CLIENT ALERTS & INSIGHTS

Digital Data Broker Stuck in Class Action for Allegedly Selling User App Data

AUGUST 15, 2023

Authors: David M. Krueger

In the rapidly evolving digital world, plaintiffs' attorneys have found renewed interest in pursuing class action claims under the California Invasion of Privacy Act (CIPA) and similar laws, arguing that third-party companies are unlawfully intercepting and eavesdropping on their online activity.

The Northern District of California's recent decision in *Greenley v. Kochava, Inc.* offers insight on some of the hot issues in the realm of data privacy for businesses operating in the digital space, particularly those involved in data brokering and app development.

Kochava, Inc., the defendant, is a data broker that provides a software developer kit (SDK) to app developers to assist them in developing their apps. In return, the app developers allow Kochava to obtain location data from app users via its SDK. Kochava then sells customized data feeds to its clients, such as Airbnb, Disney+, and Kroger, to assist in advertising and analyzing foot traffic at stores or other locations.

The plaintiff, a California resident, filed a putative class action suit on behalf of similarly situated California residents, alleging that Kochava collected personal information, geolocation data, and communications from his cellular telephone without his consent. This data included visits to sensitive locations, advertisement clicks, and specific communications from SDK-installed apps. This conduct, according to the plaintiff, violated CIPA and the Computer Data Access and Fraud Act (CDAFA), amongst other laws.

Kochava moved to dismiss, arguing that the plaintiff had failed to plausibly allege standing (that is, actual or concrete injury from the alleged eavesdropping) and plausible claims under California law. The court found that the plaintiff had legal standing to pursue his claims, rejecting Kochava's argument that the plaintiff had consented to the data collection through the installation of the SDK-embedded third-party apps on his phone. The court noted that the plaintiff was not only unaware of his ability to opt-out but also unaware of Kochava's data collection altogether.

The court also found that Kochava's data collection practices could potentially violate California's privacy laws. The plaintiff alleged that Kochava had circumvented attempts to safeguard users' privacy, such as Apple's framework that requires users to affirmatively opt-in to allowing data brokers to track their device unique identification number for advertisers on their iPhones. The court found that the information Kochava allegedly secretly collected, including geolocation data, sexual orientation, and medical conditions, is the exact type of personal information users regularly expect to keep private absent knowing and voluntary consent and disclosure.

This decision is notable for businesses that collect and use personal data. Candidly, the court's decision finding that the plaintiff had standing and plausibly alleged injury is no surprise. Challenging standing is a hot litigation trend owing to the Supreme Court's semi-recent decision in *Ramirez v. TransUnion*. But the reality is that the Court's decision in *Ramirez* involved relatively narrow and specific facts. While challenging standing may be plausible depending on the specific circumstances, it is-in the author's opinion-generally a waste of time unless the alleged legal violations are truly technical in nature. And (allegedly) secretly monitoring someone's online activity and selling information on their sexual proclivities to interested third party buyers? Eh, all cases are fact dependent, but that seems hard to sell as a mere "technical" statutory violation.

Regardless, with respect to the underlying allegations themselves, *Greenley* underscores the importance of understanding and complying with privacy laws and regulations, which require businesses to inform individuals that their personal data is being collected or stored and to obtain a written release from the individual. Businesses that fail to comply with privacy laws could face lawsuits from individuals who claim that their personal data was collected or used without their consent.

Businesses should review their data collection and use practices to ensure they are in compliance with applicable laws and regulations. They should also consider seeking legal advice to understand the potential risks and liabilities associated with the use of personal data. As the legal landscape continues to evolve, staying informed and proactive is the best defense.

For more information on this topic, contact David M. Krueger at dkrueger@beneschlaw.com or 216.363.4683.