ad exchanger

May 15, 2017

MARKETERS, WHEN USING GEOFENCING TO WATCH CONSUMERS, REGULATORS MAY BE WATCHING YOU

by Gary A. Kibel

To marketers, geofencing sounds like a perfect way to target the right consumer, at the right time, with the right ad.

To consumers, geofencing may sound a bit Big Brotherish.

To regulators, geofencing sounds like a practice that requires greater scrutiny.

One advertising agency recently discovered the hard way that geofencing is indeed a sensitive practice that is attracting the interest of regulators. The Massachusetts attorney general recently settled an investigation into the geofencing practices of Copley Advertising. The agency used geofencing technology to tag consumers' smartphones when entering a specific geographic location to display ads on the devices for up to 30 days.

Sounds reasonably harmless and simple to implement technically, but the attorney general was concerned that consumers did not have any notice about these practices. Further, specific implementation of this service raised eyebrows. The agency specifically tagged users when they entered women's reproductive health clinics and later targeted the devices with anti-abortion ads while the users were near or in the waiting rooms of such facilities.

The attorney general believed that the practice of collecting a user's private health status for ad targeting purposes without users' knowledge or consent was unfair or deceptive in violation of Massachusetts law. In the settlement, the agency agreed not to geofence users in the vicinity of any medical center located in Massachusetts to infer health status, medical condition or medical treatment.

It is widely acknowledged in the industry that precise location data is sensitive, so any practice that relies on this data should consider how it is being implemented and how users are being put on notice.

In another example, Uber is under investigation by the Department of Justice in connection with its Greyball program, where Uber used location data to identify and circumvent government regulators who may be examining Uber's practices. While somewhat the reverse of ad targeting, the users had no idea that they were being excluded from features of the service based on their location or other data.

Most people agree that sensitive data is always just that – sensitive. However, there is not often agreement on what constitutes sensitive data or how consumers should be informed about its use.

The Digital Advertising Alliance (DAA) defines sensitive data as personal information of children under 13, financial account numbers, Social Security numbers, pharmaceutical prescriptions or medical records; precise location data is also treated with a higher standard. The Network Advertising Initiative has a broader definition of sensitive data, and calls out precise location data as well. The Federal Trade Commission, in its recent cross-device tracking report, called out the DAA sensitive data definition as too narrow.

All ad tech providers and customers should ask themselves three simple questions prior to implementing any technology that relies upon location-based services: How do users get notice of the service? How do users get into the service? How do users opt out of the service?

If those questions cannot be easily answered, they should carefully consider if it is worth the risk to proceed.

ABOUT THE AUTHOR

Gary A. Kibel is a partner in the Digital Media, Technology & Privacy Practice Group of Davis & Gilbert. Mr. Kibel advises interactive companies, advertising agencies, media providers and other commercial entities regarding transactions for interactive advertising, behavioral advertising, social media, user-generated content, viral marketing, mobile marketing, affiliate marketing, gaming and other emerging products and services. He also serves as general counsel to the Performance Marketing Association. He may be reached at 212.468.4918 or gkibel@dglaw.com.