AN A.S. PRATT PUBLICATION
JULY-AUGUST 2026
VOL. 12 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 6** **July-August 2026**

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)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.
LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2026 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

(2026–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR
Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenisberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Sidley Austin LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

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. Copyright 2026 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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.

Managing the Long Tail of a Data Breach: Lessons Learned on Data Analytics and Notification

By Jacqueline F. "Lyn" Brown, Megan L. Brown, Erin M. Joe and Alissa Lynwood*

In this article, the authors delve into issues such as the importance of establishing and maintaining clear data organization and classification, the data analytics workstream, managing notification timing, government and regulatory reporting requirements, and more.

When a cyber incident occurs, the focus is often on the initial incident response with a rush to involve outside counsel, retain the right forensic consultants, and "stop the bleeding." A key but often overlooked function early in a cyber incident is the need to understand what data may have been compromised so that a legal review of impacted data can be started and the victim company can begin to assess the legal, regulatory, and business risk implications of a cyber incident. Thorough and prompt data analytics are needed to understand regulatory, contractual, or international notification obligations and determine when third-party notifications are required.

The long tail of a data breach progresses well beyond the initial detection and response, as notification obligations can give rise to future litigation, regulatory inquiries, or enforcement actions. Having a cyber incident response plan simply is not enough. Organizations need to consider and plan for in-depth data analysis to inform and comply with a variety of regulatory requirements.

1. ESTABLISH AND MAINTAIN CLEAR DATA ORGANIZATION AND CLASSIFICATION TO ENABLE FASTER INCIDENT SCOPING

In large scale incidents, post incident analytics often turns first on whether the organization can efficiently identify where relevant data resides and how it is categorized. As organizations rely on increasingly distributed environments, clarity around data structure and ownership becomes an important input into timely and accurate analytics.

Key Takeaway

Data analytic incident responders perform best when organizations have already established:

* The authors, attorneys with Wiley Rein LLP, may be contacted at lbrown@wiley.law, mbrown@wiley.law, ejoe@wiley.law and alynwood@wiley.law, respectively.

- A current data map identifying systems of record, data owners, and retention practices.
- Data classification mechanisms that identify sensitive or regulated datasets – including employee data, personally identifiable information including financial information, customer data, export-controlled information, and government contract data.
- Strict data management and retention policies and practices.
- Accessible documentation that allows forensic teams to quickly locate potentially impacted data.

Why It Matters

Clear and well-structured data organization enables incident response teams to efficiently scope and prioritize forensic analysis, minimizing unnecessary data collection and allowing resources to be directed toward systems and datasets most likely to influence legal, regulatory, and business outcomes. When data is clearly labeled, categorized, and stored in a logical manner, organizations can more quickly determine what information may be implicated, assess potential exposure, and make informed decisions early in the response process.

Conversely, inconsistently maintained data environments often require significant time and effort to reconstruct data flows, identify relevant systems, and locate affected information—driving up costs and delaying critical response milestones. In those scenarios, organizations may spend significant time understanding the scope of the dataset before substantive forensic work even begins. This uncertainty may lead to broader review of data populations and the need to run parallel workstreams, which can increase both time and cost. Thoughtful data organization in advance, therefore, not only improves response efficiency and accuracy, but also serves as a meaningful cost-containment and risk-management measure in the event of a data breach.

2. TREAT DATA ANALYTICS AS A CORE INCIDENT-RESPONSE WORKSTREAM AND RESOURCE IT EARLY

From a breach response perspective, data analytics is not a short, discrete task—it is a sustained workstream that often drives downstream legal, notification, and operational decisions. In larger incidents, analytics can extend for weeks or months as data sources are identified, scoped, validated, revalidated, and compiled into a usable report of potential notification obligations or areas of possible business risk for evaluation by key decision makers and stakeholders.

Key Takeaway

Organizations are often best positioned when they approach analytics as a planned, resourced response function, rather than an ad hoc exercise. This includes:

- Defining early how data will be collected, staged, searched, and validated across systems and third party environments.
- Establishing clear ownership and roles among IT, forensic providers, and legal teams for analytics decisions and documentation.
- Organizing and labeling data to map to reporting requirements.
- Anticipating the need for iterative analysis as scope evolves, assumptions are refined, and new data is incorporated over time.
- Maintaining clear records of methodologies, limitations, and confidence levels associated with analytical conclusions.

Why It Matters

Data analytics frequently becomes the foundation for notification populations, notice timing, regulatory engagement, and executive decision making. When analytics is structured, documented, and coordinated from the outset, organizations are better positioned to manage expectations, avoid rework as findings evolve, and support defensible decisions when conclusions are later reviewed by regulators, auditors, or other stakeholders.

When analytics is under-resourced or poorly coordinated, organizations often experience rework as conclusions change—requiring revised notifications, updated regulatory communications, or supplemental disclosures. These inefficiencies often increase costs and can draw scrutiny from regulators. A disciplined analytics strategy helps manage expectations, reduce rework, and support defensible decisions if findings are later examined.

3. ACTIVELY MANAGE INDIVIDUAL NOTIFICATION TIMING THROUGH A COORDINATED, PROJECT-DRIVEN PROCESS

Multi jurisdictional notification obligations under applicable state or international data breach notification laws may involve overlapping deadlines and sequencing challenges, particularly where analytics continue to mature close to statutory notice deadlines.

Key Takeaway

Organizations should consider managing notification timing through:

- A centralized tracker for jurisdiction specific deadlines (timing for notifications to consumers, regulators, etc.).
- Clear documentation of discovery dates.
- Early identification of dependencies among analytics completion, mailing logistics, and regulatory notifications.

Where appropriate, organizations may also consider whether phased or preliminary notification strategies may warrant evaluation as facts continue to develop.

