Articles + Publications | January 11, 2024

Locke Lord QuickStudy: Consent Has Never Been More ?Important: Take-Aways From the FTC Settlement Relating to ??Tracking Technologies

Locke Lord LLP

WRITTEN BY

Tara L. Trifon | Thomas J. Cunningham

RELATED OFFICES

Hartford | West Palm Beach

Litigation over tracking tools, such as cookies and pixels, has become commonplace over the past few years. In general, plaintiffs' claims revolve around the collection and sharing of data through session replay and/or chatbot tools that collect information about a user's interaction with a web page. Lawsuits relating to the tracking technologies have been brought against individual companies and data brokers alike, typically asserting wiretap violations (in the relevant jurisdictions) and invasion of privacy claims.

Now the Federal Trade Commission wants in on the action. On January 9, 2024, the FTC announced an unprecedented settlement with a data broker relating to individual users' geolocation data that, among other things, will restrict the data broker's use of data for the next twenty (20) years. While the FTC was particularly focused on the data broker's alleged practice of collecting and selling data that could be used to track a user's visit to sensitive locations (including healthcare facilities, churches, and schools), the impact of this settlement is likely to be far-reaching.

Consequently, as we begin a new year that will undoubtedly include more cookie and pixel litigation, it is a good time to confirm that any privacy policy, terms of use, or contract meets the requirements articulated in the recent FTC decision and order. In particular, businesses should focus on obtaining that consumer consent to the collection and to the transfer of any personal data before it is shared with a third party.

The FTC's Allegations

According to the FTC's recent complaint, one of the largest U.S. location data brokers sells and/or licenses consumers' raw location data to hundreds of clients, including advertisers, software as a service companies, analytics firms, consulting firms, research organizations, and private government contractors. Those third-party companies purportedly use that information for their own purposes, such as marketing and brand analytics, or they share the data with their own customers. According to the FTC, the data broker utilizes more than 10 billion location data points from all over the world.

The FTC specifically alleged that the raw location data given to the data broker's clients includes mobile devices' unique persistent identifier, along with the latitude, longitude, and timestamp of the observations. This information

allows a company to match a user's mobile device with the locations the user visited. The FTC claimed that the data broker advertises that the location data is 70% accurate within a 65-foot (or less) radius. The FTC also alleged that the data broker itself analyzes the location data and creates "audience segments." These "audience segments" include groups based on the characteristics purportedly revealed by the geolocation data, such as "Size Inclusive Clothing Stores" or "Military Bases," and this information is presumably shared with the data broker's clients.

What The FTC Claims The Data Broker Did Wrong

The FTC complaint sets forth seven different ways in which the data broker allegedly violated Section 5(a) of the FTC Act, prohibiting unfair or deceptive acts or practices. *See* 15 U.S.C. § 45(a):

1. Sale of sensitive data, particularly related to information about visits to sensitive locations;
2. Failure to honor consumer privacy choices by collecting and selling consumers' location data for the purposes of developing consumer profiles, surveilling the consumers, and targeting them with advertising, even if the consumer opted out of having their collection data used for these purposes;
3. Collecting/using consumers' location data without first obtaining the consumers' informed consent;
4. Collecting/using consumers' location data through third-party apps without taking reasonable steps to verify that the consumers consented to this practice;
5. Placing consumers into audience segments based on sensitive characteristics, such as visits to medical offices, for marketing purposes;
6. Failure to inform consumers that the location data could be provided to government contractors for national security purposes; and
7. Using consumer disclosures that mislead consumers about the purposes for which their location may be used, including failing to disclose that the information would be provided to government contractors for national security purposes.

Consent Order

In order to avoid further litigation on these issues, the FTC and the data broker entered into a consent order that will limit the data broker's practices for the next twenty (20) years. For instance, the data broker must impose limits on sharing data relating to certain sensitive locations and also implement procedures to ensure that consumers' location and identity are protected in certain circumstances. The data broker must develop a supplier assessment program to ensure that companies providing information to the data broker have obtained consent from their consumers. In addition, consumers must be provided with an easy way to withdraw their consent for the collection/use of their data and the deletion of any data that was previously collected. Consumers must also be given a conspicuous way to request the identity of any individuals or businesses to whom their data was given, or provide consumers a way to delete the personal location data from the commercial databases of all the recipients of the data. Furthermore, the data broker must establish and implement a comprehensive privacy program that is designed to protect the privacy of consumers' personal information.

This Settlement Will Likely Impact All Companies That Utilize Tracking Technologies

The agreement between the FTC and the data broker highlights some issues that will likely be included in future lawsuits (whether brought by the FTC or by consumers themselves). First, the FTC believes that there are, or should be, limits on how businesses can use a consumer's data. The FTC rejects the idea that a company can

use a consumer's personal information in any way it wants as soon as it has access to such data. Instead, a business should be required to obtain explicit consent from the consumer regarding the collection and sale of their information.

Second, the FTC's position is that if a business transfers consumer data to a third party, it needs to do more than impose a contractual limitation on how the third party can use the information. Instead, a company must take steps to ensure that a consumer gives consent for the collection and distribution of that data, including reviewing the disclosures, notices, and opt-in controls provided to consumers buy the third party. In other words, data brokers (or other entities that transfer data to third parties) will be held responsible for their clients' or vendors' compliance failures relating to data collection and distribution.

At the end of the day, the best way for a company to guard against future claims relating to tracking technologies is to make sure that it obtains appropriate consent from consumers. Thus, we recommend reviewing any privacy policies and terms of use to confirm that the information regarding the company's data sharing practices is conspicuous and written in language that can be easily understood. In addition, companies should also consider whether the website banners should address all tracking practices, not just the use of cookies. Lastly, we recommend reviewing any agreements with third parties to ensure that they satisfy the FTC's directive that a business take reasonable steps to confirm that the consumer has consented to the data transfer.

RELATED INDUSTRIES + PRACTICES

- Antitrust
- Corporate
- Financial Services
- Litigation + Trial
- Privacy + Cyber