AN A.S. PRATT PUBLICATION
JANUARY 2019
VOL. 5 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 1 JANUARY 2019

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
Customer Service Web site .... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or .... (800) 223-1940
Outside the United States and Canada, please call .... (937) 247-0293

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*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [1] (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.

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

(2019–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. Copyright 2019 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, 646.539.8300. 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.

Preparing for Ohio's Cybersecurity Safe Harbor Law

Steven G. Stransky and Thomas F. Zych[*]

Corporate victims of data breaches often become the targets of litigation and governmental enforcement actions, adding costly insult to serious injury. The authors of this article discuss a new Ohio law addressing this inequity by providing (limited) protection from private litigation to businesses that suffer a data breach despite their cybersecurity planning and execution.

Cyberattacks are a reality that can impact even the best-prepared business. Unfortunately, corporate victims of data breaches often become the targets of litigation and governmental enforcement actions, adding costly insult to serious injury. The Ohio legislature has addressed this inequity by providing (limited) protection from private litigation to businesses that suffer a data breach despite their cybersecurity planning and execution.

Beginning November 2, 2018, businesses will have the ability to invoke a cybersecurity safe harbor provision pursuant to Ohio law (SB 220) to obtain tort-related liability protection if they suffer a data breach. Businesses can undertake simple measures to efficiently and effectively avail themselves of Ohio's cybersecurity safe harbor.

BACKGROUND ON SB 220

What Does the Cybersecurity Safe Harbor Protect Against?

Pursuant to SB 220, a "covered entity" that has adopted a written cybersecurity program may raise an affirmative defense to any tort action alleging that its "failure to implement reasonable information security controls resulted in a data breach" involving either personal information or restricted information. In other words, this safe harbor will enable businesses that have implemented appropriate cybersecurity programs to counter allegations of tort liability due to a data breach. This often occurs when plaintiffs initiate negligence or privacy-related claims after their personal information is compromised in a data breach. However, the safe harbor does not protect against liability for violating contractual obligations (e.g., contractual provisions governing data protection) or alter any other obligation that a business may have to

[*] Steven G. Stransky is senior counsel in Thompson Hine's Business Litigation, Privacy & Cybersecurity, and Government Contracts groups, advising clients on national and international privacy and information security issues. Thomas F. Zych is a partner at the firm, chair of the Emerging Technologies Practice, and head of the Privacy & Cybersecurity team, focusing on a range of data protection, intellectual property, consumer protection, social media, competition, and antitrust matters. Mr. Zych is also a member of the Board of Editors of *Pratt's Privacy & Cybersecurity Law Report*. The authors may be reached at steve.stransky@thompsonhine.com and tom.zych@thompsonhine.com, respectively.

report the data breach to affected individuals, government or regulatory agencies, or any other entity.

Who Can Invoke the Safe Harbor?

SB 220 applies to a "covered entity," which is defined as any type of business, including a nonprofit organization that "accesses, maintains, communicates, or processes" personal or restricted information "in or through one or more systems, networks, or services." SB 220 incorporates the definition of "personal information" from Ohio's data breach notification law, which defines it as an individual's name (i.e., first name or first initial and last name) linked to a Social Security number, driver's license or state identification number, or financial account or credit card data. In contrast, the term "restricted information" means "any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual."

Generally, the definitions of personal and restricted information exclude data that is unreadable (e.g., encrypted or redacted) and would not cause any harm or risk to individuals in the event that either is compromised in a data incident. SB 220 provides safe harbor only to data breaches involving electronic documents and does not provide any liability protection in the event that physical (i.e., hard-copy) documents or records are lost, stolen, or otherwise compromised.

How to Qualify for the Safe Harbor?

In order to invoke the Ohio cybersecurity safe harbor provision, a business must "create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards" to protect personal information (or personal and restricted information) and that "reasonably conforms to an industry recognized cybersecurity framework." The law identifies, among others, the following as acceptable industry recognized cybersecurity frameworks:

- The Framework for Improving Critical Infrastructure Cybersecurity – developed by the National Institute of Standards and Technology ("NIST");
- NIST Special Publication 800-171;
- The Federal Risk and Authorization Management Program Security Assessment Framework;
- ISO/IEC 27000, Information Security Management Systems;
- The Health Insurance Portability and Accountability Act's security rule; and
- The Payment Card Industry Data Security Standard.

The law provides some context to the "reasonably conforms" criterion by stating that the "scale and scope" of a covered entity's cybersecurity program "is appropriate" if it is based on the following: the size and complexity of the covered entity; the nature and scope of the covered entity's activities; the sensitivity of the information; the cost and availability of tools to improve information security and reduce vulnerabilities; and the resources available to the covered entity.

STRATEGIZE AND LEVERAGE YOUR EXISTING CYBERSECURITY EFFORTS

To effectively and efficiently avail themselves of Ohio's cybersecurity safe harbor, businesses should (1) consolidate their existing cybersecurity measures, (2) identify which of the above-mentioned cyber standards set forth in SB 220 most closely aligns with their current cybersecurity program, and (3) update their cybersecurity practices to satisfy any outstanding requirements.

Consolidate Existing Cybersecurity Measures

SB 220 does not require businesses to establish any particular cybersecurity program, nor does it create new liability for failing to do so. Rather, the purpose of the law is to incentivize businesses to proactively implement cybersecurity measures to protect personal data under their control. Many businesses have already implemented some technical, physical, and administrative data security measures to protect corporate data (e.g., trade secrets, protected health information, intellectual property). For example, businesses routinely use encryption protocols, firewalls and other technical programs to safeguard corporate data, as well as incident response procedures, confidentiality requirements and other administrative security measures. However, these safeguards, plans and policies may have been generated and implemented in a disparate and inconsistent manner. The safe harbor provision requires these policies be reviewed and consolidated under a unified – and written – cybersecurity program.

Identify Where Your Program Aligns

Once a business determines the scope of its existing cybersecurity program, it should compare and contrast it to the acceptable cybersecurity frameworks set forth in SB 220 to identify the framework with which it most closely aligns. Thereafter, it will be better positioned to more narrowly create and implement the remaining elements of the cybersecurity framework needed to satisfy the safe harbor provision. Separately, for businesses that are already subject to an acceptable cybersecurity framework set forth in SB 220, they may simply need to expand their existing cyber program to cover personal information in their possession. For example, businesses that have a medical benefits plan that is subject to HIPAA will have likely implemented several of the cybersecurity measures required by the HIPAA security rule. Similarly, government contractors processing defense-related information will have likely already satisfied NIST 800-171 requirements pursuant to federal acquisition regulations. If these businesses simply expand their security controls from their existing scope (e.g., protected health information, covered defense information) to address all personal information, then they would be able to rely upon Ohio's safe harbor law.

Satisfy Outstanding Requirements

Once a business determines the acceptable cybersecurity framework with which it most closely aligns, it should implement any outstanding physical, technical, and administrative measures needed in order to satisfy the framework's remaining requirements. In addition, to ensure that a business can rely upon the safe harbor provision, it will need to establish an internal or external process to continuously monitor its cybersecurity program for compliance purposes.

CONCLUSION

Cyberattacks against the private sector continue to increase in scope and sophistication, and the Ohio law provides a valuable safe harbor to businesses that proactively build a cybersecurity program.