AN A.S. PRATT PUBLICATION
JUNE 2025
VOL. 11 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 5** **June 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 opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

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

Navigating Use of Generative AI at Work: Best Practices and Legal Considerations

By Damien DeLaney and M. Adil Yaqoob*

In this article, the authors explain how organizations that have integrated generative artificial intelligence into their daily operations can manage its use effectively.

In today's fast-evolving digital landscape, generative artificial intelligence (AI) has become a powerful tool that employees increasingly rely on for a variety of tasks. From drafting emails and producing reports to generating creative content and analyzing data, these technologies are reshaping how work gets done. As organizations integrate AI into their daily operations, employers face the challenge of managing its use effectively. Balancing innovation with accountability and legal compliance is critical to ensuring that AI enhances productivity without significant drawbacks.

DATA PRIVACY AND CONFIDENTIALITY

One of the foremost legal challenges is ensuring that the use of AI complies with data privacy requirements. As employees input sensitive or confidential information into AI systems, there is an increased risk of data exposure – especially if third-party platforms are involved. Employers must establish protocols that protect sensitive information and comply with privacy laws.

In addition to international frameworks such as the General Data Protection Regulation (GDPR) in the European Union, several U.S. states have enacted robust privacy laws that may be implicated by AI use. For example, the California Consumer Privacy Act (CCPA), along with its successor, the California Privacy Rights Act (CPRA), imposes strict requirements on how personal data is collected, processed, and shared. These laws can affect employers who use generative AI to handle employee data, as any inadvertent exposure or misuse of sensitive information could trigger compliance issues making it essential for employers to evaluate the data flows associated with AI tools and implement measures to mitigate risks.

One particular risk to employer privacy stemming from AI use in the workplace is the use of AI systems that do not strictly limit how user inputs can be used – for example, for further training or fine-tuning of the model. Examples of such systems include certain commercial versions of OpenAI's ChatGPT, Anthropic's Claude, and Google's Bard. Information that is entered into these systems might be shared with another unintended user and retained in the AI's network. For these reasons, businesses should

* The authors, attorneys with Akerman LLP, may be contacted at damien.delaney@akerman.com and adil.yaqoob@akerman.com, respectively.

exercise caution whenever inputting sensitive or confidential information into an AI tool and should understand whether such information is used to train the AI model or if it is transmitted or stored outside the business's network.

OVERSIGHT AND ACCOUNTABILITY

Integrating AI into work processes raises important questions about employee oversight and accountability. Although AI can automate and streamline tasks, employees are ultimately responsible for verifying the accuracy of its outputs. This dual responsibility can blur the lines between machine assistance and human oversight, potentially leading to errors or omissions. Employers must develop clear guidelines specifying how AI outputs should be reviewed and validated to mitigate risks that could lead to operational or legal challenges.

Moreover, as noted above, employers should implement guidelines prohibiting employees from inputting confidential information into AI systems such as certain commercial versions of ChatGPT, Claude, and Bard that do not strictly limit how user inputs can be used, in order to protect such information from potential disclosure.

OVERTIME CLASSIFICATION

Generative AI can change the nature of an employee's work by redistributing tasks and shifting job responsibilities, with direct implications under the Fair Labor Standards Act and its state equivalents. As AI tools assume repetitive functions, employees may take on managerial responsibilities such as monitoring, verifying, or supplementing AI-generated work. Employers must carefully assess whether these new responsibilities warrant adjustments in employee classifications.

Indeed, under the Fair Labor Standards Act, an employee whose primary duty is the performance of office or non-manual work directly related to the management or general business operations of the employer and who exercises discretion and independent judgment with respect to matters of significance may qualify under the administrative exemption, allowing employers to classify such employees as exempt from overtime pay.

EMPLOYEE MONITORING

The National Labor Relations Act safeguards employees' rights to engage in protected concerted activities, including discussing wages, working conditions, and unionizing efforts. As employers increasingly deploy generative AI to monitor productivity and manage workflow, it is critical to examine how such technology intersects with these NLRA protections.

When AI systems are used to analyze employee communications or monitor work patterns, there is a risk that the technology could inadvertently capture or suppress protected activities. For instance, if an AI tool scans internal emails, chat messages, or other digital communications to assess productivity, it might also detect conversations about working conditions or collective grievances. Such monitoring could be considered

to discourage employees from discussing issues that they are legally entitled to discuss. Employees may become reluctant to express concerns or engage in discussions about their rights if they believe their communications are subject to constant AI analysis – risking a violation of the NLRA.

CONCLUSION

Managing use of generative AI is not a one-time effort; it requires continuous assessment and policy refinement. Organizations must adopt a proactive, collaborative approach that involves HR, IT, legal, and – when applicable – labor representatives. Developing policies that are responsive to technological advancements and regulatory changes is essential. Regular training sessions, routine audits of AI outputs, and transparent communication with employees are all critical components of an effective management strategy. By fostering a culture of continuous improvement, employers can ensure that AI tools are used responsibly to enhance performance while safeguarding the organization against legal risks.

The integration of generative AI into the workplace presents both exciting opportunities and complex challenges. Employers who proactively manage the use of these technologies can drive innovation and boost productivity while mitigating legal risks related to data privacy, employee monitoring, and accountability. Comprehensive policies, continuous training, and a culture of transparent communication are essential to navigating this evolving landscape. As generative AI continues to reshape work processes, staying informed and adaptable remains the key to transforming potential risks into sustainable competitive advantages.