Proskauer

City Attorney of Los Angeles Sues Popular Weather App Claiming Deceptive Collection and Sharing of Geolocation Data

New Media and Technology Law Blog on **January 4, 2019**

Yesterday, Los Angeles City Attorney Mike Feuer filed an unfair competition lawsuit on behalf of the People of the State of California against the operator of the popular Weather Channel app ("TWC app") for allegedly failing to conspicuously disclose to users that the TWC app collects and shares users' mobile geolocation data. (*People v. TWC Product and Technology, LLC* (Cal. Super., L.A. County)). In essence, the suit alleges that the TWC app mines users' precise geolocation data after receiving permission to gather location information to provide "personalized local weather data" without also adequately disclosing that the app also packages this data trove for advertising and analytics services unrelated to weather reporting. The City is seeking injunctive relief and civil penalties under state law for this alleged unfair business practice. Feuer held a press conference today further detailing the State's position in this lawsuit and expressed his hope that this case would spur litigation in other jurisdictions and legislation on the issue.

According to the suit, when seeking users' permission to access their location, the TWC app suggests that such data will be used only to provide users with "personalized local weather data, alerts and forecasts" and does not directly disclose to users that TWC will transmit anonymized data to third parties for commercial purposes. (View screenshot).

The suit contends that the app does not reference or link to privacy notices at the permission prompt that might give users more information about how their location data might be used. Furthermore, the complaint alleges that users who delve into the app's Privacy Policy or the Privacy Settings section are faced with what the City claims are "vague" statements about its geolocation collection practices:

- The Privacy Settings section, according to the complaint, states that geolocation data may be used for "geographically relevant ads and content" and shared with "partners" for "the provision of services such as business operations, advertising solutions or promotions."

- The Privacy Policy states: “We also collect location information through the Services so that we can offer you certain location-based services (such as severe weather alerts through our mobile applications), provide advertisements that are relevant to your geographic location, and conduct analytics to improve the Services.”
- The Privacy Policy also states that: “We may aggregate or otherwise alter information (including location information) that is collected from the Services so that it does not identify your device and cannot reasonably be linked to your device. We may use or share such information with third parties for research or commercial purposes (e.g., analyzing trends based on foot traffic).”

Geolocation data has been a hot issue of late (we just wrote about mobile locational tracking issues last month). So, what permissions are needed for mobile apps to collect, use and share locational information? This is a question that app developers, mobile platform providers, end-users of locational data, consumers and regulators are asking. The topic has been the subject of a steady stream of legal developments over the last year that touch geolocation privacy, including the rollout of the GDPR (and multiple complaints against tech companies for geolocation collection) and a Supreme Court ruling about the Fourth Amendment implications of the collection of cell-site location information. This California suit comes on the heels of a noteworthy *New York Times* article on geolocation tracking that, along with other media coverage, seemingly brought the practices of the TWC app to the attention of the L.A. City Attorney (given the citations to the NYT article and other sources in the complaint). Beyond this suit, it is unknown whether the TWC app’s method of data collection comports with Apple’s or Google’s developer guidelines’ explicit restrictions on geolocation data collection (an issue which we detailed last month).

We will be monitoring this lawsuit closely. Mobile geolocation data remains a sensitive issue and developers that collect such data should craft their permission prompts and privacy settings with care (and end-users that receive such anonymized data should also be cognizant about the nature of how such data is collected).

View Original

Related Professionals

- **Jeffrey D. Neuburger**