AN A.S. PRATT PUBLICATION
JANUARY 2018
VOL. 4 • NO. 1

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

# Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 1 | JANUARY 2018



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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [4] (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

(2018–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, 718.224.2258. 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.

# A New Threat From an Old Source: Class Action Liability Under Illinois Biometric Information Privacy Act

***By William Dugan and Douglas Darch****

*The Illinois Biometric Information Privacy Act was signed into law in 2008. In the last two years, the plaintiff's class action bar has discovered the statute and its statutory penalties. As a result, employers and other private entities have increasingly been subject to lawsuits alleging violations of the Act. The authors of this article discuss the Act, recent cases, and what it means for employers.*

In 2008, the Illinois Biometric Information Privacy Act ("BIPA") was signed into law. It was designed to address the growing use of biometric identification technology, such as retina scans, fingerprint identification and facial recognition technology.

Notably, the BIPA does not prohibit the collection or use of biometric data but it does govern the collection and storage of biometric identifiers and information. In the last two years, the plaintiff's class action bar has discovered the statute and its statutory penalties. As a result employers and other private entities have increasingly been subject to lawsuits alleging BIPA violations. The threat of a lawsuit can be avoided by implementing and adhering to a compliant Biometric Information Policy.

## BACKGROUND

BIPA defines "biometric identifiers," as a retina/iris scan; fingerprints; voiceprints; and the scan of hand or face geometry. Biometric information relates to any information based on an individual's biometric identifier, regardless of how that information is captured, stored, or shared. Recent advances in fraud detection and prevention technology such as fingerprint timeclocks and secure building access necessitated by federal regulations adopted to combat terrorism threats have placed employers with operations in Illinois at risk. This risk can be avoided by adopting a Biometric Identification Policy that meets the requirements of the Illinois statute.

The cost of non compliance is substantial. BIPA creates a private right of action for statutory violations related to the collection, retention, storage, and use of biometric identifiers and information. In the case of negligent violations, private entities are liable for $1,000 per violation in liquidated damages or the amount of actual damages,

* William (Bill) Dugan is a partner at Baker McKenzie representing management in complex litigation in federal and state courts and other tribunals throughout the United States. Douglas Darch is a partner at the firm representing and counseling management in the areas of labor and employment. Resident in the firm's Chicago office, the authors may be contacted at william.dugan@bakermckenzie.com and douglas.darch@bakermckenzie.com.

whichever is greater. For intentional or reckless violations, liquidated damages are increased to $5,000 per violation or actual damages. Private entities are also liable for reasonable attorneys' fees, costs, experts' fee, and injunctive relief in addition to liquidated damages.

## RECENT CASES

A number of corporations, including internet and video game companies, food product manufacturers, gas stations, and restaurant chains, have been sued in the past few months. Since July 2017, there have been more than 25 cases filed in the state and federal courts in Illinois. In addition to the growing popularity of BIPA lawsuits with the plaintiffs' class action bar, the scope of liability is expanding. In some cases, BIPA liability has moved beyond the employer-employee relationship. For example, restaurant chain Wow Bao faces liability for using facial scans to verify customer orders at self-service kiosks. Furthermore, courts have interpreted BIPA broadly, finding defendants must face trial even when the biometric identifiers at issue are not listed in the statute. Recently, Shutterfly's motion to dismiss a lawsuit was denied on this very issue. The plaintiff alleged BIPA violations based on the use of facial-recognition software on photographs, even the photographs were not listed in BIPA's definition of biometric identifiers.

As of now, it is not clear if private entities will face liability for mere statutory violation or if plaintiffs will need to show actual injury. A district court judge in the Northern District of Illinois ruled that a showing of actual injury was not necessary for a corporate defendant to be held liable. On the other hand, the U.S. Court of Appeals for the Second Circuit oddly enough heard the same issue regarding damages under Illinois law. In that case, a New York federal judge dismissed a lawsuit concluding that BIPA statutory violations alone were an insufficient injury to have standing.

As BIPA cases are become more numerous and broad—and are being brought outside Illinois—it is important that all private entities follow the steps outlined in the BIPA to protect themselves from litigation.

## WHAT DOES THIS MEAN FOR EMPLOYERS?

Many employers have begun using timekeeping systems that use biometric identifiers, especially fingerprints, in lieu of timecards or ID badges. Corporations in the service industry are also increasingly using customer's biometric identifiers, such as face scans, to conduct transactions. As such, employers and other private entities must be vigilant in ensuring full compliance with BIPA's requirements to minimize legal liability.

## COMPLIANCE STEPS

Under Illinois law, private entities may collect, store, or use biometric identifiers and information from individuals but they must first do the following:

- Develop a written policy that is made available to the employees or the public. This policy must include a retention guideline and guidelines for permanently destroying unneeded BIPA protected data. Under BIPA, a private entity must destroy biometric identifiers and information once the purpose for which they were collected has been fulfilled or within three years of the individual's "last interaction" with the employer or entity;
- Provide written notice to all affected individuals that biometric identifiers or information is being collected and stored as well as the specific purpose and time period during which the identifiers or information will be collected, stored and used;
- Obtain written consent or a release, including a signature from all employees or customers whose biometric identifiers or information will be collected, stored, and used.

After collecting this biometric information, employers or other collectors must also:

- Adopt procedural safeguards to prevent the disclosure, sale, lease, trade of or profit from biometric identifiers and information;
- Use the industry's reasonable standard of care when storing or transmitting this information;
- Protect the biometric identifier or information in at least the same manner as other confidential and sensitive information, including genetic testing information, driver's license numbers, or social security numbers; and
- Ensure biometric identifiers and information are indeed destroyed per the written policy.

Finally, it is important that employers and other private entities take note of potential liability in other jurisdictions. A few states already have similar provisions on the books. For example, Texas passed the Capture or Use Biometric Identifier Act in 2009, Washington recently passed a law in 2017 that governs the enrollment, disclosure, and retention of biometric identifiers, and Colorado regulates the disposal of this information by including biometric data in the definition of personal information. The state legislatures in Alaska, Connecticut, Montana, and New Hampshire are considering enacting laws similar to BIPA. As the regulation of biometric becomes widespread, private entities should adopt a compliant policy now to avoid or minimize liability.