AN A.S. PRATT PUBLICATION
JANUARY 2019
VOL. 5 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 1 | JANUARY 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 [1] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2019 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

EDITOR-IN-CHIEF

Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenigsberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Baker & McKenzie LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

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. Copyright 2019 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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.

The Significance to Businesses of the California Legislature's Last Minute Revisions to the 2018 California Consumer Privacy Act

By Natasha G. Kohne, Diana E. Schaffner, Dario J. Frommer, and Jo-Ellyn Sakowitz Klein*

The California Legislature passed SB 1121 to revise certain sections of the California Consumer Privacy Act – the nation's strictest privacy protection statute which provides Californians with a right to learn what personal information certain businesses collect about them, to stop the sale of their personal information to third parties and to sue over data breaches if companies fail to adequately protect their information. The authors of this article discuss the Act and the key changes.

The California Consumer Privacy Act ("CCPA" or the "Act"), the nation's broadest privacy protection statute, was enacted by the California Legislature in June 2018 as part of a last-minute deal to stop a proposed statewide ballot measure that could have ushered in an even stricter privacy law.

Sponsored by San Francisco real estate magnate Alastair Mctaggart and privacy advocacy groups, the ballot measure was strongly opposed by business groups and tech interests. Racing to beat a statutory deadline for the Mctaggart measure to be placed on the ballot, the Legislature hastily passed the CCPA in June while promising to introduce cleanup legislation before the end of the legislative term in August.

Efforts to substantively revise the CCPA began nearly immediately after its passage, with the Attorney General's Office ("AGO") (the chief enforcement agency for the CCPA), business groups, and privacy activists pressing for focused changes. Those efforts came together around Senate Bill 1121.

At the beginning of August, Senator Bill Dodd (D-Napa) amended SB 1121 to correct various technical and drafting errors in the CCPA.[1] After intense lobbying from business groups, banks, tech interests, and California Attorney General Xavier Becerra, additional substantive amendments to the CCPA were also adopted as part of SB 1121.

* Natasha G. Kohne (nkohne@akingump.com) is a partner at Akin Gump Strauss Hauer & Feld LLP and co-leader of the firm's cybersecurity, privacy, and data protection practice. Diana E. Schaffner (dschaffner@akingump.com) is a counsel in the firm's litigation practice. Dario J. Frommer (dfrommer@akingump.com) is a partner in the firm's California public law and policy practice. Jo-Ellyn Sakowitz Klein (jsklein@akingump.com) is senior counsel at the firm focused on privacy and data security matters.

[1] AB 375 Chapter XX Statutes of 2018.

On August 22, Attorney General Becerra sent a letter to the co-authors of the CCPA outlining five key complaints that he had with the CCPA and asking for corresponding revisions to the CCPA.[2] Becerra opined that:

> (1) businesses' and third parties' rights to seek AGO opinions as to CCPA compliance issues would unduly burden the AGO and could lead to a conflict with its enforcement role;
>
> (2) the civil penalties included in the CCPA were likely unconstitutional, since they purport to amend and modify the California Unfair Competition Law's[3] civil penalty provision as applied to CCPA violations;
>
> (3) consumers should not have to provide notice to the AGO prior to filing and pursuing their private rights of action related to data breaches;
>
> (4) the AGO would need additional time and resources to draft CCPA regulations; and
>
> (5) consumers should be able to bring a private right of action for any violation of the CCPA, not only for violations tied to a data breach.

Various business groups also lobbied for substantive changes to the CCPA, including:

- adding a defense to consumers' private rights of action where a business implemented an information security framework and documented its compliance with the same;
- expanding the Gramm-Leech Bliley Act ("GLBA") exemption;
- expanding the exemption relating to medical information to cover business associates;
- narrowing the definition of "personal information" to apply to information linked or linkable to a specific individual and excluding household information;
- extending the compliance deadline to 12 months after the AGO enacts its final CCPA-related regulations;
- ensuring that the statewide preemption goes into effect immediately; and
- clarifying the definition of "consumer" to exclude employees, contractors and those involved in business-to-business interactions.

On August 31, SB 1121 passed both houses of the California Legislature and it was approved by the governor on September 23, 2018. The key substantive changes included in SB 1121 are detailed below.

---

[2] X. Becerra Ltr. (Aug. 22, 2018.), *available at* https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical.

[3] Cal. Bus. and Prof. Code.

OVERVIEW OF CHANGES TO CCPA IN SB 1121

The revisions included in SB 1121 fall into two categories: (1) technical or grammatical revisions adopted to fix drafting errors, revise internal inconsistencies, etc.; and (2) substantive revisions that change the enforcement of the CCPA itself. This alert will focus on the latter category. SB 1121 makes the following important changes to the CCPA:

