



SEPTEMBER 2019 • NO. 3

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

On September 13, 2019, 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. As such, employers will need to take immediate action in order to ensure compliance with the CCPA by the time the law goes into effect in less than four months.

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 must be satisfied by the time the law goes into effect on January 1, 2020.

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 is 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 sent to the California governor to be signed into law. Given the limited window of time before the law goes into effect, covered employers should take immediate steps to make the necessary changes to bring themselves into compliance with the applicable obligations by the January 1, 2020 effective date, including the following:

- 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, complete a data mapping and inventory exercise to determine what personal information is "in scope" for purposes of California's privacy law;
- 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, and identify a mechanism for providing the notice to employees, job applicants, and third-party contractors; and
- as the employee exemption does not apply to the CCPA's "reasonable security" requirement and related private right of action, implement the necessary "reasonable" data security measures to comply with the CCPA.

For additional information, please contact:

Jennifer J. Daniels (Data Privacy)
412.932.2754 | daniels@blankrome.com

Ana Tagvoryan (Corporate Litigation, Class Action Defense)
424.239.3465 | atagvoryan@blankrome.com

David J. Oberly (Data Privacy)
513.362.8711 | doberly@blankrome.com

Ana Amodaj (Corporate Litigation)
424.239.3403 | aamodaj@blankrome.com

Kathy E. Herman (Corporate)
215.569.5734 | kherman@blankrome.com