SOVEREIGN
INTELLIGENCE

Government Use of Location Intelligence
Our Policy & Commitment
Sovereign Intelligence

Background

A number of recent articles including "*Federal Agencies Use Cellphone Location Data for Immigration Enforcement*," February 7, 2020 by the Wallstreet Journal, highlight the global tension between legal and ethical use of open source data to thwart criminal or fraudulent behavior. The U.S. Department of Homeland Security, according to the article, has used the information for "immigration and border enforcement."

Previously, in December 2018, The New York Times reported that marketing companies and data providers use geolocation metadata derived from smart-device applications to enhance user experience as well as personalize advertisements.[1]

Effectively, the only way geolocation metadata is shared from an individual's phone to either the applications used or advertisements offered is through an "opt-in" process, meaning that the user affirmatively selects to engage location services.

In sum, we know the data is being used for law enforcement purposes; we know marketing companies are using the data as well as selling the information; and finally; each end-user of a smartphone device has the freedom to choose whether to share their location information with the provider.

Legal Precedent

- The Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523 generally requires the government to secure a warrant to access data about the use of electronic communications.
- The USA PATRIOT Act of 2001 reinforces that law, but allows for exceptions related to non-U.S. citizens, where the data was retrieved, etc.
- In *Carpenter v. United States*, the U.S. Supreme Court in 2018, held that a warrant is required for police to access cell site location information (CSLI) from a cell phone company—the detailed geolocation information generated by a cellphone's communication with cell towers. Warrantless access to CSLI is still allowed in exigent circumstances.

[1] Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, The New York Times, December 2018.

Frequently asked questions (FAQs)

- Where does Sovereign derive its supporting data? Sovereign collects geolocation metadata from multiple sources including GPS, IP Geolocation, Grid, Cell Towers, and other information. The information is considered Open-Source or publicly accessible data, in that any person may purchase the information.
- What is geolocation metadata? Geolocation metadata includes information derived from geo coordinates of an activity (addresses, points of interest, etc.) or device along with date and time of the information. Metadata enrichment can add other information depending on the richness of metadata (i.e., network address, provider, etc.).
- How does Law Enforcement use Sovereign's Location Intelligence? Sovereign provides access to our software via a restricted access secure webpage. Law Enforcement analyst's strictly use their findings as a "lead generation tool." This means that actual evidence collected to determine the location of a suspect in a crime, must be derived from an approved warrant in accordance with *Carpenter, et al.*

Our Policy & Commitment

See our Privacy Policy as well as contact our Data Privacy Officer via dpo@sovereign.ai with any questions. Sovereign operates our services in compliance with all U.S. and international applicable laws and regulations.

Additionally, Sovereign maintains the highest standard of data protection by implementing these precautionary measures as a standard business practice:

1. Collection of geolocation metadata is strictly anonymous.
2. Data is encrypted to the highest industry standards.
3. Records relating to customer access, usage, and products are logged.
4. Personally identifiable data related to geolocation metadata is never stored.