- *Extends Time for the AGO to Adopt Regulations*:[4] The deadline by which the AGO has to adopt CCPA-related regulations was extended by six months from January 1 to July 1, 2020. Attorney General Becerra requested additional time to draft and pass regulations in his August 22 letter.
- *Postpones Enforcement to the Earlier of Six Months from the Date the AGO Adopts its Regulations or July 1, 2020*:[5] In a corresponding change to that noted above, SB 1121 also extends the date on which the AGO can begin enforcing the CCPA by the *earlier* of either six months from the date that the AGO adopts its final CCPA-related regulations or July 1, 2020. Should the AGO adopt its final CCPA-related regulations on July 1, 2020, it appears that businesses may be faced with having to comply with the CCPA on the first day those regulations are promulgated. This could complicate compliance.
- *Makes Statewide Preemption Provision Effective Immediately*:[6] The revisions speed up enforcement of the statewide preemption provision to ensure that it takes effect immediately upon the governor signing SB 1121 into law. This revision is a direct response to local privacy protection efforts, including a "Privacy First" city ballot initiative that San Francisco voters approved in November 2018. As a result of the successful ballot initiative, San Francisco voters approved a new "Privacy First Policy" to which the city, its contractors and its permit holders have to adhere. The city government is supposed to consider the Policy when drafting and proposing a privacy ordinance containing more detailed rules. The SB 1121 will ensure that the CCPA's requirements preempt certain local laws statewide where the local laws overlap with the CCPA.
- *Removes Various Prerequisites to a Consumer Pursuing a Private Right of Action*:[7] SB 1121 removes Subsections 1798.150(b)(2) and (3) from the CCPA, which required consumers to notify the AGO within 30 days of filing a private right of action and then outlined the potential responses of the AGO to that notice. Some of the AGO responses under Subsection 1798.150(b)(2) appeared to limit consumers' ability to pursue their private rights of action if the AGO

[4] Section 1798.185(a).
[5] Section 1798.185(c).
[6] Section 1798.199.
[7] Section 1798.150(b)(2), (3).

responded in a certain manner. In his August 22 letter, Attorney General Becerra complained of the onus that these provisions would put on the AGO and requested that they be eliminated. With this revision, it appears that the only prerequisite a consumer has prior to pursuing a private right of action is providing a business 30 days' notice of an alleged violation and a chance to cure.

- *Modifies the GLBA Exemption*:[8] The revised GLBA exemption eliminates the original requirement that it would apply only if the CCPA was in conflict with the GLBA. It also expands its protection to include personal information covered by the California Financial Information Privacy Act. The new language provides that the CCPA is not applicable to personal information collected, processed, sold or disclosed pursuant to the GLBA or the California Financial Information Privacy Act.[9]
- *Modifies Medical Information Exemptions to Expand Coverage*:[10] While the CCPA included an exemption aimed at limiting its applicability where privacy protection already existed under the California Confidentiality of Medical Information Act ("CMIA")[11] or the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 (together with their implementing regulations, "HIPAA"), the provision was poorly crafted and unduly narrow. SB 1121 overhauls this provision, making important improvements. "Medical information" as defined under and governed by CMIA is exempted. "Protected health information" as defined under HIPAA that is collected by a HIPAA covered entity (such as a hospital or a health plan) or business associate (such as a vendor providing services for the hospital or a health plan that involve processing protected health information) is also exempted. "Providers of health care" as defined under CMIA and HIPAA covered entities are exempted to the extent that they maintain patient information in the same manner as medical information or protected health information in accordance with CMIA and HIPAA, as applicable. Questions remain as to whether a company offering a mobile health app that collects information directly from individuals, without the involvement of a licensed health care professional, may take advantage of these exemptions. In addition, SB 1121 adds a new exemption for information collected as part of clinical trials, as long as the study was subject to certain human-research, subject-protection requirements.
- *Retains the Broad Definition of Personal Information*:[12] Language was added to the existing definition of "personal information" in SB 1121 to clarify that

[8] Section 1798.145(e).
[9] Cal. Fin. Code § 4050 *et seq*.
[10] Section 1798.145(c).
[11] Cal. Civ. Code Part § 56 *et seq.*
[12] Section 1798.140(o)(1).

personal information includes the various examples listed in the CCPA if "it identifies, relates to, describes, is capable of being associated with or could be reasonably linked, directly or indirectly, with a particular consumer or household."

- *Continues Requirement for Intentional Conduct to Trigger Highest Penalty*:[13] At least one of the various iterations of SB 1121 (as amended on August 24) would have amended the CCPA to permit the AGO to seek the highest civil penalty ($7,500) for each violation of the CCPA, intentional or otherwise. However, the final version of SB 1121 reimposed the original limits in the CCPA, including a $2,500 cap for the amount that the AGO can seek for each general violation and a $7,500 cap for the amount that the AGO can seek for each intentional violation.

CONCLUSION

The CCPA goes into effect on January 1, 2020. It remains to be seen whether the business community will continue to push for further CCPA amendments when the Legislature reconvenes in January 2019. These efforts may intensify as more businesses nationwide realize the CCPA's far-reaching scope. Indeed, some estimates suggest that as many as 500,000 companies may fall under the statute. Given that Democrats increased their large majorities in both houses of the Legislature in November, there may be little appetite to scale back CCPA consumer protections. Governor Jerry Brown (D), who was instrumental in brokering the compromise to keep the Mctaggart measure off the ballot, is also set to leave office and will be replaced by Gavin Newsom (D). In addition, there is a likelihood that the CCPA may further embolden other state and local governments outside of California to adopt similar measures. Getting ahead of some of these privacy issues now, before they go into full force in California, may provide businesses with the best means of driving policy development in an area that is sure to affect business practices and costs for years to come.

[13] Section 1798.155(b).