AN A.S. PRATT PUBLICATION
JUNE 2020
VOL. 6 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 NUMBER 5 JUNE 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*, [6] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [131] (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.

For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. 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, 230 Park Ave. 7th Floor, New York NY 10169.

The Rise of Internet of Things Security Laws: Part I

By Jeffrey N. Rosenthal and David J. Oberly*

This is the first article in a two-part series examining the enactment of California's Internet of Things ("IoT") security law, and the wave of similar IoT laws expected to follow close behind in 2020. This part discusses the current legal landscape as it relates to the security of connected devices and takes a closer look at California's new IoT security law—which went into effect at the start of the year. The second part, which will appear in an upcoming issue of Pratt's Privacy & Cybersecurity Law Report, *provides tips and strategies for IoT device manufacturers to comply with the IoT security regulations expected to begin to blanket the country.*

At the turn of the century, internet-connected devices were still a thing of science fiction. But rapid technological advances fueled a widespread proliferation of smart technology, otherwise known as the "Internet of Things"—"IoT" for short. Today, the number of IoT devices continues to expand at breakneck speed, with over 75 billion devices projected to be in use by 2025. At the same time, this technology also presents unique risks and challenges—especially as it relates to data security—with cyber-attacks on IoT devices surging a staggering 300 percent in 2019. In response, legislators have sought to enact new laws governing the security of connected devices.

California recently enacted the nation's first law for the "Security of Connected Devices," which expressly governs security requirements for manufacturers of smart devices. Companies should expect additional states enacting similar laws throughout the year. At this juncture it is essential all companies operating in the world of IoT take proactive measures to develop compliance strategies with these laws that will likely become the *de facto* standard for IoT security in the not-too-distant future.

RECENT DEVELOPMENTS AND LOOKING AHEAD

In 2016, the world was introduced to the security risks and vulnerabilities that exist in connection with smart technology when the now-infamous Mirai IoT botnet denial-of-service ("DDoS") attack took place—bringing one of the world's largest website hosting entities to its knees and causing widespread internet outages throughout the U.S. and Europe.

* Jeffrey N. Rosenthal is a partner at Blank Rome LLP. Mr. Rosenthal concentrates his corporate litigation practice on consumer and privacy class action defense. David J. Oberly, an associate at the firm, is a member of the firm's Cybersecurity & Data Privacy group. The authors may be contacted at rosenthal-j@blankrome.com and doberly@blankrome.com, respectively.

Since then, federal lawmakers have introduced a range of bills aimed at implementing uniform minimum security standards for connected devices across all 50 states. To date, however, Congress has failed to enact a federal IoT law; instead the issue of smart device security has been left to the discretion of individual IoT device manufacturers.

That changed in 2018, however, when California enacted a first-of-its-kind IoT security law mandating that all connected devices be equipped with "reasonable security features" to "protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."

California's law will likely be a game-changer for IoT security—not just in California, but across the entire country. Like how California was the first state to enact a mandatory breach notification law in 2002—with all other 49 states following suit—companies can anticipate a similar trend to occur with other states implementing copycat IoT security laws. And much like how the California Consumer Privacy Act of 2018 ("CCPA") is expected to set the standard for consumer privacy laws, California's new IoT law will likely serve as the *de facto* national standard for the IoT industry. In fact, this trend already began in 2019 with Oregon's enactment of its own IoT security law.

In addition, in 2019 the Federal Trade Commission ("FTC") stepped up its enforcement efforts against companies responsible for manufacturing vulnerable connected devices that put consumers' sensitive information at risk.

For example, last year the FTC brought an enforcement action against D-Link, a multinational networking equipment manufacturing company, which ultimately forced the company to overhaul its security platform to remediate significant security shortcomings that left sensitive personal data exposed to third-parties and vulnerable to hackers. It is anticipated the FTC will not just continue, but increase, its enforcement efforts in the area of IoT security moving forward—especially in the absence of any federal IoT security law.

A CLOSER LOOK AT CALIFORNIA'S IOT SECURITY LAW

At its core, California's IoT security law mandates that all connected devices be equipped with "reasonable security features" to "protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."

The definition of "connected device" is extremely expansive, as the law defines the term as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address." This broad definition casts an extremely wide net; wide enough to encompass essentially all devices that are part of the IoT universe, including fitness trackers, connected cars, and smart home devices such as Google Home and Amazon Echo.

Importantly, the California law requires IoT manufacturers to equip their devices with "reasonable security features." Reasonable security features are defined as those that are:

(1) Appropriate to the nature and function of the device;

(2) Appropriate to the information the device may collect, contain, or transmit; and

(3) Designed to protect the device, and any information contained therein, from unauthorized access, destruction, use, modification, or disclosure.

Although the law does not provide any discussion of what constitutes "reasonable security features," it does provide that if a device can be accessed outside a local area network with a password, it will be deemed to have a "reasonable security feature" if the device is equipped with a unique password for each device, or requires users to generate their own password before they can access the device. As such, the California IoT law marks the end of generic default credentials. Importantly, however, the scope of the law is limited to the issue of authentication. Outside of that, the law merely mandates undefined, indeterminate "reasonable security features" as it relates to IoT devices.

The California IoT security law is also short on specifics around enforcement, providing only that it does not provide a basis for a private right of action and that enforcement authority is possessed exclusively by the California attorney general, as well as city, county, and district attorneys. Yet despite the lack of a statutory private right of action, it is expected that the Plaintiff's bar will nevertheless point to the California IoT law as a basis to bring consumer class actions in which the law is deemed to set the industry standard for "reasonableness" in a suit alleging negligence.

Although the ultimate impact of the law remains uncertain, enforcement of California's IoT security law has the potential to significantly expand IoT manufacturers' scope of liability exposure, including precluding certain IoT makers from operating in some of the largest markets.

CONCLUSION

In 2019, many companies spent considerable time and resources attempting to comply with the California IoT law in advance of its January 1, 2020 effective date. Because of the vagueness of the law, and the absence of any substantive guidance/discussion as to what constitutes "reasonable security features," many covered entities experienced significant compliance headaches in trying to ascertain what needed to be achieved by the time it went into effect. Compliance with California's IoT security law will remain a moving target over the course of the next year, especially in the absence of any tangible guidance as to what satisfies the threshold for maintaining "reasonable security features."

At the same time, companies should anticipate additional IoT security laws—modeled heavily after the California law—will be enacted by other state legislatures

across the country. As such, it is important IoT manufacturers continue to pay close attention to the landscape of IoT security law in 2020 as compliance burdens continue to increase.

Further, while the specifics of these anticipated IoT security laws are not currently known, there are still nonetheless many actions that IoT makers can take to proactively prepare for the impending laws. IoT companies should not wait for new laws to be passed, but instead, should take preemptive action by tweaking the design of their IoT security programs to implement several key security controls that will become a common thread among all newly enacted IoT security regulations which. Experienced counsel should be included in all such planning discussions. In doing so, IoT makers can put themselves in the best position to comply with any new regulations that are added to the mix over the course of the next year and beyond.

***

The second part of this article will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report*.