AN A.S. PRATT PUBLICATION
APRIL 2019
VOL. 5 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 3 | APRIL 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 [69] (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 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.

Privacy and Cybersecurity Developments

Jadzia Pierce*

This article looks back at the highlights of 2018 and previews what the remainder of 2019 may have in store in the United States, Europe, and China.

2018 was a busy year for privacy and cybersecurity. This article looks back at the highlights of 2018 and previews what the remainder of 2019 may have in store in the United States, Europe, and China.

UNITED STATES

Privacy

Last year saw a proliferation of several state and federal legislative proposals aimed at protecting consumer privacy and bolstering cybersecurity protections. Notably, California passed the most sweeping privacy law in the country thus far (the California Consumer Privacy Act of 2018 or "CCPA"),[1] and amendments[2] to the law will continue well into next year until the law enters into force in 2020. Following the CCPA, many members of Congress and the administration began proposing their own, federal-level privacy laws (including Senators Ron Wyden (D-OR) and Brian Schatz (D-HI)). It is unclear which of these proposals stands the greatest chance of moving forward in 2019, or how many additional proposals will be introduced by members of the new Congress.

Cybersecurity

As of 2018, all 50 states (plus the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands) have their own state breach notification laws. In addition, Ohio Senate Bill 220[3] entered into force in November. The new law creates a "safe harbor" from certain types of tort-based liability for any "covered entity" that implements a cybersecurity program that satisfies certain requirements. These new laws were enacted against the backdrop continually increasing frequency of and costs associated with cyber incidents.

Federal Trade Commission

The year 2018 ushered in a brand new Federal Trade Commission ("FTC"), which began to signal its enforcement priorities through the "Hearings on Competition and

* Jadzia Pierce is an associate in Covington & Burling LLP's Washington, D.C., office, and a member of the Data Privacy and Cybersecurity and Communications and Media Practice Groups. She may be contacted at jpierce@cov.com.

[1] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[2] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB1121.

[3] https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220.

Consumer Protection in the 21st Century."[4] The hearings suggest that the FTC will continue to focus on privacy, and may pay closer attention to the intersection of privacy and competition. 2019 is becoming a particularly interesting year for the agency, as many federal privacy legislative proposals include provisions that would expand the scope of the agency's authority and provide the agency with rulemaking authority and/or the ability to levy civil penalties.

Surveillance Law

The CLOUD Act,[5] which was signed into law in March 2018, created a framework for government access to data held by tech companies worldwide. We may see that framework be put into action as the United States considers how to approach entering into bilateral executive agreements with certain countries. In addition, the U.S. Supreme Court's decision in *Carpenter vs. United States*[6] held that law enforcement must obtain a warrant in order to obtain cell cite location information from telecommunications providers. The debate over the scope of the decision will continue as federal courts consider what, if any, additional types of information held by third parties may require a warrant.

Privacy in the Courts

In October 2018, a New Jersey federal court dismissed an eight-count class action complaint against smart TV makers, which included a complaint that the makers allegedly violated the Video Privacy Protection Act (VPPA). The Illinois Supreme Court will decide the statutory standing requirements under the Illinois Biometric Information Privacy Act ("BIPA") – the only state biometric law that contains a private right of action.

EUROPE

Of course, the story of the year in 2018 was the General Data Protection Regulation ("GDPR") entered into force[7] on May 25, 2018. The law fundamentally changed the European Union's data protection framework, and has inspired similar laws and legislative proposals in countries such as Brazil[8] and India.[9] European regulators already are intensifying their enforcement of the GDPR, with several investigations launched and fines levied in the past few months alone.

---

[4] https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st?utm_source=govdelivery.

[5] https://www.congress.gov/115/bills/hr1625/BILLS-115hr1625eah.pdf.

[6] https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

[7] https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[8] https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf.

[9] http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.

In addition, in December 2018 the European Commission published[10] its report on the second annual review of the EU-U.S. Privacy Shield. The report concluded that the Privacy Shield "continues to ensure an adequate level of protection" for personal data transferred from the EU to the United States. Separately, the International Trade Administration's Privacy Shield Team released new guidance regarding how a Privacy Shield participant may rely on the Privacy Shield to receive personal data from the United Kingdom following its planned withdrawal from the EU. In particular, the guidance advised that companies that wish to receive data from the United Kingdom will need to update their privacy policies to do so.

The EU also continued to consider the privacy implications of next-generation technologies such as artificial intelligence. The Declaration on Ethics and Protection in Artificial Intelligence[11] was issued at the 40th Annual Data Protection and Privacy Commissioner's Conference in Brussels in October 2018, and in December 2018 the EU High-Level Expert Group on AI published new draft guidance on "AI Ethics." The non-binding guidance stresses that AI must be developed and implemented with a "human-centric approach" that results in "Trustworthy AI," including by respecting privacy.

In 2019, the story of the year will likely be Brexit, with the United Kingdom scheduled to leave the European Union. As of the date of this article, we are unsure whether there will be a transition period, or whether the departure will be a "hard" Brexit. However, on December 13, 2018, the Information Commissioner's Office issued guidance on the state of UK data protection law in the event of a "hard" Brexit.

CHINA

In 2018, China issued[12] the national standard on protection of personal information,[13] which entered into force on May 1, 2018. This standard (although not legally binding) effectively sets out "best practices" that will be expected by regulators who audit companies and enforce China's existing data protection rules.

In addition, China's Ministry of Public Security ("MPS") issued the Draft Regulation on Cybersecurity Multi-Level Protection Scheme,[14] which provides guidance for network operators to comply with obligations relating to the Multi-Level Protection Scheme ("MLPS"), as required by China's Cybersecurity Law. Once the Draft is finalized, enforcement actions by the MPS are expected.

---

[10] https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf.

[11] https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.

[12] http://std.sacinfo.org.cn/gnoc/queryInfo?id=5765F72B812F670F1571443FF09C12D2.

[13] GB/T 35273-2017 Information Technology – Personal Information Security Specification.

[14] http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html.

MPS also released the Regulation on the Internet Security Supervision and Inspection by Public Security Organs, which took effect on November 1, 2018. This regulation provides detailed procedural guidance with respect to how public security bureaus (China's police force, the "PSB") conduct cybersecurity inspections of companies that provide a broad range of "Internet services" in China. This regulation will likely pave the way for more cybersecurity enforcement actions from PSBs in the future.

In 2019, the Regulation for the protection of Critical Information Infrastructure ("CII Regulation") will likely be finalized. The CII Regulation will clarify how CII operators are expected to protect their networks against cyber threats. It will also set out additional obligations that CII operators may face, including allowing officials to perform cybersecurity inspections. In addition, cross-border transfer rules for personal information and other important data are expected to be finalized. Under the latest draft version released on May 19, 2017, companies could face a general obligation to assess the security of their cross-border transfers and potentially undergo security assessments for such transfers by the Chinese government.