Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Transparency In Consumer Tracking Can Ward Off Legal Woes

By **Allison Grande**

Law360, New York (June 12, 2014, 2:42 PM ET) -- Federal lawmakers, regulators and class action plaintiffs have recently stepped up their scrutiny of online and in-store consumer location tracking by retailers and others, but attorneys say the self-regulatory schemes favored by companies may be enough to stave off legislation and limit liability related to the covert data-gathering method.

In the Senate, lawmakers are currently weighing a bill proposed by Sen. Al Franken, D-Minn., in March that would enhance privacy protections for the commercial use of location information by companies. During a hearing last week, stakeholders including the Federal Trade Commission voiced their support for requiring more prominent notice and opt-in consent for tracking activities, while the National Retail Federation and others expressed concerns that the changes would stifle innovation without addressing any actual harms.

Outside Capitol Hill, regulators and consumers have also been paying close attention to the growing practice of retailers, advertisers and others tracking individuals' movements in-store and online to improve marketing strategies or provide better staffing. The FTC held a seminar on mobile device tracking in February, and plaintiffs have lodged class actions against companies such as Apple Inc. and Microsoft Corp. over allegedly unlawful smartphone tracking.

The industry has responded with various voluntary codes and principles aimed at better explaining how they are collecting location data and for what purpose it is being used. While the push for more formal regulation continues, attorneys say that companies' current voluntary efforts to be more transparent about their practices are likely to be the most effective way to address concerns and dodge claims that their tracking has harmed consumers.

"The landscape right now suggests that disclosure goes a long way toward protecting yourself, whether you are an online retailer or a brick-and-mortar retailer," said Yaron Dori, the co-chair of Covington & Burling LLP's communications and media practice group. "As long as disclosures in privacy policies or posted in stores about what is occurring are clear enough, it's hard to see what sort of law or regulation a company would be violating."

Because there are no laws or regulations that specifically mandate how far companies can go to keep track of consumers' activities and preferences, companies are basically free to explore innovative ways to more effectively connect with their customers. However, attorneys noted that even though there are no formal restrictions, tracking practices are not without risks.

"The biggest issue that overarches all of this is the competition between the ick factor on the customers' side and retailers' desire for relevance," said Craig Cardon, the co-chair of Sheppard Mullin Richter & Hampton LLP's privacy and data security group. "When companies start explaining how they are using the information they collect to be more relevant to the consumer, then it becomes less creepy, and consumers understand what is happening and why."

To date, the regulatory enforcement proceedings and class actions that have been brought over location tracking have centered on violations of common law or statutes that prohibit companies from deceiving consumers or accessing their devices without their knowledge.

On the class action side, consumers have floated allegations such as that Apple unlawfully collected and stored geolocation data on its devices; that Microsoft illegally gathered location information from users' smartphones; and that online analytics giant comScore Inc. installed data-harvesting software on Web users' computers without their consent.

However, with the exception of the comScore case — which was certified as the largest-ever privacy class action in April 2013 and was recently settled by the company for $14 million — companies for the most part have been able to escape the class actions because of plaintiffs' inability to demonstrate any actual harm caused by the data-collection efforts, an outcome that attorneys say should encourage retailers to be more forthcoming about their practices.

"The biggest risks and where most of the claims are coming from is from doing something different than what you publicly say you're doing," Cardon said. "The key is to be transparent and make sure disclosures aren't buried in miles of legalese, but rather that they are explaining it up front and engaging consumers."

The same approach can help avoid backlash from the FTC, which has pursued enforcement actions concerning location tracking practices using its authority under Section 5 of the FTC Act to police unfair and deceptive acts or practices.

"Right now, the FTC is taking the position that if a company engages in surprising, undisclosed tracking of people, that that might be an unfair or deceptive practice," said Jim Halpert, the head of DLA Piper's privacy and security practice. "If you're doing something that users might not expect, it would make sense to make sure that users are informed or have the ability to say no."

To date, the commission has used its authority to bring claims including that mobile messaging service company Snapchat Inc. broke its promise not to collect geolocation data and that the maker of a popular flashlight app secretly shared users' location data with advertisers, and attorneys expect that, given a recent ruling by a New Jersey federal judge backing its authority to bring data security claims against Wyndham Worldwide Corp., that it will continue to use Section 5 to aggressively pursue companies that mislead consumers about their tracking practices.

Given the possible liability risks, retailers and other companies that employ consumer tracking should look to self-regulatory standards that have been developed in recent months as a guidepost for their practices, attorneys say.

The Digital Advertising Alliance is in the process of enforcing self-regulatory principles that require mobile apps to give clear, meaningful and prominent notice if transferring geolocation data to third parties, while a group of data analytics companies including Euclid Inc. and Mexia Interactive Inc. in

October published a first-of-its-kind code of conduct for tracking retail customers' in-store movements in an effort to soothe concerns that the monitoring technology is often operated without the proper consent, disclosures or security controls.

"There is something to be said for allowing the industry to experiment," Foley Hoag LLP attorney Christopher Hart said. "There's a lot more flexibility in implementing self-regulatory principles that can more easily adapt to changes in technology."

The industry has also worked to craft technical specifications to curb widespread consumer tracking. Apple Inc. last week announced that its newest mobile operating system will include a feature that automatically randomizes the unique device identifier that retailers and others pick up from phones trying to connect to wireless networks, and the World Wide Web Consortium's tracking protection working group in April overcame years of bickering to release a model for a standardized signal that consumers can use to tell servers they don't want their data collected across different websites.

"If the gatekeepers are making it harder technically to track people on mobile phones and elsewhere, then it doesn't matter as much what the formal law or policies or best practices are," Halpert said.

While Franken is continuing to aggressively push his location privacy bill, which passed the Senate Judiciary Committee during the last congressional session, attorneys predict that the widespread support for provisions meant to curb uses of location information by stalkers won't be enough to encourage more backing for the commercial provisions.

"Typically, where privacy legislation has been successful in the past is where it's not trying to regulate a specific technology but rather being used to address a specific harm," said Paul Martino, the co-leader of Alston & Bird LLP's privacy and security practice. "What is likely to come out of these efforts is a more narrowly focused bill that principally addresses the specific harms that cyberstalking raises, while leaving out the commercial provisions."

If any type of legislation related to commercial location tracking were to pass, it would likely follow a model similar to a bill approved by California lawmakers last year that requires companies to disclose how they respond to signals that indicate a consumer's online tracking preference.

"The recent California law is a nice balance, because it focuses on telling consumers what a company does as opposed to the model of setting prohibitions, which is more common in Europe," Cardon said.

But even if formal legislation continues to lag, attorneys say, the risk of raising the ire of consumers is likely to keep tracking practices from running wild.

"What is often forgotten is the real market constraints facing companies," Martino said. "Stores won't be in business very long if they do things that cause consumers to lose trust in them. Consumers will vote with their feet if they're not comfortable with how their data is being used."

--Editing by Jeremy Barker and Katherine Rautenberg.
