THE WORLD OF GEOLOCATION DATA

Information about where devices are located can serve as a proxy for where individuals are located over time, which can be very revealing of individual behavior, interests, or beliefs. How is location data generated, who has access to it, and how is it used?

HOW A DEVICE LOCATES ITSELF

Mobile devices contain hardware sensors that allow them to detect a wide variety of signals.

- Cell Towers
- Known Bluetooth Signals
- Nearby Wi-Fi Networks
- Satellites (GPS)
- Proximity to Other Devices

HOW LOCATION DATA IS COLLECTED

Collecting location data from a device usually requires a coordinated interaction between the user, the operating system (OS), and the physical hardware. Here is how those layers interact:

1. The device hardware detects signals from surroundings.
2. The OS analyzes the signals and provides the technical permission layer for Apps to request access to a precise location measurement.
3. The App requests permission from the user via the OS.
4. The OS provides a precise location measurement and timestamp to the app.

DETERMINING RISK IN LOCATION DATASETS

Location datasets may reveal personal behavior and impact the privacy of individuals or groups. Here are some factors to consider when evaluating privacy risks:

- Proximity vs. Location
  - Proximity to nearby devices or signals can be less risky than collecting a detailed location history of a device.
- Precision and Accuracy
  - Location data can be accurate (revealing of a device’s “true location”) or inaccurate, as well as precise (such as a street corner), or imprecise (such as a city or country).

POTENTIAL SAFEGUARDS

Different entities are subject to different restrictions. Broadly applicable privacy and consumer protection laws may also apply. Here are some examples:

- **Carriers**
  - Cell phone carriers generally know where devices are located because they direct calls and content to phones through local cell towers. This information is collectively known as cell site location information (CSLI).

- **Data Brokers, Aggregators, and Other Third Parties**
  - Location data may be licensed, sold, or otherwise disclosed to a variety of downstream entities that do not have a direct relationship with the user, for example: advertising networks, hedge funds, consumer data re-sellers, traffic and transportation analytics firms, or government buyers.

- **Apps and App Partners**
  - Many apps provide location-based features, such as weather alerts. In addition, many share location data with partners, for example to detect fraud, provide analytics, or to target ads. Most apps use Software Development Kits (SDKs), or code developed by third parties, to enable features and allow partners direct access to data.

- **Location Analytics Providers**
  - Many airports, stadiums, and stores analyze signal data emitted by connected devices (mobile phones, fitness trackers, etc.) to better understand their busiest hours or in-store foot-traffic.

- **Sensitivity Locations**
  - Known locations (such as a person’s home or workplace), or sensitive locations (such as schools or clinics) can increase risk of re-identification or reveal intimate information.

- **De-identifying Techniques**
  - Many techniques can be applied to reduce the risk of identifying individuals within a location dataset, including aggregating the data, or applying computational methods such as differential privacy. Risk can also be reduced through administrative access controls.