Feds Order Software Provider to Pay $16M: 3 Compliance Tips for Businesses on Website Data Collection and Targeted Ads

Insights
7.02.24

Federal officials recently banned a software provider from selling, disclosing, or licensing any web browsing data for advertising purposes – and ordered to pay $16.5 million. The Federal Trade Commission (FTC) alleged that Avast unfairly collected, stored, and sold consumers' browsing information without adequate consent or notice. The FTC also said the company deceived consumers by claiming its software would protect their privacy by blocking third-party tracking. Additionally, the company failed to adequately inform consumers that it would sell their detailed, re-identifiable browsing data, according to the FTC's June 26 order. Notably, this is just one of many recent privacy and security enforcement actions brought by the FTC against companies that collect, store, or sell user data — which highlights the importance of reviewing your website data collection practices and use of third parties for online targeted ads. Read on to review our three top tips to help you stay compliant.

1. Consider Obtaining Affirmative Express Consent

When should you obtain consent? You should consider obtaining affirmative express consent from consumers at the point of data collection if you:

- collect browsing information from website visitors through cookies or other technology; and
- wish to use that information to target ads to those website users on social media or other third party websites, or wish to sell that information to third parties or share it with affiliates or third parties without restrictions on how the data will be used.

What is "affirmative express consent"? This means an individual freely gives specific, informed, and unambiguous consent following a clear and conspicuous disclosure. The individual should be informed of what information will be used, sold, licensed, transferred, shared, or disclosed – and told the purpose.

What is a "clear and conspicuous" disclosure? This generally means you are not burying the language in the middle of lengthy privacy policies, terms of service, terms of use, or other similar document. Rather, you are placing the disclosure where the consumer is more likely to see it before starting to browse through the website. In defending against claims of deceptive practices, critical factors include where the disclosure is placed on the website and how it is displayed to consumers.

According to the FTC and some state regulators, hovering over, muting, pausing, or closing a piece of content does not constitute affirmative express consent.

Are cookie consent pop-ups enough? These may be insufficient if the language is generic and doesn't actually tell consumers that their browsing data may be sold or shared for targeted ad purposes. Furthermore, it may be problematic if browsing data is already being collected and shared automatically before the consumer gets a chance to read and click on the cookie consent banner. These are things you should review with your consumer privacy counsel.

What are the benefits of obtaining affirmative express consent? Some state privacy laws require opt-in consent. But even if the states applicable to your operations do not, you should consider a strategy that goes beyond minimum compliance with current requirements. After all, the FTC takes enforcement action against businesses for practices it considers to be deceptive and unfair.

For example, the FTC has recently focused on businesses that collect data that can identify and track website users across the internet. You could get in trouble if you sell or monetize the data without sufficiently disclosing that you are doing so and without giving website users the opportunity to make an informed choice about whether to consent to having such data about them be sold or shared in this manner.

If your business shares browsing data with third parties, you'll want to minimize the risk of state or federal regulators alleging that your website engages in deceptive or unfair practices. So, you should consider implementing a process for obtaining affirmative express consent for selling, licensing, transferring, sharing, or otherwise disclosing to a third party any of the following:

- browsing data collected by the business;
- information derived from or incorporating the browsing data; or
- models or algorithms derived from the browsing data.

These are the items the FTC identified in its June 26 order against software provider Avast.

2. Don't Be Misleading

Businesses should ensure that their websites (including privacy policies, terms of service, and cookie banners) do not make any express or implied misrepresentations to the consumer about any of the following:

- The purpose for collection, use, disclosure, or maintenance of consumer information;
- The extent to which consumer information is aggregated or anonymized;
- The extent to which you collect, use, disclose, or maintain consumer information, or otherwise protect the privacy, security, availability, confidentiality, or integrity of consumer information.

Consumer information does not only include browsing information, but also names, addresses, contact information, financial information, a persistent identifier, and geolocation information (IP address).

3. Review Your Storage and Retention Policies and Practices

Is browsing information aggregated or anonymized when in storage? The FTC has taken the position that browsing information should be aggregated or anonymized when in storage, rather than maintained in a form that is granular and makes it re-identifiable (meaning the data can be traced back to the individual).

Can third parties track specific users? Even if your business is incapable of using the browsing data to identify and track consumers, sometimes it can be used in such a manner by third parties, like data brokers. Therefore, you should assess whether third parties that receive the data would be able to track specific users or associate specific users — and their browsing histories — with other information.

Are you obtaining consent related to storage? According to the FTC, businesses should obtain affirmative express consent to both the storage and method of storage of consumers' browsing data.

How long are you storing such data? The FTC has also indicated that businesses should not be storing browsing data indefinitely.

Conclusion

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team, or the Privacy and Cyber Practice Group. Fisher Phillips will continue to monitor consumer privacy law developments and will provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

Related People

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Alexandra Volpicelli
Associate
415.926.7650
Email

Service Focus

Consumer Privacy Team

Counseling and Advice

Privacy and Cyber