AN A.S. PRATT PUBLICATION
MARCH-APRIL 2025
VOL. 11 NO. 3

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

**EDITOR'S NOTE: BEST PRACTICES**
Victoria Prussen Spears

**7 BEST PRIVACY PRACTICES FOR COMPANIES WHEN USING GEOLOCATION TOOLS TO TRACK WORKERS**
Kate Dedenbach and Usama Kahf

**DOES YOUR AI CHATBOT COLLECT BIOMETRIC DATA?**
Shani Rivaux, Catherine Perez, Jeewon K. Serrato and Shruti Bhutani Arora

**DIGITAL WIRETAPPING LITIGATION: TOP 5 SURPRISING TAKEAWAYS**
Kate Dedenbach and Usama Kahf

**FEDERAL TRADE COMMISSION CRACKS DOWN ON SELLING SENSITIVE LOCATION INFO; RESTRICTS USE OF CONSUMER DATA FOR THE FIRST TIME**
Bess Hinson-Greenspan, Haylie D. Treas and Brandon L. Lewis

**SECURITIES AND EXCHANGE COMMISSION SETTLES WITH COMPANIES OVER CHARGES RELATING TO CYBERSECURITY DISCLOSURES**
Eric S. Wu, Pavel (Pasha) A. Sternberg and Mary Ann H. Quinn

**U.S. DEPARTMENT OF JUSTICE AND U.S. DEPARTMENT OF HOMELAND SECURITY'S CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY ISSUE NEW NATIONAL SECURITY PROGRAM TO REGULATE FOREIGN ACCESS TO SENSITIVE DATA**
Megan L. Brown, Duane C. Pozza, Kathleen E. Scott, Jacqueline F. "Lyn" Brown and Sydney M. White

# Pratt's Privacy & Cybersecurity Law Report

**VOLUME 11** **NUMBER 3** **March-April 2025**

**Editor's Note: Best Practices** 75
Victoria Prussen Spears

**7 Best Privacy Practices for Companies When Using Geolocation Tools to Track Workers** 77
Kate Dedenbach and Usama Kahf

**Does Your AI Chatbot Collect Biometric Data?** 81
Shani Rivaux, Catherine Perez, Jeewon K. Serrato and Shruti Bhutani Arora

**Digital Wiretapping Litigation: Top 5 Surprising Takeaways** 85
Kate Dedenbach and Usama Kahf

**Federal Trade Commission Cracks Down on Selling Sensitive Location Info; Restricts Use of Consumer Data for the First Time** 88
Bess Hinson-Greenspan, Haylie D. Treas and Brandon L. Lewis

**Securities and Exchange Commission Settles With Companies Over Charges Relating to Cybersecurity Disclosures** 92
Eric S. Wu, Pavel (Pasha) A. Sternberg and Mary Ann H. Quinn

**U.S. Department of Justice and U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency Issue New National Security Program to Regulate Foreign Access to Sensitive Data** 95
Megan L. Brown, Duane C. Pozza, Kathleen E. Scott, Jacqueline F. "Lyn" Brown and Sydney M. White

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

(2025–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.

# Federal Trade Commission Cracks Down on Selling Sensitive Location Info; Restricts Use of Consumer Data for the First Time

***By Bess Hinson-Greenspan, Haylie D. Treas and Brandon L. Lewis****

*In this article, the authors review recent Federal Trade Commission enforcement actions that, for the first time, prohibit the use of consumer data collected for a certain purpose to then be used for other purposes.*

The Federal Trade Commission (FTC) recently announced two significant enforcement actions – one against data broker Mobilewalla, Inc.,[1] and the other against data analytics provider Gravy Analytics, Inc. (and its subsidiary Venntel, Inc.)[2] for unlawfully collecting and selling location data. The FTC further explained in its Technology Blog[3] that it went a step further in its remedies as to Mobilewalla and restricted the use of consumer data collected during online advertising auctions to be used only for the purpose of participating in such auction processes, not for other purposes (such as selling to other advertisers and analytics providers).

The FTC reiterates in these actions that location data is sensitive data and that companies must not retain data for purposes outside of the original purpose(s) of collection, unless consumer consent is obtained. These actions highlight the FTC's increased scrutiny and regulatory efforts to protect consumer privacy, particularly concerning data collected through websites that reveal, or can reveal, visits to sensitive locations, such as healthcare facilities, places of worship and military installations.

## THE FTC'S CLAIMS

The FTC's complaint against Gravy Analytics asserts that the company obtained consumer location data from other data suppliers. Gravy Analytics utilized location signals and other information gathered from consumers' mobile phones, including a

* The authors, attorneys with Holland & Knight LLP, may be contacted at bess.hinson@hklaw.com, haylie.treas@hklaw.com and brandon.lewis@hklaw.com, respectively.

[1] FTC Press Release, "FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data," Dec. 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data?utm_source=govdelivery.

[2] FTC Press Release, "FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers," Dec. 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers?utm_source=govdelivery.

[3] FTC Technology Blog post, "Unpacking Real Time Bidding through FTC's case on Mobilewalla," Dec. 3, 2024, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla?mkt_tok=MTM4LUVaTS0wNDIAAAGXMdI851a-ZO2WG_qiBt6gDDd433m2CA-v6cDNN6JuhgjgC_XCQ8A3VKjqmPcovHOkCeRUMJnIRg0qWydMeu92_MccBilW7XeHzTDdcITJHMjG

unique Mobile Advertising ID. The FTC alleged that Gravy Analytics used geofencing to "identify and sell lists of consumers who attended certain events related to medical conditions and places of worship" and then "sold additional lists that associated individual consumers to other sensitive characteristics."[4] Gravy Analytics advertised its location data as being very precise, identifying a consumer within approximately 1 meter of precision.

