



JANUARY 2019

Spotlight on Precise Location: Understanding the Impact of the L.A. City Attorney’s Office Lawsuit Against Weather Channel App Makers Over Collection of Precise Geolocation Data

by *Jessica B. Lee and Caroline W. Hudson*

The office of L.A. City Attorney Michael Feuer recently filed a [complaint](#) in Los Angeles County Superior Court against the makers of the Weather Channel app over the collection, sharing, and monetization of users’ precise geolocation data. According to the complaint, TWC Product and Technology, LLC tracks users’ “second-by-second movements with startling precision,” including how much time they spend at each location, even when users are not actively using the Weather Channel app. TWC then monetizes this data through its own “audience-derived location targeting platform.”

The City Attorney’s office challenges the consent language used by the app, which states only that “You’ll get personalized local weather data, alerts and forecasts.” The City Attorney alleges that this permission process deceives users, since the app does not disclose that (a) TWC will transmit location data to third parties, and (b) location data will be used for advertising and other commercial purposes “bearing no relation to weather or the services provided by the app.” Instead, according to the complaint, the opt-in language “misleadingly suggests that such data will be used only to provide users with ‘personalized local weather data, alerts and forecasts.’”

The City Attorney’s office further objects that this consent process does not reference or link to any other sections of the app for more information. Users therefore have no reason to “comb[] through” the

Privacy Policy for “buried” disclosures, which the complaint further criticizes as “lengthy,” “opaque,” and “vague.”

The lawsuit seeks injunctive relief and civil penalties of up to \$2,500 per violation, plus an additional civil penalty of up to \$2,500 for each violation perpetrated against senior citizens or disabled persons.

Domestic and International Focus on Location Data

The complaint comes on the heels of, and cites, a recent New York Times [investigative report](#) that examined the nature and scope of location data collected from certain mobile apps. The article raised concerns about the scope of the collection, noting that some mobile apps continuously collect precise geolocation information from users’ devices and can effectively create databases that map users’ movements throughout the day. The article also highlighted the lack of notice given to users about how their location data is used.

The L.A. City Attorney’s complaint is the latest in a series of recent enforcement actions that appear to shine a spotlight on collection of precise geolocation data. At the end of 2018, German regulators accused China’s Mobike of violating the European Union’s

This publication may constitute “Attorney Advertising” under the New York Rules of Professional Conduct and under the law of other jurisdictions.

General Data Protection Regulation (GDPR) by collecting precise location data when customers are not using a bike, and several French location data companies received warnings about the validity of the consent mechanisms used to obtain consent for the use of precise location data.

App platforms have been paying attention as well. Apple has removed certain apps that share location data with third parties without users' explicit consent. We expect to see continued regulatory scrutiny of companies' practices with respect to the collection, use, and sharing of geolocation data and other sensitive consumer information.

What Should You Do?

The GDPR is heading into its first full year of enforcement, and a number of new U.S. and global privacy laws are in effect or on the horizon (including laws in California, Colorado, Iowa, Nebraska, Brazil, and South Africa). Now is a good time to consider whether there are additional steps your company can take to reduce its risks.

- Talk to your team to understand the scope of data collected (is precise location data collected? does the app track location when it's not in use?) and how that information is being used.
- Review the notices and disclosures provided to confirm that they are accurate, clear and "just in time" (i.e., presented just before the location data is collected). Consider the consumer's reasonable expectations when deciding whether information may be considered material and require more prominent disclosure.
- Review your internal practices to confirm that the appropriate technical and organizational security controls are in place. Access to precise location data should be limited and such data should not be retained indefinitely.

- If you are subject to the GDPR, or will be subject to the [California Consumer Privacy Act](#) (CCPA), or any other new global privacy regulations that have been enacted over the past year, you will need to confirm whether your practices are in line with the requirements of each regime.

This alert is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This alert does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

© 2019 Loeb & Loeb LLP. All rights reserved.