AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2019
VOL. 5 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 9 NOVEMBER-DECEMBER 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 [275] (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

(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. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries 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.

Biometrics Developments: BIPA & Beyond

By Mary Buckley Tobin*

Using biometrics can be an easy solution for companies to employ and solve a variety of everyday tasks: clocking in and out of work; unlocking a phone; or authenticating identities. The ease associated with swiping a fingerprint or using facial recognition is not without risk, however. This article discusses recent developments in biometric information privacy.

As companies across all industries continue to collect and utilize a wide range of personal information, biometric data has become an increasingly popular identifier to utilize in the workplace, especially for health care providers. For example, long term care facilities are implementing biometric timekeeping systems for their employees, and hospitals are using biometrics to identify their patients.

BIOMETRIC INFORMATION PRIVACY

Three states in the United States currently have statutes entirely dedicated entirely to biometrics – Illinois, Washington, and Texas. The most stringent of the three is Illinois' Biometric Information Privacy Act ("BIPA"), which was recently interpreted by the Illinois Supreme Court found that the plaintiff did *not* need to allege actual harm in order to be considered an aggrieved party under the BIPA. Federal lawmakers also have taken a recent interest in biometric privacy, a bill introduced in March would require companies to obtain consent prior to sharing facial recognition data, and impose a variety of other limitations on the use of facial recognition technology. Any company collecting or using biometrics should be aware and monitoring legal developments to understand the necessary compliance measures which may be required.

ILLINOIS' BIOMETRIC INFORMATION PRIVACY ACT

BIPA is currently the most stringent statute in the nation regulating biometric identifiers and information. It was enacted in response to the growing use and recognition that biometrics are unlike other unique identifiers, especially when used to access finances or other sensitive information. BIPA does the following:

- BIPA applies to any "Private entity," which means any individual, partnership, corporation, limited liability company, association, or other group, however organized (excludes government agencies);

* Mary Buckley Tobin is an associate in the Health Care Operations practice group at Polsinelli PC, focusing her practice on regulatory issues affecting health care providers, including reimbursement, fraud and abuse, and clinical research. She may be contacted at mtobin@polsinelli.com.

- Creates a private right of action for aggrieved persons, with damages ranging from liquidated damages of $1,000 or actual damages for a negligent violation (whichever is greater), to liquidated damages of $5,000 or actual damages for an intentional or reckless violation (whichever is greater); and
- Allows for attorney's fees and litigation costs or other relief, including an injunctive relief.

RECENT DEVELOPMENTS

In *Rosenbach v. Six Flags*, a plaintiff alleged that Six Flags improperly collected the thumbprints of their son when he purchased a season pass for the theme park on a school field trip. There were no allegations that the thumbprints were stolen or misused, rather the complaint alleged Six Flags violated BIPA due to:

1. Not obtaining a written release before collecting biometric data;
2. Not informing that biometric data would be collected and stored, or for what purpose; and
3. Not stating the length of time the biometric data would be kept or used.

Six Flags argued the plaintiff did not have a claim under BIPA because there were no allegations of harm resulting from the collected thumbprints and, therefore, the plaintiff did not have standing as an "aggrieved person" under BIPA. Six Flags relied on an Illinois appellate court decision that indicated a mere technical violation of BIPA alone was not sufficient to pursue damages, but rather an injury or adverse effect must actually be alleged.

However the Illinois Supreme Court rejected this argument, finding that an "aggrieved person" under BIPA does not need to have "sustained actual damage beyond violation of his or her rights under the Act in order to bring an action under it," reasoning that the Illinois legislature enacted BIPA to safeguard biometric privacy rights before they can be compromised.

This decision is important for companies collecting biometric data, as an increasing number of companies elect to utilize biometric data to create efficiencies and improve their services. An increasingly popular example is companies using biometrics for timekeeping purposes so employees can clock in and out more accurately. Several class action suits have been filed challenging this practice, including one currently pending in federal court against Southwest Airlines. To that care, where employees are challenging the airline's requirement that employees clock in and out using their fingerprints.

PROPOSED FEDERAL LAW

Companies collecting biometric data should track federal legislation that may impact their use of biometric information. The Commercial Facial Recognition Privacy Act, introduced in March 2019, requires companies to first obtain consent prior to using facial recognition technology, in addition to a variety of other measures to help consumers maintain autonomy over their biometric data, specifically images of their faces. Companies would also be required to:

- Notify individuals when their facial recognition data is used or collected;
- Provide, if contextually appropriate, where the individual can find more information about the use of facial recognition technology; and
- Provide documentation and general information that explains the capabilities and limitations of facial recognition technology in terms that individuals can understand.

The legislation would also provide additional protection to individuals whose biometric information is collected by prohibiting the use of facial recognition technology to discriminate against an end user in violation of applicable federal or state law. Users of facial recognition technology would be prohibited from repurposing facial recognition data for a purpose that is different from that initially presented to individuals, and also from sharing the data with unaffiliated third parties without consent.

KEY TAKEAWAYS

Using biometrics can be an easy solution for companies to employ and solve a variety of everyday tasks: clocking in and out of work; unlocking a phone; or authenticating identities. The ease associated with swiping a fingerprint or using facial recognition is not without risk, however. Companies utilizing biometric technologies should balance the benefits of utilizing this of technology against the burdens associated with legal compliance in certain jurisdictions. In Illinois, this means:

- Obtaining consent from individuals;
- Developing a written policy establishing guidelines for the collection and destruction of biometric data;
- Establishing a retention schedule and guidelines for destroying biometric identifiers; and
- Informing individuals not only of the collection, but also what collection is being used for and how it is being retained (including the length of time that biometric data is being stored).