AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2020
VOL. 6 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 9** **NOVEMBER - DECEMBER 2020**

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 [245] (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

(2020–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, 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.

U.S. Senators Introduce Bill Imposing Stringent, National Biometric Privacy Regulation

By Jeffrey N. Rosenthal and David J. Oberly *

Biometric data generally encompasses unique, measurable human biological or behavioral characteristics – including fingerprints, voiceprints, and scans of hand or face geometry – for identification and authentication purposes. To protect this data, the National Biometric Information Privacy Act of 2020 was introduced in the U.S. Senate. The authors of this article discuss the Act, which would impose requirements closely mirroring the Illinois Biometric Information Privacy Act.

Biometric data – like fingerprints and facial geometry scans – allows companies across all industries to significantly enhance their operations in a myriad of ways. At the same time, the call for regulation over this especially sensitive type of personal data continues to grow. U.S. Senators Jeff Merkley and Bernie Sanders introduced the National Biometric Information Privacy Act of 2020 (the "Act"). If enacted, the Act would impose uniform, draconian requirements closely mirroring the Illinois Biometric Information Privacy Act ("BIPA") – which has led to massive, plaintiff-driven litigation – across all 50 states.

While it is unknown whether this bill will ultimately become law, the Act highlights the need for all companies using biometric data – regardless of where they are located – to take proactive measures to implement flexible, adaptable biometric privacy compliance programs.

OVERVIEW OF BIOMETRIC DATA

Biometric data generally encompasses unique, measurable human biological or behavioral characteristics – including fingerprints, voiceprints, and scans of hand or face geometry – for identification and authentication purposes. Importantly, biometric data is different from Social Security numbers and other forms of personally identifiable information ("PII") that are unique to specific individuals. Once compromised, biometric data has forever lost its ability to be used as a secure identifying mechanism.

Applicability

One of the more significant aspects of the Act pertains to its essentially unlimited scope. The Act would apply to "private entities" – which is defined as "any individual, partnership, corporation, limited liability company, association, or other group,

* Jeffrey N. Rosenthal is a partner at Blank Rome LLP and leads the firm's Biometric Privacy Team. He concentrates his complex corporate litigation practice on consumer and privacy class action defense. David J. Oberly is an attorney at the firm advising sophisticated clients on a wide range of cybersecurity, data privacy, and biometric privacy matters. The authors may be reached at rosenthal-j@blankrome.com and doberly@blankrome.com, respectively.

however organized." Thus, unlike some other recently-enacted privacy laws – like the California Consumer Privacy Act of 2018 ("CCPA") – the Act would not be limited by any preliminary thresholds for entities to fall under the scope of the law, such as total gross revenue.

Core Requirements Similar to Illinois Biometric Privacy Act

Under the Act, covered entities would be subject to many of the same requirements and restrictions mandated by Illinois' biometric privacy law:

- *Public Policy*: Covered entities must maintain a publicly available biometrics privacy policy that includes, at a minimum, a retention schedule, and guidelines for permanently destroying biometric data within mandated timeframes.
- *Written Notice*: Before collecting or using an individual's biometric data, covered entities must provide the individual with written notice detailing the entity's biometric practices and its use of the individual's biometric identifiers.
- *Written Release for Initial Collection/Use*: Before collecting or using an individual's biometric data, covered entities must obtain a written release from the individual authorizing such collection or use.
- *Written Release for Disclosures*: Similarly, a written release must be obtained from an individual before disclosing that individual's biometric data to any third party.
- *Prohibition on Selling, Leasing, or Otherwise Profiting from Biometric Data*: The Act bars covered entities from selling, leasing, trading, or otherwise profiting from the use of biometric data.
- *Reasonable Security Measures*: Covered entities must safeguard biometric data from unauthorized access, disclosure, or acquisition: (1) using the reasonable standard of care applicable to the entity's given industry, and (2) in a manner that is the same or more protective than the manner used by the entity to safeguard other types of sensitive personal data.

Additional Requirements Beyond BIPA

In addition, the Act also contains several additional requirements not found in BIPA:

- *Purpose Requirement*: Covered entities are prohibited from collecting or otherwise obtaining individuals' biometric data unless the entity requires such data to provide a service, or for some other valid "business purpose" (which is not defined in the Act).

- *Right to Know*: The Act also contains a "right to know" similar to that contained in the CCPA, which requires covered entities – upon request – to disclose information regarding the biometric data the entity has collected, where the data originated, the use(s) of the data, and whether and to whom the data is being disclosed or sold.

- *Prohibition on Use of Biometric Data for Advertising Purposes*: In addition to prohibiting the sale of, or otherwise profiting from, the use of biometric data, the Act also bars the use of biometric data for advertising purposes as well.

Penalties and Enforcement

Also similar to BIPA is the Act's primary enforcement mechanism, which entails a private right of action permitting any "aggrieved individual" to pursue litigation against an entity that fails to comply with the Act. Consumers can pursue individual or class lawsuits and can recover up to $1,000 in liquidated damages for each negligent violation, and actual damages and any punitive damages awarded up to $5,000 for each intentional or reckless violation.

Critically, the Act also features a unique provision that "[a]ny such violation constitutes an injury-in-fact and a harm to any affected individual" – which would allow plaintiffs to completely avoid any potential statutory standing hurdles that often serve as roadblocks in similar litigation, as the law explicitly specifies that individuals possess standing to sue for any violations of the law.

In addition, the Act also enables state attorneys general to bring suit on behalf of their residents as well.

KEY TAKEAWAYS

The Act in the very early stages of the legislative process and will likely face fairly stringent opposition from both the tech industry and a number of senators, especially as it relates to how the law should be enforced and, more specifically, whether a federal law of this nature should provide a private right of action for individuals to pursue litigation directly against covered entities.

Ultimately, however, even if the Act fails to make its way into law, it is clear the scope of potential liability exposure in connection with the use of biometric data will continue to increase rapidly in the immediate future. Companies should not wait for new regulation to be passed, but instead, should take preemptive action by enhancing their compliance programs to directly address biometric privacy This can be achieved by implementing the overarching privacy principles that are found in today's most stringent biometric privacy statutes and bills, including notice, consent, written releases, and biometric data security measures.

WHAT TO DO NOW

If your organization currently utilizes any type of biometric data – or if it is considering doing so in the future – the best course of action is to speak with experienced counsel to ensure your organization has the necessary policies, procedures, and practices to satisfy the full range of current and anticipated biometric regulatory compliance obligations, and to properly manage potential risk.