AN A.S. PRATT PUBLICATION
JANUARY 2020
VOL. 6 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 | NUMBER 1 | JANUARY 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 [1] (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. 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 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, 630 Central Ave., New Providence, NJ 07974.

Despite the Passage of CCPA Employee Amendment, Employers Still Face Significant Compliance Burdens Under California's New Privacy Law

By Jennifer J. Daniels, Ana Tagvoryan, David J. Oberly, Ana Amodaj, and Kathy E. Herman*

The California legislature brought much-anticipated clarity and focus to the scope of the California Consumer Privacy Act of 2018 ("CCPA") with the passing of five amendments—including Assembly Bill 25 ("AB 25")—which focuses specifically on employees, job applicants, and other similar classes of individuals. AB 25 places a moratorium until January 2021 on certain CCPA compliance obligations as they relate to employees, job applicants, contractors, and agents, but still requires employers to comply with the privacy notice obligation and the reasonable security provision of the law in 2020. The authors of this article discuss the requirements and offer compliance tips.

The California legislature closed its 2019 legislative session in grand fashion, passing a total of five amendments to the California Consumer Privacy Act of 2018, all of which are expected to be signed into law by the California governor. Included in these amendments is Assembly Bill 25, commonly known as the CCPA's "employee exclusion" amendment.

To the dismay of many employers, however, while an earlier version of AB 25 would have excluded employees altogether from the scope of the CCPA, the version of AB 25 that was ultimately passed by the California legislature stops well short of providing a comprehensive "get out of jail free" card for employers that are covered by California's new sweeping privacy law.

Rather, while offering some benefit to employers by excluding employees from the CCPA's definition of "personal information" at least until 2021, AB 25 contains two critical carve-outs which—taken together—place substantial compliance obligations on employers that had to be satisfied by the law's effect date January 1, 2020.

* Jennifer J. Daniels (daniels@blankrome.com) is a partner at Blank Rome LLP providing counsel on regulatory and general corporate law matters. Ana Tagvoryan (atagvoryan@blankrome.com), a partner at the firm, vice chair of the corporate litigation practice group, and co-chair of the class action defense team, defends high-stakes, consumer class action claims. David J. Oberly (doberly@blankrome.com) is an associate at the firm representing clients in a wide variety of cybersecurity and data privacy and Telephone Consumer Privacy Act matters. Ana Amodaj (aamodaj@blankrome.com) is an associate at the firm concentrating her practice on complex corporate litigation matters. Kathy E. Herman (kherman@blankrome.com) is an associate at the firm providing advice and counsel to companies, management, and entrepreneurs on a broad variety of business issues.

EMPLOYERS STILL OBLIGATED TO PROVIDE NOTICE OF DATA COLLECTION PRACTICES TO EMPLOYEES

Most importantly, AB 25 does not offer any relief to employers as it relates to the CCPA's requirement that covered businesses "shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used" and "shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."

As such, even with the passing of AB 25, by January 2020, an employer covered by the CCPA was required to provide a notice to all job applicants, employees, contractors, and agents that describes how the employer uses and discloses their personal information.

EMPLOYERS STILL SUBJECT TO CCPA'S PRIVATE RIGHT OF ACTION PROVISION

In addition, AB 25 also fails to remove employers from the scope of the CCPA's private right of action provision. Significantly, this private right of action allows consumers, including employees, to pursue individual or class litigation—with sizeable allowable statutory damages—where the consumer's personal information is impacted by a security breach incident and the covered entity is found to have violated its duty to implement reasonable security measures.

Consumers can pursue individual or class lawsuits if their data is compromised by a data breach, and can recover between $100 and $750 in statutory damages per incident. Although this damages figure may seem small, employers must keep in mind that a class of just 10,000 employees under the CCPA would subject an employer to $7.5 million in potential exposure.

Consequently, even with the passing of AB 25, employers will still nonetheless face considerable litigation exposure in the event the employer suffers a data breach that involves the personal information of job applicants, employees, or similar classes of individuals.

In addition, in absence of any exemption from the private right of action provision, employers must also comply with the law's "reasonable security" requirements, which will require employers to put in place "reasonable security practices and procedures" to protect personal information from unauthorized access, exfiltration, theft, or disclosure.

RELIEF FROM OTHER PROVISIONS OF THE CCPA

With that said, AB 25 does give employers some measure of relief from the remaining requirements of the CCPA until January 2021, at least with respect to

personal information used solely in the context of the employee relationship. So, until January 2021, businesses will not need to honor requests for access, erasure, or opt-out from job applicants, employees, contractors, and agents with respect to personal information collected and used solely for employment purposes.

COMPLIANCE TIPS

Many employers that have delayed the commencement of their CCPA compliance efforts in order to obtain additional clarity on the scope of the law's employee amendment will need to speed up their privacy compliance efforts now that the employee amendment has been finalized and signed into law. Covered employers that have not already done so, should take immediate steps to make the necessary changes to bring themselves into compliance with the applicable obligations.

As a starting point, because the employee exception applies only to personal information relating to employees, job applicants, and similar classes of individuals when such data is used solely for employment purposes, employers must complete a data mapping and inventory exercise to determine what personal information is "in scope" for purposes of California's privacy law. At the same time, this mapping and inventory exercise will allow employers to gain an understanding of what data the employer possesses and where it is located, which can be utilized to build out the privacy notices that are mandated by the CCPA.

After determining the universe of personal information that is subject to the CCPA, the next step for employers is to prepare the CCPA-compliant privacy notices which, at a minimum, must provide notice of the categories of personal information that are collected by the employer, as well as the purposes for which that data will be used. In addition, employers will also need to identify a mechanism for providing notice to employees, job applicants, and third-party contractors, and ensure that the employer's notices are made available to those individuals by—at the latest—the start of 2020.

Finally, as the employee exemption does not apply to the CCPA's "reasonable security" requirement and related private right of action, employers must also implement the necessary "reasonable" data security measures to comply with the CCPA. The CCPA requires that employers put in place "reasonable security procedures and practices" to protect personal information from unauthorized access, exfiltration, theft, or disclosure.

Significantly, employers must ensure that they comply with this obligation, as consumers—including employees—are entitled to pursue litigation under the CCPA's private right of action provision if their data is impacted by a data breach event and the employer is found to have violated its duty to implement reasonable security measures.