AN A.S. PRATT PUBLICATION
JULY-AUGUST 2023
VOL. 9 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: YOUR GREATEST DATA PRIVACY RISK
Victoria Prussen Spears

MITIGATING YOUR GREATEST DATA PRIVACY RISK: HOW TO ESTABLISH AN EFFECTIVE VENDOR MANAGEMENT PROCESS
Kathryn T. Allen and Kelsey L. Brandes

NAVIGATING THE HIPAA RISKS OF WEBSITE TRACKERS
Alexander Dworkowitz and Scott T. Lashway

MARITIME RANSOMWARE
Vanessa C. DiDomenico, Sharon R. Klein and Karen H. Shin

FEDERAL TRADE COMMISSION PROPOSES FURTHER RESTRICTIONS ON META'S PRIVACY PRACTICES AND A COMPLETE PROHIBITION ON META MONETIZING YOUTH DATA
Christopher N. Olsen and Nikhil Goyal

LIMIT YOUR HEALTH DATA SHARING AND CALL ME IN THE MORNING: FEDERAL TRADE COMMISSION PRESCRIBES ENFORCEMENT OF THE HEALTH BREACH NOTIFICATION RULE
Kathleen Benway, David C. Keating, Sara Pullen Guercio and Hyun Jai Oh

WASHINGTON TRANSFORMS CONSUMER HEALTH DATA LANDSCAPE WITH PASSAGE OF MY HEALTH MY DATA ACT
Meghan O'Connor and Kiana Baharloo

ILLINOIS SUPREME COURT CLARIFIES SCOPE OF STATE'S BIOMETRIC INFORMATION PRIVACY ACT CLAIMS: FIVE YEAR STATUTE OF LIMITATIONS AND CONTINUOUS ACCRUAL OF CLAIMS
Kathleen L. Carlson, Lawrence P. Fogel, Geeta Malhotra, Stephen W. McInerney, Vera M. Iwankiw, Andrew F. Rodheim and Carly R. Owens

ÖSTERREICHISCHE POST: EUROPEAN COURT OF JUSTICE SPECIFIES THE REQUIREMENTS FOR COMPENSATION FOR BREACHES OF GENERAL DATA PROTECTION REGULATION
Huw Beverley-Smith and Jeanine E. Leahy

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 6** **July - August 2023**

Editor's Note: Your Greatest Data Privacy Risk
Victoria Prussen Spears 183

Mitigating Your Greatest Data Privacy Risk: How to Establish an Effective Vendor Management Process
Kathryn T. Allen and Kelsey L. Brandes 186

Navigating the HIPAA Risks of Website Trackers
Alexander Dworkowitz and Scott T. Lashway 191

Maritime Ransomware
Vanessa C. DiDomenico, Sharon R. Klein and Karen H. Shin 194

Federal Trade Commission Proposes Further Restrictions on Meta's Privacy Practices and a Complete Prohibition on Meta Monetizing Youth Data
Christopher N. Olsen and Nikhil Goyal 198

Limit Your Health Data Sharing and Call Me in the Morning: Federal Trade Commission Prescribes Enforcement of the Health Breach Notification Rule
Kathleen Benway, David C. Keating, Sara Pullen Guercio and Hyun Jai Oh 202

Washington Transforms Consumer Health Data Landscape with Passage of My Health My Data Act
Meghan O'Connor and Kiana Baharloo 208

Illinois Supreme Court Clarifies Scope of State's Biometric Information Privacy Act Claims: Five Year Statute of Limitations and Continuous Accrual of Claims
Kathleen L. Carlson, Lawrence P. Fogel, Geeta Malhotra, Stephen W. McInerney, Vera M. Iwankiw, Andrew F. Rodheim and Carly R. Owens 213

Österreichische Post: European Court of Justice Specifies the Requirements for Compensation for Breaches of General Data Protection Regulation
Huw Beverley-Smith and Jeanine E. Leahy 218

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2023–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.

Mitigating Your Greatest Data Privacy Risk: How to Establish an Effective Vendor Management Process

By Kathryn T. Allen and Kelsey L. Brandes*

In this article, the authors explain that facing a regulatory body or your customers after you experience a data breach will be less painful when you can point to a comprehensive, all-encompassing vendor management process.

What is the greatest data privacy threat to companies now? It is commonly thought that a company's employees are the greatest data privacy threat, as they may fall prey to phishing attacks, click bait, lost devices and other situations that can compromise company data. Employees can be a threat, but in reality, this threat can be effectively mitigated within the company by implementing solutions such as tighter controls on company devices, employee trainings and internal safeguards.

The greatest data privacy threat companies actually now face is their vendors: the third-party businesses a company must do business with. Companies are increasingly engaging third-party vendors to provide a host of services. It is often cheaper to outsource key services and infrastructure to cloud services rather than develop and maintain such services and infrastructure inhouse. Yet, these vendors are a data privacy threat. Consider the numbers:

- 63% of data breaches are tied to or directly caused by third-party vendors; and
- The average cost of responding to largescale third-party breach is $10 million.

In addition to response costs, data breaches can lead to a number of other challenges for companies, such as:

- Increased operational costs associated with asset recovery and system downtime;
- Regulatory investigations or actions;
- Litigation;
- Reputation harm;

* The authors, attorneys with Polsinelli, may be contacted at kallen@polsinelli.com and kbrandes@polsinelli.com, respectively.

- Customer loss; and
- Decrease in shareholder value.

