AN A.S. PRATT PUBLICATION
JUNE 2017
VOL. 3 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 5 | JUNE 2017

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 [159] (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

(2017–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.

Illinois Continues Legislative Efforts Aimed at Protecting Consumers' Privacy Rights

By Aaron K. Tantleff and Julia K. Kadish*

The authors of this article explain three bills the Illinois legislature is currently considering to enhance consumer privacy protections.

The Illinois legislature is currently considering three different bills designed to enhance consumer privacy protections. The Right to Know Act[1] would give consumers the right to know what information has been collected about them and who has access to it. The Geolocation Privacy Protection Act[2] prohibits private entities from collecting geo-location information without first meeting specific notice requirements and receiving express consent. Finally, the Microphone-Enabled Device Act[3] protects consumers from the unauthorized use of a device's microphone.

Any business that collects information from Illinois residents will need to revisit their privacy policies and notice and consent procedures to ensure continuing compliance if these laws are enacted.

WHAT DO THE BILLS REQUIRE?

Proposed Act	Requirements
Right to Know Act	Upon consumer request, an organization must provide the following information within 30 days, at no cost to the consumer: • all categories of personal information disclosed; and • names of third parties that receive the personal information.

* Aaron K. Tantleff, a partner and intellectual property lawyer with Foley & Lardner LLP, works with clients on privacy, security, and information management matters as well as state, federal, and international restrictions on the use of information. Julia K. Kadish is an associate at the firm, where her practice focuses on drafting and reviewing technology agreements, and counseling clients on privacy and data security matters. The authors may be contacted at atantleff@foley.com and jkadish@foley.com, respectively.

[1] http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=91&GA=100&DocTypeId=HB&DocNum=2774&GAID=14&LegID=104098&SpecSess=&Session=.

[2] http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=91&GA=100&DocTypeId=HB&DocNum=3449&GAID=14&LegID=&SpecSess=&Session=.

[3] http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=91&GA=100&DocTypeId=HB&DocNum=3819&GAID=14&LegID=105797&SpecSess=&Session=.

Geolocation Privacy Protection Act	Prohibits an entity from collecting, using, storing, or disclosing geolocation information unless it receives affirmative express, consent after providing notice that: • informs the person that his geolocation information will be collected; • discloses the specific purposes for use of such information; and • provides the person a hyperlink or "comparably easily accessible means to access the information.
Microphone-Enabled Devices Act	Prohibits an entity from enabling a digital device's microphone unless it receives informed, written consent after notifying the user in writing: • the microphone will be turned on; • the frequency and length of time the microphone will be turned on; • the specific categories of information the microphone will listen for; and • the specific purpose for collecting the information.

Under the Right to Know Act, any entity that discloses consumer personal information to a third party must make the following information available to the consumer upon request (free of charge): (1) all categories of personal information that are disclosed; (2) the names of all third parties that receive the customer's personal information; and (3) provide a description of the consumer's rights. Businesses must respond to customers *within 30 days of a request*, so organizations should be sure to have a mechanism in place to promptly investigate and address any inquiries. The requirements are not retroactive and will apply only to personal information disclosed on a going forward basis. Failure to comply with this act constitutes a violation of the Consumer Fraud and Deceptive Business Practices Act. Lawsuits filed for a violation of this act shall only be filed by the Attorney General or appropriate State's Attorney's office on behalf of the consumer. Any awards granted for violations will be deposited into the Cyber-secure Illinois Educational Advancement Fund created via the act.[4]

The Geolocation Privacy Protection Act prohibits an entity from collecting, using, storing, or disclosing geolocation information unless it receives "affirmative express consent" after providing "clear, prominent, and accurate notice" that: (1) informs the

[4] The Right to Know Act was amended on April 4, 2017. The amendments to the proposed bill are reflected in this article.

person that his geolocation information will be collected; (2) discloses the specific purposes for use of such information; and (3) provides the person a hyperlink or "comparably easily accessible means to access the information." Violations of the act grant consumers a private cause of action to seek injunctive relief, in addition to any other rights under the Consumer Fraud and Deceptive Business Practices Act.

Lastly, the Microphone-Enabled Devices Act prohibits an entity from enabling a digital device's microphone unless it informs the user in writing:

(1) the microphone will be turned on;
(2) the frequency and length of time the microphone will be turned on;
(3) the specific categories of information the microphone will listen for; and
(4) the specific purpose for collecting the information.

The entity must receive the "informed, written consent" (including through an electronic means) before enabling a device's microphone. Like the other two laws, this act also provides a private cause of action, and consumers may recover liquidated damages ($5,000), injunctive relief, and reasonable attorneys' fees.

ILLINOIS IS NO STRANGER TO TRAILBLAZING PRIVACY LEGISLATION

Enacted in 2008, Illinois' Biometric Information Privacy Act[5] generally requires companies to obtain a person's consent before collecting, capturing, or purchasing a person's "biometric identifier" or "biometric information." Since late 2015, at least six cases have been filed alleging claims under the statute, and the first reported settlement was approved for $1.5 million dollars on December 1, 2016.

While Illinois and Texas are currently the only states with such laws on the books, five other states have pending biometric legislation in committee review (Alaska, Connecticut, Montana, New Hampshire, and Washington). Since BIPA provides a private cause of action unlike Texas' statute which only allows for enforcement through the attorney general, BIPA serves as the model for these other states considering biometric laws.

NEXT STEPS

Now would be a good time for companies to consider reviewing their existing privacy policies and consent practices. California already has a statute similar to the Right to Know Act, impacting companies collecting information about California residents. New York has proposed[6] a comparable bill in January that is still making its way through committee. Regardless of the passage of the Illinois bills, other states are already taking action, and therefore businesses should be prepared to account for

[5] 740 ILCS 14/1 or "BIPA."
[6] https://www.nysenate.gov/legislation/bills/2017/S72.

these existing and pending laws. These laws, both pending and enacted, provide private causes of action, which tend to create increased publicity and ultimately, liability, from regulators as well as the public, including the plaintiffs' bar.

In light of the existing and proposed legislation, companies should consider the following steps:

- Revisit and update your organization's privacy policy to verify that it accurately notifies consumers about the type of information collected.
- Ensure that the privacy policy informs consumers who will be given access to their information, including any third parties to whom their data may be sold.
- Provide contact information whereby consumers can request or obtain copies of the information that has been collected or disclosed.
- Utilize click-wrap or other affirmative consent procedures for collection of geo-location information.