AN A.S. PRATT PUBLICATION
JULY - AUGUST 2020
VOL. 6 • NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 6** **JULY - AUGUST 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 byMatthew Bender & Company, Inc. For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH45342 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 II

By Jeffrey N. Rosenthal and David J. Oberly*

This is the second part of a two-part article 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. The first part of this article, which appeared in the June 2020 issue of Pratt's Privacy & Cybersecurity Law Report, *discussed the current legal landscape as it relates to the security of connected devices and took a closer look at California's new IoT security law – which went into effect at the start of the year. This second part provides tips and strategies for IoT device manufacturers to comply with the IoT security regulations expected to begin to blanket the country.*

In the blink of an eye, Internet of Things ("IoT") technology – which connects household and consumer items to the internet – brought about advanced capabilities that were just years ago thought to be matters of science fiction. Notable examples include connected cars, smart homes, and wearable tech, just to name a few.

At the same time, IoT technology also presents a unique set of risks and challenges – particularly around data security. Because of security vulnerabilities inherent in smart devices, and as IoT technology continues to be applied in numerous new and creative ways, legislators have responded with laws specifically geared toward regulating such connected devices.

Consequently, manufacturers of connected devices must find a way to address the mounting security threat posed by hackers and other cyber criminals, while also complying with the growing body of law governing smart technology. Fortunately, there are several actionable steps IoT manufacturers can take to produce IoT devices with enhanced features and functionality in a manner that complies with the law and provides robust security controls to combat cyber risk.

THE ONCE AND FUTURE IOT SECURITY LAWS

California's new IoT security law requires 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 Federal Trade Commission ("FTC") and state attorneys general have used their enforcement powers to penalize manufacturers that fail to implement "reasonable steps" to secure smart devices. Combined, IoT manufacturers and vendors should approach

* 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.

their compliance efforts with an eye toward implementing "reasonable" security measures in a manner that protects the security of not only consumers, but the general public at large.

Critically, while the California IoT law mandates the implementation of "reasonable security features," the law provides no discussion or insight as to what is sufficient to satisfy this standard. Nor has the FTC (or any other legislative or regulatory body) issued standards or guidance as to what constitutes "reasonable security features" in the context of IoT technology. Without clear direction, IoT manufacturers are placed in a precarious position in terms of determining whether their efforts satisfy the requirements for compliance.

PASSWORD/AUTHENTICATION PRACTICES AND PROTOCOLS

Ultimately, to comply with California's new IoT security law (and expected state laws modeled heavily off the California law), the first step for IoT manufacturers is to revamp their password/authentication practices and protocols. As the California law makes clear, connected devices can no longer rely on default passwords, but must instead feature initial password management requirements that entail – at a minimum – preprogramed passwords for each device or, alternatively, forced generation of new passwords before users can access a device for the first time.

To effectively ensure the security of IoT technology, in most instances it will be necessary to go beyond these minimal password requirements. Here, IoT manufacturers can look to the National Institute of Standards and Technology's ("NIST") Special Publication 800-63B, which offers guidelines on best practices for authentication and digital identity, and which can be directly applied to smart technology. Among NIST's recommendations are to remove password hints and knowledge-based authentication (e.g., what is the first city you lived in?); move from a six-character password minimum to an eight-character minimum; and utilize passphrases instead of simpler passwords (which are common and easily guessed by hackers).

IMPLEMENTATION OF CYBERSECURITY FRAMEWORKS

Ultimately, IoT manufacturers' compliance obligations do not end with enhancement of their devices' password/authentication mechanisms. Importantly – as exemplified by the California IoT law – in addition to implementing new password/authentication protocols, IoT manufacturers must also tailor their smart device security controls to satisfy three broader, more general "reasonable security features" principles to achieve compliance: e.g., appropriate to the nature and function of the device; appropriate to the information collected, contained, or transmitted; and designed to protect the device from unauthorized access, destruction, use, modification, or disclosure, as is required as part of California's IoT security law.

In the absence of any clear direction, IoT manufacturers can look to several well-recognized cybersecurity frameworks for guidance.

First, IoT manufacturers can look to the Center for Internet Security's Critical Security Controls ("CIS Controls"), which offers a list of 20 controls frequently characterized as the gold standard for effective security.

Importantly, in its 2016 Data Breach Report, the California attorney general endorsed the CIS Controls as constituting reasonable security measures. As such, these defensive cyber controls – and, in particular, the *CIS Controls' Internet of Things Companion Guide* that focuses specifically on assisting organizations in applying the CIS Controls to IoT technology – can serve as a blueprint to satisfy the "reasonable security features" standard. At the same time, compliance with the Companion Guide can also put IoT manufacturers in a position to quickly respond to the changing legal landscape and achieve compliance with any similar laws added to the mix in 2020.

In addition, IoT makers should also consider supplementing the CIS Controls by incorporating best practices and recommendations from several other widely-accepted IoT-specific cybersecurity frameworks.

In particular, NIST recently released its Core Cybersecurity Feature Baseline for Securable IoT Devices ("NIST Core Baseline"), which establishes a baseline guide for security that manufacturers may adopt for the IoT devices they produce to build secure devices that incorporate "reasonable security features" from the ground up, as well as information on how to identify and implement features most appropriate for their devices and recommendations for what security features an IoT device should possess.

The Cloud Security Alliance ("CSA") IoT Security Controls Framework also offers guidance on base-level security controls, and is applicable across many IoT domains – from systems which process only "low-value" data with limited impact potential to highly-sensitive systems that support critical services. The CSA Framework can also assist manufacturers in identifying appropriate security controls applicable to specific IoT devices and allocating them to specific components within their systems.

While none of these programs will absolutely ensure IoT devices are impervious to security vulnerabilities, adhering to these programs/frameworks can provide IoT manufacturers with an extra layer of compliance which, in turn, would further aid in demonstrating compliance with "reasonable" security features in the event the manufacturer's security controls are questioned or challenged by enforcement authorities.

OTHER VITAL SECURITY CONTROLS

Finally, in addition to implementing one or more of the above frameworks, IoT manufacturers should also consider implementing several specific, targeted security controls essential to combating the security risks associated with IoT technology:

- IoT manufacturers should incorporate the principle of least privilege, which entails limiting access rights for users, devices, accounts, and programs to only that information/resources that are absolutely necessary to performing legitimate activities which, in turn, can significantly minimize the overall attack surface that can be exploited to compromise smart devices.
- IoT manufacturers should ensure all IoT data is encrypted, both while in transit and while at rest.
- IoT manufacturers should incorporate effective mechanisms into their IoT devices that allow for post-market patching, monitoring, and vulnerability handling after smart devices have entered the stream of commerce.

THE FINAL WORD

California's new IoT security law, which officially went into effect on January 1, 2020, represents the beginning of a new era in IoT regulation – one that will be marked by mandatory security requirements designed to combat the significant vulnerabilities that exist in connection with IoT technology. While California's IoT security law is the first of its kind, it will not be the last. IoT manufacturers should expect to see similar laws popping up in other state legislatures across the United States.

To ensure compliance with this new wave of IoT security laws, IoT manufacturers should take immediate action to confirm security is built into their IoT devices at the outset of the design planning process, which will not only allow manufacturers to align their devices with today's heightened security requirements, but will also enable IoT makers to ensure that their smart devices are secured from today's growing cyber risks to the greatest extent possible. Including experienced counsel in this process remains an important first step that can pay significant dividends.