Less than 10 days after announcing its complaint and proposed settlement against location data broker X-Mode, the Federal Trade Commission (FTC) followed its recent spate of enforcement in the location and sensitive data space with the announcement of another enforcement action and proposed settlement with InMarket Media, Inc. (InMarket).

In some ways, the InMarket complaint and proposed order bear striking similarities, but there are key differences as well.

InMarket's Practices

Though the FTC made headlines with its statement about prohibiting InMarket from selling or sharing consumer location data, unlike X-Mode, the FTC did not allege that InMarket sells location data at all. Instead, the FTC's complaint against InMarket is grounded on InMarket's *use* of location data to show targeted ads, including by creating audience segments such as "well-off suburban moms," "Christian church goers," "single parents," and "affluent savers," which advertisers could use to target ads to consumers. The FTC also did not allege that InMarket sold data to government actors for national security purposes, as it did with X-Mode. Thus, whereas the FTC's allegations against X-Mode were largely rooted in the fact that purchasers of its data could use it to reidentify individuals or track their visits to sensitive locations, its allegations against InMarket are based on the collection of sensitive information for advertising purposes alone. The FTC also took issue with InMarket's five-year retention period for location data, contending that such retention "increases the risk that this sensitive data could be disclosed… and linked back to the consumer."

Alleged Failure To Obtain Sufficient Consent

Like X-Mode, InMarket obtained location data directly from users of its own apps and through an SDK embedded in other apps. As with its X-Mode complaint, the FTC found that InMarket's consent mechanism for both methods was inadequate and that the failure to obtain sufficient consent was unfair. While X-Mode did notify users of its apps that their location data would be used for advertising purposes (but neglected to mention sales to government actors for other purposes), InMarket did not mention any advertising uses at all, and instead suggested that location would be used for functionality purposes only. Similarly, while X-Mode suggested consent language to the developers of apps that used its SDK, X-Mode required them to comply with applicable law only. The FTC found that as a result, InMarket "does not know whether users of hundreds of third-party apps that incorporate the InMarket SDK were informed of their data being collected and used for targeted advertising" and noted that several sought consent using incomplete and misleading disclosures. Thus, the FTC alleged, InMarket obtained and used location data without informed user consent, resulting in likely consumer injury in the form of "loss of privacy about the day-to-day movements of millions of consumers and an increased risk of disclosure of such sensitive information."

Mandated Supplier Assessment Program

The relief mandated in the X-Mode and InMarket orders are quite similar, including the obligation to establish a Supplier Assessment Program under which they must conduct affirmative due diligence to ensure that developers that use their SDK provide sufficient notice and obtain sufficient consent. This requirement suggests that the FTC does not consider contractual language sufficient and may imply an obligation on those that collect highly sensitive data (or possibly other forms of personal information) to adopt and maintain programs designed to ensure proper transparency and choice.

Conclusion

The complaint and order against InMarket demonstrate that the FTC's interest in location data extends beyond those that sell location data and exists even in the absence of harm or suggestion that the data could be linked to consumers' real-life identities. Framing the "substantial injury" from the collection of location information for marketing purposes with insufficient consent as "loss of privacy about the day-to-day movements of millions of consumers and an increased risk of disclosure of such sensitive information," the FTC has shown that only clear consent to a notice that fully articulates uses and disclosures of location data for advertising (or other relevant purposes) will suffice.

This action underscores that those that collect location data from and about consumers must ensure that they have complete and accurate notices and consent mechanisms. The action also makes it abundantly clear that those that process location data should assess their data retention practices and be able to articulate a business

reason for retaining location information.

Authors

Meredith B. Halama

Partner
MHalama@perkinscoie.com 202.654.6303

David Hume

Associate
DHume@perkinscoie.com

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field.

View the blog