DAVIS GILBERT

Privacy + Data Security

Choppy Waters: Recent Privacy Developments in Targeted Advertising on Both Sides of the Atlantic

The Bottom Line

- New state privacy laws are not the only challenges facing the ad tech industry.
- Regulators on both sides of The Pond are targeting the ad tech industry.
- Under these ever-changing developments, compliance grows ever more challenging for companies.

Recent privacy developments on both sides of The Pond make it clear that targeted advertising is becoming more challenging in both the United States and Europe. The latest Interactive Advertising Bureau (IAB) Europe's Transparency and Consent Framework (TCF) decision clarifies IAB Europe's role under the General Data Protection Regulation (GDPR) framework. Meanwhile, in the U.S., competing and shifting regulatory frameworks continue to foster uncertainty in the advertising technology landscape.

The Latest TCF Decision: IAB Europe May Operate as Joint Controller

The recent decision by the Court of Justice of the European Union (CJEU) provided clarity on IAB Europe's role within the TCF framework. The TCF is an industry-designed mechanism to facilitate obtaining a GDPR compliant legal basis to process data, such as cookies, within the ad tech ecosystem, underlying many targeted advertising practices.

In its ruling, the CJEU emphasized first that TCF consent strings do constitute personal data, when they can be linked with reasonable means to an identifier, like an IP address or device ID, and, second, that the IAB Europe is considered a joint controller (along with the TCF participants) when it creates and facilitates the usage of the strings by publishers and vendors.

In its ruling, the CJEU noted that the TCF provides specifications for its processing and, if IAB Europe influences the processing of the strings, IAB Europe acts as a joint controller. However, the CJEU clarified that IAB Europe is not always a joint controller. Where TCF participants, including publishers and vendors, subsequently process data for independent purposes, including digital advertising, personalization or measurement, IAB Europe is not a joint controller, as it has no control over such processing.

In the next phase of the ongoing IAB Europe saga, the Belgian Market Court will continue its review of IAB Europe's substantive arguments in the wake of the CJEU's decision.

FTC Finds Sensitive Data Includes Location and Browsing Data

On the American side of the Atlantic Ocean, the Federal Trade Commission (FTC) has ratcheted up the confusing compliance landscape for companies engaging in targeted advertising. Three recent FTC enforcement actions – involving Avast, X-Mode Social, and InMarket, respectively – demonstrate the FTC's focus on sensitive data handling practices, which now includes browsing and location data.

In January, the FTC settled with X-Mode and InMarket over claims concerning both data aggregators' handling of consumer location data. According to the FTC, the companies each mishandled consumer location data by collecting precise location data from consumer phones and using the data in manners not disclosed to consumers. X-Mode allegedly sold location data to government contractors without consent, while InMarket allegedly sorted consumers' location data into audience segments, like "parents of preschoolers" or "Christian Churchgoers."

While there is no federal comprehensive privacy law in the U.S., the FTC uses its authority under the FTC Act to regulate "deceptive and unfair" practices to enforce its view of privacy compliance. There are numerous state privacy laws that consider precise location information to be sensitive data, warranting additional protections. The X-Mode and InMarket settlements reflect the consensus that precise location information is sensitive data.

In late February, the FTC announced its settlement with security software company Avast, who, according to the FTC, unfairly sold consumers' "granular and re-identifiable browsing information" that it collected through its software and browser extensions. According to the FTC, Avast publicly stated that it would only disclose consumer browser data in an aggregated and anonymous format.

All three recent FTC settlements involving consumer data underscore two key themes that apply to those in the digital advertising ecosystem: First, precise geolocation data and browsing data can constitute sensitive personal data and, second, transparency about data handling practices, especially sensitive data-handling practices, must be communicated to consumers in a clear and understandable way.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Emily Catron

Associate
212 468 4857
ecatron@dglaw.com