AN A.S. PRATT PUBLICATION
SEPTEMBER 2020
VOL. 6 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 7** **SEPTEMBER 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.

Beyond Borders: COVID-19 Highlights the Potential Widespread Impact of the Illinois Biometric Information Privacy Act

By P. Russell Perdew, Taylor Levesque, and Brandan Montminy*

Because of the unprecedented increase in the use of technology due to the pandemic and the large penalties that can accumulate under the Illinois Biometric Information Privacy Act, businesses and insurers need to understand the risks associated with recording or collecting biometric information. The authors explain.

The COVID-19 pandemic created a new normal for Americans – one where family members of all ages work and go to school from home. Businesses and schools have turned to technology to facilitate remote work and e-learning. Companies in the education space have rapidly adapted to offer expanded online educational experiences. Although distance learning tools have allowed schools to continue teaching despite the pandemic, the new online platforms and software offerings raise concerns about student data privacy.[1]

Similarly, employers rushing to facilitate work from home may not have considered the legal risks associated with data collection and analytics as thoroughly as they would have under normal circumstances. Unfortunately, the desire to quickly roll out technology for videoconferencing, identity verification, and timekeeping may expose businesses to liability under the Illinois Biometric Information Privacy Act ("BIPA" or the "Act").[2] Companies that capture or collect biometric information such as fingerprints or voiceprints[3] run the risk of violating BIPA if proper disclosures and procedures are not in place. Because of the unprecedented increase in the use of technology and the large

* P. Russell Perdew (rperdew@lockelord.com) is a partner at Locke Lord LLP litigating complex commercial, class action, and tort cases and providing compliance and regulatory advice to clients in heavily regulated industries. Taylor Levesque (taylor.levesque@lockelord.com) is an associate at the firm handling cases in the construction, energy, finance, housing, insurance, intellectual property, and technology industries. Brandan Montminy (brandan.montminy@lockelord.com) is an associate at the firm counseling clients in a wide array of litigation matters, as well as in privacy, data protection, cybersecurity compliance, and incident preparedness and response.

[1] Valerie Strauss, "As schooling rapidly moves online across the country, concerns rise about student data privacy," *Washington Post* (March 20, 2020).

[2] Biometric Information Privacy Act (eff. 10-03-08), *available at* https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57%E2%80%8E.

[3] Although a "voiceprint" is not defined by the statute, voiceprints are referenced as one of the many "biometric identifiers" protected by BIPA. "'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color." *See* 740 ILCS 14/10 (2016).

penalties that can accumulate under BIPA,[4] businesses and insurers need to understand the risks associated with recording or collecting biometric information.

COVID-19 WILL RESULT IN INCREASED BIPA CLAIMS AGAINST BUSINESSES SERVICING THE "RUSH TO REMOTE"

The recent class action filed in the Northern District of California illustrates some of the risks accepted by businesses assisting with remote learning. In *H.K. et al. v. Google LLC*, two students, through their father, filed a class action complaint against Google, LLC ("Google").[5] In the complaint, the plaintiffs allege violations of Illinois' BIPA and the federal Children's Online Privacy Protection Act ("COPPA"). The complaint alleges that Google provided ChromeBooks with its pre-installed "G Suite for Education" platform, collecting and storing face scans, voiceprints, and other forms of personal identifying information for children.[6] Specifically, the complaint alleges that Google violated BIPA by providing software to the students and collecting certain biometric data without (1) providing a written policy regarding data retention and destruction of biometric identifiers or biometric information, and (2) securing informed written consent.[7]

Although the class action brought against Google is not specifically tied to actions Google took in response to COVID-19, the lawsuit exemplifies the increased exposure to privacy regulations faced by stakeholders of the recent increases in remote work, learning, and services.

THE RISE IN BIPA LITIGATION

Although BIPA became effective in 2008, the recent uptick in BIPA litigation is a natural result of major court opinions permitting litigants to pursue causes of action against private entities for technical violations of statutory rights. Specifically, in a January 2019 opinion, the Illinois Supreme Court held that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[8]

As hundreds of BIPA-related lawsuits have now been filed by customers and employees in the last two years, biometric information privacy and security has quickly became a

---

[4] BIPA permits any "person aggrieved" by a statutory violation to sue for the greater of either actual damages or "liquidated damages" of $1,000 for a negligent violation or $5,000 for an intentional or reckless violation. *See* 740 ILCS 14/20 (2016).

[5] *H.K. et al. v. Google LLC*, Class Action Complaint, 5:20-cv-02257 (April 2, 2020), *available at* https://www.docketalarm.com/cases/California_Northern_District_Court/5--20-cv-02257/H.K._et_al_v._Google_LLC/.

[6] Class Action Complaint, ¶ 6.

[7] Class Action Complaint, ¶¶ 18-19.

[8] *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1207 (Ill. 2019).

major risk for businesses and their insurers. This increased litigation has raised questions regarding federal court standing and BIPA's extraterritorial impact.

FEDERAL COURT STANDING

Beyond the debates surrounding state statutory standing, the U.S. Courts of Appeals have begun to wrestle with federal court Article III standing. In May 2020, the U.S. Court of Appeals for the Seventh Circuit held that a plaintiff's claims that defendant failed to fulfill the informed consent requirements of BIPA's Section 15(b) satisfied Article III's injury-in-fact requirement.[9] Specifically, the court stated that "[t]his was not a failure to satisfy a purely procedural requirement" as "[plaintiff] did not realize that there was a choice to be made and what the costs and benefits were for each option. This deprivation is a concrete injury-in-fact that is particularized to [her]."[10]

Apart from deepening a circuit split on the standing issue, the court's decision also alerts employers that removal to federal court is one more strategy available in the defense of putative class actions.

EXTRA-TERRITORIALITY

Although businesses may assume their operations are not restricted by BIPA as long as they do not operate in Illinois, this assumption could be costly. The extent of BIPA's geographical reach is not yet fully known. Recent cases like *H.K. et al. v. Google LLC*, filed in California, shed light on the extraterritorial impact of BIPA. But ultimately, the application of BIPA to activity outside of Illinois is fact intensive. This need for case-specific inquiry means that discovery will likely be required before the viability of extraterritoriality defenses can be determined.

In light of the need for rapid action and reaction to the hurdles created by COVID-19, as well as the lack of clarity regarding just how far BIPA regulations extend, businesses can reduce their exposure to BIPA liability by familiarizing themselves with the requirements of the Act and implementing data policies consistent with those requirements.

---

[9] *Bryant et al. v. Compass Group U.S.A. Inc.*, No. 20-1443 (7th Cir. May 5, 2020).
[10] *Id.*