AN A.S. PRATT PUBLICATION
OCTOBER 2024
VOL. 10 NO. 8

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

# Pratt's Privacy & Cybersecurity Law Report

**VOLUME 10** **NUMBER 8** **October 2024**



LexisNexis®

**QUESTIONS ABOUT THIS PUBLICATION?**

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)



*An A.S. Pratt Publication*
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

# *Editor-in-Chief, Editor & Board of Editors*

*Pratt's Privacy & Cybersecurity Law Report* is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.  For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

# Software Provider Ordered to Pay $16 Million: 3 Compliance Tips for Businesses on Website Data Collection and Targeted Ads

***By Usama Kahf****

*In this article, the author offers three tips to help companies that collect, store or sell user data comply with Federal Trade Commission privacy rules.*

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 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 author, an attorney with Fisher Phillips, may be contacted at ukahf@fisherphillips.com.

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 does not 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 will 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.[1]

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/202_3033_-_avast_final_consent_package.pdf.

## 2. DO NOT 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.