THE CONCEPT OF VENDOR MANAGEMENT

Can companies manage vendor risk in a way similar to how they have begun to manage employee risk? The answer is yes, if they follow a comprehensive third-party vendor management program. Many companies rely on their procurement department to gather information on vendors and/or to establish a risk profile through vendor assessments. But as more and more vendors have cloud-based or Internet of Things components (even for the most mundane products and services), it is time to pull vendor management away from the procurement team and implement different measures.

Vendor assessments and surveys are no longer enough to protect a company, as they may not provide a complete picture. Assessments and surveys are often based on moments in time (i.e., what the vendor is doing or not doing at that particular moment when they complete the assessment or survey). Vendors rarely go back and update customers when they make changes to their security policies. Assessments and surveys are a great way to get to know your vendors from a technical standpoint as of the date of completion of the assessment or survey, but the vendor selection process cannot stop there. Additionally, there might not be repercussions associated with assessments or surveys if the vendor experiences a data breach. This is where written agreements between your company and its vendors can protect your company in ways that an assessment or survey cannot.

THE INFORMATION SECURITY AGREEMENT

Based on the type of company and what it does, the company must be the party establishing parameters for its risk tolerance and legal and regulatory obligations. But how does a company do so while contracting with hundreds of vendors each year?

A written document is recommended, whether a stand-alone agreement or an exhibit or addendum to the underlying relationship agreement, that sets forth specific physical and technical standards as well as ongoing obligations by your vendors to keep your data safe. There should also be legal remedies in the event vendors fail to keep their obligations. This document is commonly referred to as an information security agreement (ISA).

At a minimum, an ISA should address the following:

- *Certifications.* Certain industries have required certifications (e.g., the Health Information Technology for Economic and Clinical Health Act), while others follow industry standards (e.g., SOC2). Vendors should provide copies of their certifications.
- *Data Breach Notification.* How will the vendor notify you if your data is breached? When must the vendor notify you of a breach? What does the vendor have to do for you and the data subjects post-breach?

- *Encryption of Data.* Does the vendor encrypt data only at rest or also in transmission? What level of encryption is used?

- *Audits.* Do you want to be able to audit the vendor's compliance with the ISA? What about after a data breach?

- *Employee/Subcontractor Management.* Do vendor employees need background checks? Can the vendor engage subcontractors without your approval?

- *Data Storage/Destruction.* Where can and cannot the vendor store your data? What happens to your data when your agreement with the vendor is over?

- *Malware.* What internal processes does the vendor have in place to detect malware and prevent cyberattacks? Does the vendor regularly scan its systems (and make the results of those scans available to you upon request)? What happens if the vendor passes a virus on to you?

- *Disaster Recovery/Business Continuity.* If the vendor experiences a major interruption in business, how long will it need to recover? This is particularly important to infrastructure vendors.

- *Regulations.* Examples may include the European Union's General Data Protection Regulation and the California Consumer Privacy Act.

- *Insurance.* Does the vendor have sufficient insurance in place that will make you whole in the event the vendor experiences a data breach? Is the vendor properly capitalized to stand behind its liability?

- *Liability.* What is the minimum liability your company will be comfortable with accepting in the event of a vendor's data breach or breach of the ISA? The vendor's liability for breaches must be higher or uncapped for regulated businesses.

THE VENDOR MANAGEMENT PROCESS

Prework

Draft a template ISA that reflects your company's actual needs, considering various factors such as the company's industry, data collected, regulatory environment, and products or services. With the onslaught of new data privacy legislation both domestically and abroad, it is recommended that you consult with your privacy counsel on any data privacy provisions.

Prework action steps:

- Establish written criteria that define when vendors will be required to sign an ISA (i.e., when the vendor will have access to your data, infrastructure or network);
- Work with the legal and information security teams to draft a form ISA;
- Establish written parameters for tolerance on vendor-requested changes to the ISA; and
- You should work with attorneys who can assist with ISA prework, including drafting an ISA that includes requirements and risks your company is comfortable with.

Internal Rollout

When rolling out the ISA to your company, you must educate those who are part of the vendor selection process and work with vendor management and legal and compliance to ensure all individuals understand what the ISA is, what it does and the importance of it. Consider hiring an external party to present required trainings for all relevant internal stakeholders for maximum impact and adoption.

Internal rollout action steps:

- Educate internal stakeholders about the ISA, its purpose and its effectiveness;
- Modify the company's internal process so that an ISA is now provided to any new vendor that meets the established criteria; and
- Establish who has authority within the organization to approve vendor-requested deviations to the ISA.

External Rollout

Sending the ISA to prospective vendors is easy. But what will you do when vendors request to negotiate certain provisions, or decline to review your ISA altogether and instead provide their own set of information security terms (which may not be in the form of a legally binding agreement)? Consider establishing a relationship with outside counsel that has expertise in data privacy and information security and who can assist in identifying and quantifying the risk associated with a vendor's changes or terms.

External rollout action steps:

- Send the ISA to vendors with clear messaging that explains the ISA's purpose and relationship to other legal documents;

- Create a process for the receipt of vendor changes and establish who will negotiate with the vendor; and
- Establish a repository of ISAs that can be called on easily when there is an issue with the vendor.

Your attorneys should be able to assist with responding to any proposed changes by vendors and determining the risk associated with such changes.

CONCLUSION

Facing a regulatory body or your customers after you experience a data breach will be less painful when you can point to a comprehensive, all-encompassing vendor management process. And the process will be even less painful when you can get relief from the vendor that is responsible for the breach instead of paying out of your own pocket.