Why It Matters

A coordinated approach to timing can support clearer internal alignment and allow organizations to manage notice obligations alongside evolving facts. These breakdowns can result in corrective notices, regulatory follow-up inquiries, or allegations that notice was delayed without justification—each of which increases cost and business disruption.

Proactive, project-driven management helps mitigate these risks by aligning legal requirements with operational realities as an incident develops. By tracking deadlines and evolving analytical conclusions in a coordinated manner, organizations can make more deliberate timing decisions, reduce rework, and maintain consistency across communications. This structured approach not only enhances defensibility but also allows response teams to remain focused on remediation and recovery rather than reacting to avoidable timing issues.

4. PROACTIVELY IDENTIFY AND COORDINATE GOVERNMENT AND REGULATORY REPORTING OBLIGATIONS

In many cyber incidents, individual notification is only one part of a broader reporting landscape. Depending on the nature of the incident, organizations may face overlapping reporting obligations to regulators, sector-specific agencies, and the government. These requirements often operate on different timelines, use different triggering standards, and evolve as facts develop.

Key Takeaway

Organizations are often best positioned when they proactively work in advance with counsel by:

- Identifying which regulatory regimes may apply (e.g., securities disclosures, critical infrastructure reporting, sector-specific rules, government contract obligations, or law-enforcement coordination), based on the company's business profile and data environment.

- Establishing clear internal owners for regulatory reporting workstreams so counsel knows who can quickly validate facts, timelines, and technical details.
- Organizing and labeling data to align with reporting regime requirements.
- Managing and deleting legacy data.
- Coordinating communications through counsel to help align disclosures, manage privilege, and avoid inconsistent or premature reporting across agencies.

Why It Matters

Regulatory reporting is increasingly scrutinized in the wake of significant cyber incidents. Early coordination and disciplined tracking allow organizations to meet mandatory obligations, make informed judgment calls where discretion exists, and work with counsel to manage regulatory risk in a way that remains consistent as the incident evolves.

For organizations handling government data, thoughtful data organization is especially critical. Entities should consider structuring government-related data by contract number and clearly identifying and marking controlled data (e.g., Covered Defense Information (CDI), defense articles and technical data under the International Traffic in Arms Regulations (ITAR), dual use technology under the Export Administration Regulations (EAR) or other access-restricted data). Under the Defense Federal Acquisition Regulations (DFARS) cyber incident reporting requirements, defense contractors are required to rapidly report a cyber incident involving a covered contractor information system or CDI. Contractors are generally expected to identify and report affected contracts and the types of controlled data implicated by an incident. Clear data segregation and labeling enables more accurate and narrowly tailored reporting, reducing uncertainty and the risk of over-or under-reporting.

Conversely, when government data is commingled with non-government or non-controlled data within the same system, and cannot be readily distinguished, organizations face a heightened risk that additional data production may be required in response to information sought by the Department of Defense as part of a cyber incident damage assessment. In practice, if an organization cannot reliably demonstrate which data sets were or were not affected, it may be required to produce information more broadly under DFARS obligations. This can expand the amount of information provided to the government, increase compliance burden, and result in an overproduction of non-contract related information to the government. Proactive data organization and labeling, therefore, plays a meaningful role not only in operational efficiency, but also in helping organizations manage government

reporting and assessment or investigative risk with greater precision and confidence during a cyber incident.

5. PLAN FOR POST-NOTIFICATION OBLIGATIONS AND PRESERVE DOCUMENTATION TO SUPPORT ONGOING ENGAGEMENT

Regulatory engagement, internal review, and follow up inquiries may continue well after notifications are issued. These longer term considerations are often easier to manage when documentation is assembled contemporaneously.

Key Takeaway

Organizations should consider preserving:

- Clear records of investigative scope, methods, and findings, including how systems were identified for review, what forensic tools or techniques were used, and the conclusions reached as the investigation progressed.
- Documentation supporting key technical judgments and response decisions, such as determinations regarding data exposure and exfiltration, scope limitations, reporting triggers, notification timing, and any assumptions or constraints that informed those decisions at the time they were made.

Why It Matters

Well maintained records can facilitate prompt response to regulatory engagement, support internal audits, and provide continuity as response teams shift focus over time. Contemporaneous documentation helps form a defensible record that response actions were proportionate and based on the reasonably available information at each stage of the incident, an important consideration in today's regulatory and litigation-oriented environment.

By contrast, when documentation is incomplete, fragmented, or recreated months later, organizations often incur additional legal and forensic costs responding to follow-up inquiries from customers, various government agencies or regulators, auditors, plaintiffs' attorneys, or possibly the media. Attempting to reconstruct previous decision-making can result in inconsistencies, create uncertainty around key judgments, and invite heightened scrutiny into whether earlier actions were justified. Contemporaneous documentation helps mitigate these risks by forming a defensible record demonstrating that response actions were proportionate, methodical, and grounded in the information reasonably available at each stage of the incident.

CONCLUSION

The most resource intensive aspects of a data breach often arise during the extended period of analytics, notification execution, and regulatory engagement. Organizations that proactively invest in data governance, analytics planning, and notification processes are typically better positioned to manage, legal, regulatory, and business exposure over the long tail of an incident.

Advanced preparation saves time, reduces business disruption, can minimize costs, and possibly help guard against potential litigation or other undesirable consequences. Organizations should consider how their data is maintained whether it is segregated or retained appropriately, and who is responsible and accountable for data management. Maintaining legacy or poorly managed data presents risk and, if compromised, potentially triggers a variety of notification obligations and brings increasing litigation or regulatory risk. As part of prudent cyber incident response planning, organizations should also carefully consider data mapping, labeling, and retention – including moving data to cold storage and enforcing data deletion policies to enhance their advance preparation and resilience to a cyber incident and data breach.