as expected.

- Turn off settings (typically known as FindMy or Find My Device settings) that allow a lost, stolen, or misplaced device to be tracked.
- Minimize web-browsing on the device as much as possible, and set browser privacy/permission location settings to **not** allow location data usage.
- Use an anonymizing Virtual Private Network (VPN) to help obscure location.
- Minimize the amount of data with location information that is stored in the cloud, if possible.

If it is critical that location is **not** revealed for a particular mission, consider the following recommendations:

- Determine a non-sensitive location where devices with wireless capabilities can be secured prior to the start of any activities. Ensure that the mission site cannot be predicted from this location.
- Leave **all** devices with any wireless capabilities (including personal devices) at this non-sensitive location. Turning off the device may not be sufficient if a device has been compromised.
- For mission transportation, use vehicles without built-in wireless communication capabilities, or turn off the capabilities, if possible.

## Protect data, protect privacy, protect the mission

While it may not always be possible to completely prevent the exposure of location information, it is possible—through careful configuration and use—to reduce the amount of location data shared. Awareness of the ways in which such information is available is the first step.

## Works Cited

[1] Pai, Ajit, “Status of the FCC’s Investigation into the Disclosure of Consumers’ Real-Time Location Data,” Federal Communications Commission, 31 January 2020. [Online] Available at: https://docs.fcc.gov/public/attachments/DOC-362222A1.pdf

[2] J. Dunn, “Security weaknesses in 5G, 4G, and 3G could expose users’ locations.” Sophos, 04 February 2020. [Online] Available at: https://nakedsecurity.sophos.com/2019/02/04/security-weaknesses-in-5g-4g-and-3g-could-expose-users-locations/

[3] S. Lee, J. Lim, J. Park, K. Kim. “Next Place Prediction Based on Spatiotemporal Pattern Mining of Mobile Device Logs.” PubMed Central, US National Library of Medicine, 23 January 2016. [Online] Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4801523

[4] Y. Cao, S. Li, E. Wijmans. “(Cross-) Browser Fingerprinting via OS and Hardware Level Features.” The Network and Distributed System Security Symposium, 27 February 2017. [Online] Available at: https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/

[5] Moz://a location service Overview. Mozilla, 2012-2020. [Online] Available at: https://location.services.mozilla.com

[6] A. Mosenia, X. Dai, P. Mittal, N. Jha. “PinMe: Tracking a Smartphone User around the World.” Cornell University, 05 February 2018. [Online] Available at: https://arxiv.org/pdf/1802.01468.pdf

[7] FTC Staff Report, “internet of things: Privacy & Security in a Connected World.” Federal Trade Commission, 09 January 2015. [Online] Available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[8] T. Weyand, I. Kostrikov, J. Philbin. “PlaNet - Photo Geolocation with Convolutional Neural Networks.” Cornell University, 17 February 2016. [Online] Available: https://arxiv.org/abs/1602.05314

### *Disclaimer of Endorsement*

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

### *Contact*

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov