AN A.S. PRATT PUBLICATION
SEPTEMBER 2021
VOL. 7 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 7** **September 2021**

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [217] (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

(2021–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.

How to Comply with BIPA's Security Requirement to Mitigate Class Action Liability Exposure

By David J. Oberly*

One of the aspects of the Illinois Biometric Information Privacy Act that creates the greatest liability exposure for covered businesses also remains one of the least discussed: data security. The author of this article discusses data security under the biometric law and cautions that companies that operate with biometric data security as an afterthought do so at their peril.

To date, much of the focus on the Illinois Biometric Information Privacy Act ("BIPA") has been on the law's privacy policy, notice, and consent requirements. And for good reason—the vast majority of BIPA class action suits have centered on these particular elements of Illinois' biometric privacy statute.

Significantly, however, one of the aspects of BIPA that creates the greatest liability exposure for covered businesses also remains one of the least discussed: data security. Those companies that operate with biometric data security as an afterthought do so at their peril, as it is only a matter of time before malicious actors begin to succeed in their cyber-attacks targeting biometric data with relative consistency. When that time inevitably comes, the data security facet of Illinois' biometrics law will become a central component of BIPA class lawsuits.

As such, companies and their in-house legal teams must ensure they have in place defensible biometric security programs to satisfy this critical aspect of BIPA and put themselves in the best position to defeat any claims of purported violations of BIPA's security mandate in the event of a security incident that brings class litigation with it in its wake.

THE DATA SECURITY COMPONENT OF ILLINOIS' BIOMETRIC PRIVACY STATUTE

As is the case with the majority of other privacy laws, the statutory language of BIPA offers no substantive guidance of any kind for implementing security measures in a fashion that satisfies this core component of Illinois' biometric privacy statute. Rather, BIPA's text merely provides that companies must maintain security measures that:

* David J. Oberly is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Biometric Privacy, Privacy Class Action Defense, and Cybersecurity & Data Privacy groups. His practice encompasses both defending clients in biometric privacy, privacy, and data breach class action litigation, as well as counseling and advising clients on a wide range of biometric privacy, privacy, and data protection/cybersecurity matters. He can be reached at doberly@blankrome.com.

(1) utilize the "reasonable standard of care" within the private entity's industry; and (2) protect biometric data in the same or a more protective manner than which the company safeguards other types of sensitive personal information. As a result, significant uncertainty exists as to what businesses can do to ensure compliance with the security component of BIPA.

PRACTICAL GUIDANCE AND BEST PRACTICES FOR COMPLYING WITH BIPA'S SECURITY REQUIREMENT

Despite a lack of clear direction from the law, there are several practical, concrete steps that companies can implement to build defensible biometric data security programs that should be able to satisfy BIPA's data security requirement in the event their biometric data security practices are challenged in court.

BIPA's "Reasonableness" Standard

As a starting point, companies should remain cognizant of the fact that BIPA's security requirement does not impose a strict liability standard. Rather, plaintiffs are required to establish that a security incident resulted from a failure to maintain "*reasonable*" security practices. As such, by incorporating the following protocols as part of a comprehensive data security program, businesses can arm themselves with the ability to establish that affirmative actions were taken to safeguard sensitive biometric data which, in turn, will put them in the best position possible to successfully defeat any claims of inadequate security in violation of Illinois' biometric privacy statute in the aftermath of a breach event.

Defensive Biometric Data Security Measures and Protocols

As data breaches will almost always trigger class action litigation under BIPA, companies should place a major emphasis on implementing defensive strategies to minimize the risk of a security incident taking place in the first instance. Further, as noted above implementing stringent defensive security measures will allow businesses to demonstrate that active measures were implemented, and robust security protocols put in place, that satisfy the "reasonableness" standard of BIPA if the entity were to fall victim to a biometric data compromise incident.

In particular, companies should consider implementing the following practices where feasible:

- Delineate a specified retention period and permanently dispose of stored biometric data as soon as practicable after it is no longer necessary for the purpose for which it was collected.
- Ensure that all biometric data is encrypted, both while at rest and in transit.

- Store all biometric data separately from all other types of personal information—such as names, birthdates, and account numbers.
- Designate one or more employees to manage and oversee the company's biometric data security program.
- Maintain stringent password protection policies for gaining internal access to systems that collect and use biometric data or locations where such data is stored, which should encompass elements such as password expiration, complexity, and length.
- Provide mandatory biometrics-focused security awareness training for all employees on the company's security program and policies, as well as best practices for safely handling, transmitting, and storing biometric data.
- Perform periodic risk assessments to identify the primary risks to the biometric data possessed by the company and implement any necessary modifications to the entity's security program to minimize these risks.
- Complete penetration testing on the company's networks and systems to identify any security vulnerabilities that could be exploited by malicious hackers and implement any necessary modifications to minimize the risk of these vulnerabilities being exploited.

Importantly, as the foregoing security protocols are commonplace and widely utilized across a wide variety of sectors, implementation of these security measures will also aid most companies in satisfying BIPA's requirement that its security measures comport with those commonly used "within the private entity's industry."

Vendor Management

In addition to ensuring the security of their own networks, systems, and devices, companies must also ensure that their vendors and service providers also maintain the necessary security measures and protocols to effectively safeguard the company's biometric data while in the hands of those vendors or service providers.

There are several practical steps companies can take to ensure their third-party vendors and service providers maintain the requisite level of security to avoid falling victim to a biometric data compromise event while in the possession or control of the company's sensitive data.

First, before entering into a relationship with any vendor or service provider that will have access to biometric data, necessary due diligence and vetting must be completed by the company's in-house lawyers—or, ideally, experienced outside biometric privacy counsel—to ensure the vendor's security measures are sufficiently robust.

Second, companies should also review and update their contracts with current vendors and service providers to take into consideration the key issues raised by BIPA, including

indemnification in the event of a security incident involving the vendor/service provider and the company's biometric data. In most instances, this task should also be carried out by experienced biometric privacy counsel.

Lastly, companies must also ensure that their vendors and service providers continue to maintain sufficient security measures over time through ongoing monitoring.

CONCLUSION

At the same time that organizations across all sectors are experiencing more and more attempted—and many times successful—data breach attacks, BIPA's vague security mandate, coupled with its expansive private right of action provision, greatly increases the potential scope of liability exposure faced by companies that handle biometric data. As such, now more than ever companies and their in-house counsel must take proactive measures and implement effective defensive mechanisms to shield their networks, systems, and devices from cyber-attacks targeting sensitive fingerprints, scans of facial geometry, and other types of biometric data.

By implementing the best practices described above, companies can put themselves in the best position to minimize the risk of experiencing a catastrophic security incident involving biometrics, while at the same time putting in place robust security measures that satisfy BIPA's "reasonable" security mandate.