Chicago Daily Law Bulletin®

Volume 163, No. 123 Serving Chicago's legal community for 162 years

Geofencing to track consumers raises regulators' concerns

Geofencing is fast becoming a popular tool in the marketer's digital tool box. A geofence is a virtual boundary set up in location-aware applications, which trigger notifications or other actions when an individual with a location-aware device (such as a smartphone) enters or leaves the designated area.

Once the geofence is triggered, the marketer can both collect location-based information from the device and attempt to send or display an ad in an open app or web browser. For both online and "brick and mortar" advertisers, geofencing provides a new and unique opportunity to target consumers with ads and promotions as well as better tailor product offerings.

The use of geofencing also has caught the eye of regulators concerned with consumer privacy.

Massachusetts recently barred a digital advertising company from using geofencing technology at or near the state's health-care facilities to gather information about consumers' medical status or treatment.

In April, the state settled charges that Copley Advertising LLC violated consumer protection laws by setting up mobile geofences near reproductive health centers in several states to send targeted anti-abortion advertisements to "abortion-minded women" on their mobile devices when they entered the facilities.

Copley Advertising, a company based in Massachusetts, was commissioned in 2015 to direct targeted advertisements to women entering 140 reproductive health centers in Columbus, Ohio; New York; Pittsburgh; Richmond, Va.; and St. Louis. When a woman entered the geofenced areas, Copley tagged her mobile device ID and sent advertisements to her device that included texts such as "Pregnancy Help," "You Have Choices" and "You're Not Alone."

If the woman clicked on the text, a webpage popped up with information about abortion alternatives and access to a live web chat with a "pregnancy support specialist," according to an April 4 statement from the U.S. Attorney General's Office. And, the ads could be sent to the individual's device for up to 30 days after visiting the clinic.

Massachusetts consumer protection laws prohibit tracking a consumer's location near or inside medical facilities, disclosing that location to third-party advertisers and targeting the consumer with potentially unwanted advertising based on assumptions about his or her medical condition, all without the consumer's consent.

While Copley Advertising had not set up geofencing campaigns at or near reproductive health clinics in Massachusetts, the settlement prevents the company from ever doing so.

Geofence technology is used in an increasing variety of applications. For example, the Apple iPhone's Siri assistant uses geofencing to let users set up location-based reminders. Therefore, if you want to remember to take something out of the freezer for dinner when you get home, Siri can send you a reminder that's triggered when you walk in the door.

Businesses are also using geofencing to anticipate customers' needs, or at least suggest something customers in the vicinity might need or want. CVS Health uses geofencing to send customers ExtraCare rewards on their phones as soon as they cross the threshold of one of the company's pharmacies.

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law, as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.

Uber has deployed geofences at travel hotspots like Los Angeles International Airport to let its users know how many vehicles are ready and waiting to serve them.

The key issue in the Copley Advertising settlement is consent. Customers of businesses like Apple, CVS and Uber that use geofencing to offer services and deals have agreed to being identified and tracked by using the companies' mobile apps. Copley Advertising did not give women entering health clinics the chance to opt into or out of being sent antiabortion messages on their smartphones. Further, the targeted women could continue to receive the unwanted advertising for up to a month.

Geofence technology is used in an increasing variety of applications.

Geofencing has been around for several years, but the Federal Trade Commission has yet to offer specific guidance for advertisers that use the technology. The agency does outline how online advertisers can help protect consumers' sensitive personal information in its 2009 report, "Self-Regulatory Principles for Online Behavioral Advertising."

The FTC defines "online behavioral advertising" as "the tracking of a consumer's online activities over time — including the searches the consumer has conducted, the web pages visited and the content viewed — in order to deliver advertising targeted to the individual consumer's interests."

The FTC definition may only loosely cover geofencing, but the principles the agency offers are broad enough to help advertisers ensure their use of the technology doesn't violate consumer privacy.

First, the collection of consumer data for behavioral-based advertising should be accompanied by a "clear, concise, consumer-friendly, and prominent statement" that consumers' information is being collected and used to tailor advertisements for them and that the consumer can opt out.

Second, any consumer data collected should be reasonably secured and retained "only as long as is necessary to fulfill a legitimate business or law enforcement need."

Third, companies should collect sensitive data for behavioral advertising only after obtaining consumers' affirmative express consent to receive such advertising. Finally, if a company makes any material changes to its existing privacy promises, it should get affected consumers' affirmative express consent to the changes.

It's easy to see where Copley Advertising ran afoul of the FTC's broad privacy recommendations. But while the Massachusetts settlement focused on an advertising firm, they aren't the only parties responsible for protecting consumer privacy.

In response to the rise of smartphones and other mobile devices, the FTC released a 2013 report, "Mobile Privacy Disclosures: Building Trust Through Transparency," which addressed, among other things, the issue of who should be giving consumers control over their privacy. Should it be advertisers? Operating system providers? App developers?

According to the FTC, it's all of the above.

Operating system providers or platforms serve as the interface between users and potentially hundreds of thousands of apps, giving app developers and others access to a huge amount of consumer data from mobile devices, including geolocation information. Therefore, platforms should play a key role in communicating privacy protection information to consumers.

The FTC urges platforms to provide "just-in-time" disclosures to consumers and get their affirmative express consent before allowing apps to access sensitive content like geolocation, contacts, photos, calendar entries or the recording of audio or video content. The agency suggests that platforms: Develop a one-stop dashboard that allows consumers to review the types of content accessed by the apps they download; offer Do Not Track (DNT) mechanisms for smartphone users to prevent tracking by ad networks; and give consumers clear disclosures about the extent to which platforms review apps before making them available for download.

App developers should develop privacy policies that are easily accessible through the app stores, provide just-in-time disclosures and get affirmative express consent before collecting and sharing sensitive information, to the extent the platforms have not already done so, and improve coordination with advertising networks and other third parties, such as analytics companies, that provide services for apps in order to provide accurate disclosures to consumers.

The FTC also recommends that advertising networks work with app developer trade associations, usability experts and privacy researchers to develop short-form disclosures for app developers, promote standardized privacy policies so that consumers can compare data practices across apps and educate app developers about consumer privacy issues.

With rapidly evolving smart technology at advertisers' disposal, consumer privacy policies issued by all parties involved will need to keep pace.

The Copley Advertising case raised red flags because of the highly sensitive issue of health-related consumer privacy involved. The future of location-based technology in advertising is likely to include increasingly sophisticated relationships among advertising agencies, brands and consumers — and the FTC and other regulators will be watching for the impact on consumer privacy.