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

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

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

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.

7 Best Privacy Practices for Companies When Using Geolocation Tools to Track Workers

By Kate Dedenbach and Usama Kahf*

In this article, the authors explore the privacy obligations that come with companies monitoring their employees via geolocation tools. They also provide the seven best practices to guide companies' actions.

Many employers have turned to geolocation tools like GPS devices to monitor employees' whereabouts and movements – especially those working remotely or in field-based roles. While these tools provide an effective way to boost operational efficiency, improve safety, and optimize resources, companies must ensure they respect workers' privacy rights when deploying them. This article explores the privacy obligations that come with monitoring employees via geolocation tools and provides the seven best practices to guide employers' actions.

OFFER INFORMED CONSENT

A cornerstone of privacy law is the requirement for informed consent. Companies must make their employees fully aware of the geolocation monitoring system and how it will be used. This includes:

- *Clear Communication*: Explicitly inform employees that they will be monitored using geolocation tools, specifying the scope, purpose, and duration of the monitoring. This communication should ideally occur at the beginning of the employment relationship or before implementing geolocation tracking.
- *Voluntary Consent*: While employees may be required to consent to geolocation tracking as a condition of their employment, it must be done in a transparent and voluntary manner. Coercion or the failure to fully disclose the nature of the tracking could mean there was no informed consent.

LIMIT THE PURPOSE

Ensure that geolocation tracking is conducted for legitimate business purposes. In many cases, this involves monitoring employees in roles that require travel, delivery, or site visits. Do not use geolocation tracking for personal reasons or to monitor employees'

* The authors, attorneys with Fisher Phillips, may be contacted at kdedenbach@fisherphillips.com and ukahf@fisherphillips.com, respectively.

non-work activities. Legitimate business purposes can include, for example, protecting company property or customer property, ensuring there is no timecard fraud, checking whether employees are actually taking required meal or rest breaks (in some states), managing employee performance and efficiency, and optimizing travel or delivery routes.

Various states require consent if companies monitor vehicles used for employment purposes. They vary from state to state and sometimes depend on such factors as whether the vehicle is company-owned or privately owned. Under many state laws, for example, employee tracking must be limited to specific and transparent purposes, such as ensuring productivity, protecting safety, or ensuring that business resources are being used efficiently. That said, while limiting the purposes for which geolocation data is used, disclosure should comprehensively identify all the purposes for which a company may use this data. Using geolocation data for purposes beyond the scope of the initial consent may violate anti-stalking laws.

CONSIDER PROPORTIONALITY AND MINIMIZATION

Geolocation monitoring must be proportionate to the goals it seeks to achieve – and ideally should minimize data collection.

- This means that a company should only collect data that is necessary for the intended purpose, and the tracking should not be overly invasive. For example, monitoring an employee's movement outside of working hours may be viewed as excessive and a violation of the employee's right to privacy.

- The Federal Trade Commission (FTC) has made it clear through various enforcement actions that it considers geolocation data to be sensitive location data. The FTC emphasizes that employers should use geolocation monitoring tools in a manner that minimizes data collection and is not unduly burdensome on employees' privacy. Similar data minimization requirements exist under the California Consumer Privacy Act (CCPA).

PROTECT DATA AND PROVIDE NECESSARY SECURITY

Companies have a legal obligation to protect any personal data collected through geolocation tools. This includes:

- *Data Security*: Companies must securely store geolocation data, like any other personal information. Companies must also protect that data from unauthorized access, alteration, or loss. Make sure to implement robust

cybersecurity measures to ensure the data's integrity. This includes proper due diligence over the security measures of vendors engaged to collect, process, or store this data.

- *Retention Period*: Define and adhere to clear data retention policies. Geolocation data should only be stored for as long as necessary to fulfill its purpose. Companies should securely delete or anonymize the data when no longer needed.

PROVIDE TRANSPARENCY AND DOCUMENTATION

Companies should make sure to maintain transparency about their geolocation monitoring practices. They should provide employees with clear documentation that explains:

- How geolocation data is collected, through which devices and applications;
- What data is being tracked and for what purposes;
- How long the data will be stored;
- How the data will be used; and
- Who will have access to the data.

Companies also should make employees aware of their rights regarding access to their data. For example, California privacy law requires that covered businesses provide employees with a privacy notice that explains, among other requirements, data collection practices and retention policies. This is a best practice even if not required by applicable laws.

PRESERVE EMPLOYEE RIGHTS AND PROTECTIONS

In addition to data protection laws, employees have specific rights when it comes to monitoring. These rights vary by jurisdiction but generally include a right to privacy, particularly during non-work hours. Companies should avoid monitoring during personal time or in areas where employees would reasonably expect privacy (e.g., restrooms).

In California, the CCPA grants employees the "right to access" and the "right to correct," allowing them to obtain copies of the data held about them and request any inaccuracies be corrected. The CCPA requires employers to provide information to employees about their rights in a privacy notice.

MONITOR STATE-SPECIFIC LAWS AND JURISDICTIONAL DIFFERENCES

It is essential to understand the laws of the jurisdictions in which employees are based. For example, several states, including California, require that employers inform

employees if they are being monitored electronically. In some cases, states allow geolocation tracking of company owned vehicles, but for personally owned vehicles written consent is required.

Companies should also be mindful of international differences. For instance, European data protection laws, such as the General Data Protection Regulation, have stringent privacy regulations that may differ from those in the United States or other parts of the world.