Similarly, the FTC's complaint against Mobilewalla asserts that Mobilewalla collected unique consumer advertising identifiers along with the consumer's precise location data. Mobilewalla did not anonymize this data, rather, it "sold access to this raw data to third-parties, including advertisers, data brokers and analytic firms."[5]

Notably, the consumer data at issue in these two enforcement actions was likely collected through cookies, software development kits (SDKs) and similar technologies.

## REAL-TIME BIDDING AND FTC CONCERNS

Unlike Gravy Analytics, which obtained location data from other data suppliers, the FTC asserts that Mobilewalla unfairly collected and retained location information that it had obtained through an auction process. Many companies may not be aware that when they sell advertisement space on their websites or mobile apps, there is an auction process to sell that space where advertisers can bid to place their advertisements. The FTC refers to this as "real-time bidding" (RTB). According to the FTC, as a part of this auction process, the advertisers are sometimes provided "granular details like location or personal characteristics about the people downstream who could be the target of an ad."[6]

In the case of Mobilewalla, the FTC alleges that Mobilewalla retained the information it obtained during this auction process (even when it did not have the winning bid) and then turned around and sold this "raw data to third-parties, including advertisers, data brokers, and analytics firms."[7]

The FTC's action against Mobilewalla includes provisions restricting Mobilewalla's use of consumer data obtained through RTB, marking a significant step in regulating this complex practice.

The FTC highlighted in its enforcement action against Mobilewalla its concerns relating to RTB:

- *Invasive Data Sharing*. According to the FTC, RTB incentivizes the sharing of extensive consumer data, including precise location details, to

[4] FTC Gravy Analytics Press Release.
[5] FTC Mobilewalla Press Release.
[6] FTC Real Time Bidding Technology Blog post.
[7] FTC Mobilewalla Press Release.

attract higher bids for ad placements. This can lead to the widespread dissemination (and potential misuse) of sensitive information.

- *Cross-Border Data Transfers and Potential Data Misuse*. Data collected through RTB can be transmitted across geographic borders, which the FTC states raises concerns about potential misuse by foreign adversaries (including for "surveillance, blackmail, or social engineering campaigns").[8]

- *Lack of Control*. The rapid nature of RTB makes it challenging to control how data is used and retained by multiple parties involved in the bidding process. According to the FTC, there are few (if any) technical controls in place to ensure that advertisers who are bidding do not retain data in unintended ways. Notably, the FTC asserts that Mobilewalla retained data from auctions it did not win, which the FTC found was contrary to RTB exchange rules that prohibit the use of the consumer data for non-advertising purposes.

## KEY ACTIONS BY THE FTC

As a result of the FTC complaints against them, Mobilewalla and Gravy Analytics agreed in their respective settlement orders to implement several measures to ensure that both companies respect consumer privacy and protect sensitive data. These measures include:

1. *Prohibition on the Sale of Sensitive Location Data*. Mobilewalla and Gravy Analytics are prohibited from selling sensitive location data. This includes data that can identify individuals' visits to sensitive locations.

2. *Prohibition on the Collection of Consumer Data*. Mobilewalla is banned from collecting consumer data from online advertising auctions for purposes other than participating in such auctions, which, the FTC asserts, is the first time it has alleged that such a practice is an unfair act or practice.

3. *Data Deletion Requirements*. Both companies must delete all previously collected sensitive location data and implement measures to prevent the future collection or sale of such data.

4. *Comprehensive Privacy Programs*. Both companies must establish comprehensive privacy programs, including methods for consumers to request data deletion and to withdraw consent for data collection.

## TAKEAWAYS

In light of these recent FTC enforcement actions, companies should ensure they understand the types of data they are collecting, only use data for the purpose(s) it was

[8] FTC Real Time Bidding Technology Blog post.

collected and identify the third parties to which they disclose this data. In particular, companies should keep the following in mind:

1. *The FTC Views Location Data as Sensitive Data*. In its blog post about the Mobilewalla enforcement action, the FTC reiterates that "location data is sensitive data, full stop. Location data can reveal where we live, work, and worship, where we seek medical treatment, and even our presence at a protest or political event." Companies should therefore carefully consider their collection and use of location data and the risks associated with such data.

2. *Data Collected by Cookies and Similar Technologies*. Understanding what data is collected by cookies and how such data is used, shared or sold can be crucial for compliance with U.S. and international data protection laws and addressing FTC enforcement risk. Companies should also be aware of how advertisers may use data from cookies collected through their websites and mobile apps.

3. *Heightened FTC Scrutiny*. The FTC's actions against Mobilewalla and Gravy Analytics indicate an increase in regulatory scrutiny over the collection and sale of sensitive location data. Other companies engaged in such activities may be subject to similar enforcement actions.

4. *Compliance Is Key*. Ensuring compliance with data protection laws and obtaining explicit consumer consent for data collection, when required, are critical steps in mitigating legal and reputational risks.

5. *Transparency and Trust*. Clear communication with consumers about data collection and usage practices is essential in building and maintaining trust.

6. *Proactive Measures*. Implementing robust data management and privacy programs can help companies stay ahead of regulatory requirements and protect consumer privacy.

7. *Implement Data Deletion Protocols*. Establishing and enforcing data deletion protocols can help ensure that sensitive data is not retained longer than necessary.

## CONCLUSION

The FTC's recent enforcement actions against Mobilewalla and Gravy Analytics underscore the importance of developing compliant programs to protect consumer privacy and reduce regulatory enforcement risk.