Proskauer

Mobile Platforms to Block Data Broker from Collecting User Location Data

New Media and Technology Law Blog on **December 11, 2020**

On December 9, 2020, the *Wall Street Journal* reported that Apple and Google will block the data broker X-Mode Social Inc. ("X-Mode") from collecting location data from iPhone and Android users. Apple and Google have reportedly informed app developers to remove the X-Mode social tracking SDK from all of their apps within a short period of time or risk removal from the platforms' app stores. This action apparently was prompted by reports that X-Mode was selling location data to certain defense contractors and government entities.

The WSJ report suggests that Apple and Google notified Senator Ron Wyden about this action. Senator Wyden and a group of other Senators have been soliciting government inquiries over the last several months into the sale of location data to government contractors and agencies. It is Senator Wyden's position that such sales of users' location data by commercial data brokers to government entities are unlawful without a warrant (citing the Supreme Court case, *Carpenter v. United States*, 138 S.Ct. 2206 (2018), which held that the acquisition of cell-site location information was a Fourth Amendment search).

Senator Wyden's scrutiny over such practices does not seem to be limited to sale of location data to government sources, but more so toward the wider data tracking ecosystem. He was one of the senators that earlier this year sent a letter to FTC Chairman Joseph J. Simons urging the agency to investigate whether analytics firm Yodlee's financial data collection practices were violating the FTC Act (a request which led to at least one civil investigative demand being issued by the FTC to Yodlee and a putative class action suit over such practices). In the WSJ article, Wyden is quoted as stating: "Apple and Google deserve credit for doing the right thing and exiling X-Mode Social, the most high-profile tracking company, from their app stores. But there's still far more work to be done to protect Americans' privacy, including rooting out the many other data brokers that are siphoning data from Americans' phones."

Thus, beyond the fate of X-Mode, the big question is whether this is the beginning of the end of widespread locational sharing on mobile phones, or merely an isolated occurrence linked to certain profiling activities or the sharing of data with certain government and intelligence entities.

Regardless, the action by Apple and Google brings to mind many unanswered questions:

- How was X-Mode out of compliance with Apple and Google's developer policies and privacy guidelines concerning the collection of location data? The WSJ article states that Apple informed developers that X-Mode "surreptitiously builds user profiles based on collected user data," in violation of its terms of service. Also, when is data collection and profiling considered "surreptitious" if it is done with the requisite notice and consent to the user as required by applicable terms?
- Will the platforms enact bans against other data brokers or SDK social tracking developers that have engaged in similar "surreptitious" collection and resale practices? According to the WSJ report, X-Mode claims that the blocking was arbitrary (asking that Apple and Google reconsider) given that many other advertising SDKs collect similar data and sell it to commercial entities.
- Will Apple and Google further tighten or enforce developer policies relating to the use of a user's location data? It should be noted that Apple's iOS14 policies already provide for enhanced notice to users about the presence of third party tracking code in apps and how such data may be used, not to mention permission prompts to collect granular location data from users (and the option to allow users to not sharing precise geolocation data) And next year, Apple is slated to roll out a privacy feature that will require app operators to get opt-in permission before sharing a user's device ID for ad tracking purposes. Google too is implementing restrictions on foreground and background locational tracking.

Despite the raft of open questions, this latest development highlights two major points. First, the reality is that while location data has become more valuable and more desirable to marketers and other commercial entities, the practice will continue to be under heightened scrutiny with the evolution of more stringent privacy laws and mobile platform developer policies, as well as growing public awareness about locational data sharing. Second, given the sometimes circuitous route location and other mobile data takes to reach a reseller or analytics firm, it is important for downstream recipients of aggregated user data or reports crunching such data to perform due diligence and understand how such data is collected and whether such collection comports with contractual and mobile platform requirements.

View Original

Related Professionals

- **Jeffrey D. Neuburger**
  Partner