LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice September 23, 2019 | Number 2540

The California Consumer Privacy Act's Amendments Are Final: What Businesses Need to Know

The Act's final statutory form has taken shape, leaving the 2018 version of the law largely intact.

Key Points:

- The California State Senate and Assembly have completed their legislative session, passing only modest amendments to the California Consumer Privacy Act that the Governor is expected to sign before October 13, 2019.
- For most Covered Businesses collecting personal information from California residents and households, not much has changed: the Act's core rights and obligations still largely apply.
- Employee personal information was not completely exempted from the Act as many expected — an employer's transparency obligation to disclose its collection and use of employee personal information survived — while personal information collected through certain business-to-business interactions was exempted from most of the Act. Both limitations are subject to a one year moratorium.
- Certain "niche" changes were adopted — such as a clarified carve out for personal information subject to the FCRA and a new carve out for personal information exchanged to effectuate vehicle warranties or recalls — while most were rejected.
- Data brokers — as broadly defined by the Act — must now register with and be publicly listed by the Attorney General.
- The highly anticipated Attorney General implementing regulations are expected in draft form this fall — likely within the next month.

Refresher on the Act's Main Impact on Consumer-Facing Businesses and Related Third Parties or Service Providers

While amendments of varying practical significance were passed during the legislative session, including an eleventh-hour flurry of activity, the most important point for Covered Businesses (companies that meet the size, revenue, or other tests for transacting with California residents) is that the basic framework has not changed materially.

Consequently, companies have just months to update and remediate their information practices to comply with the Act in the following areas:

- *Transparency obligation*: Covered Businesses must disclose in their privacy policy the personal information they collect, sell, and disclose for business purposes, how that personal information is used, as well as each data right and how it can be exercised. Internal efforts must pay particular attention to the Act's definitions around "personal information," "sale," "service provider," and "third party."
- *Right to know*: Upon verifiable request, California residents have a right to request that a Covered Business provide what personal information has been collected about them and what personal information has been sold or otherwise disclosed about them — by category and specific pieces of data. Companies must have a systematic means to identify and access systems and data elements that fit within scope for implementing the right to know.
- *Right to delete*: Upon verifiable request, California residents have a right to request that their personal information be deleted. The deletion right has significant exceptions. Businesses should take into account specific systems, applications, and operations, so that the company is well-positioned to correctly handle any first-wave requests for deletion.
- *Right to opt-out*: If Covered Businesses "sell" personal information (as broadly and non-intuitively defined by the Act), California residents have the right to opt-out of the sale of their personal information. For many businesses, the (still) very broad definition of sale means that they must provide California residents the choice to opt-out of many more instances of sharing and disclosure than what may be expected. To effectuate this right, the Act requires that Covered Businesses include a "Do Not Sell My Personal Information" button on their homepage.
- *Prohibition against discrimination*: Covered Businesses shall not discriminate (as defined by the Act) against California residents for exercising any rights under the Act. The amendments have not provided much additional clarity about how to reasonably apply this novel provision, including with respect to loyalty programs. Companies need to consider their pricing and service offerings and whether differentiation between California residents runs afoul of this right.
- *Security obligation*: Covered Businesses must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information being collected.

Amendments to the Act

The six new amendments that cleared the legislative chambers this month address scope and definitions, and are important to the application and impact of the Act on Covered Businesses. The most important changes are outlined below.

AB-1355: Constituting one of the more sweeping amendments to the Act, this amendment:

- *Exempts certain personal information involved in a business-to-business communication or transaction*: Very usefully for non-consumer-oriented businesses, AB-1355 exempts from most of the Act for one year (until January 1, 2021) personal information received by a Covered Business that relates to an "employee, owner, director, officer, or contractor" of another business and that stems from a business-to-business communication or transaction within the context of conducting diligence or receiving/providing a product or service. The exemption does not apply to the right to opt-out if a Covered Business is selling this personal information

- *Clarifies exemption of personal information subject to the FCRA*: AB-1355 clarifies that the Act exempts the collection, use, disclosure, and sale of personal information "bearing on" a consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" if the activity is engaged in by a consumer reporting agency, furnisher of information, or user of a consumer report and the activity is regulated by the Fair Credit Reporting Act (FCRA).

- *Clarifies collection and retention obligations*: AB-1355 clarifies that the Act does not require a Covered Business to collect or retain a consumer's personal information that it would not otherwise collect or retain in the ordinary course of business, which should be important in the context of individuals exercising their right to know that do not have an online or other account relationship with the business. While important additional insight into this amendment may appear in the Attorney General regulations, for now, companies do not need to establish processes to collect identifying information about individuals or households where the company only has an IP address or persistent identifiers.

- *Expands obligation to inform employees of consumer rights*: As amended, the Act adds that a Covered Business must ensure that all individuals who handle consumer inquiries are, in addition to the right to know and non-discrimination, informed of the requirements and details related to the right to delete as well as how to direct California residents to exercise that right.

- *Mandates that the Attorney General regulations specifically address how companies are expected to verify, identify, or otherwise handle requests for access to household-level personal information*: AB-1355 requests that the Attorney General adopt a specific regulation to clarify the "procedures" on how to "process and comply" with verifiable requests for specific personal information related to a household as opposed to an individual California resident.

AB-25: Touching on the scope of personal information and the mechanics of a verifiable request, this amendment:

- *Temporarily exempts personal information of employees of a Covered Business from some rights, but leaves an employer's transparency obligation with regard to employee personal information in place*: The amendment exempts for one year (until January 1, 2021) from the Act personal information collected by a Covered Business about an individual "acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of" a Covered Business that is:
    - (i) used in the context of the individual's role at the Covered Business;
    - (ii) used as emergency contact information for the individual; or
    - (iii) retained to administer benefits.

  The exemption does not apply to a Covered Business' transparency obligations, nor does it apply to the private right of action for a security breach. Significantly, this means that Covered Businesses must make disclosures to employees about the data they collect about them and how it is used and shared.

- *Expands the means by which a Covered Business can verify a consumer request*: While the Act specifically solicits the Attorney General's input on how a business should determine the veracity of a "verifiable consumer request," AB-25 expands the means available by stating that a Covered Business may "require authentication that is reasonable in light of the personal information requested." AB-25 also allows a Covered Business to require a consumer who maintains an account with the Covered Business to make the request through that account. Prior to this amendment, the Act provided no such guidance, except to prohibit a Covered Business from requiring an individual to create an account to make a verifiable request (which is still prohibited).

AB-874: This amendment narrows the definition of "personal information" in the following ways:

- *Inserts the word "reasonably" in front of the broadest element of the definition of "personal information," which had been widely criticized*: AB-874 defines "personal information" as information that "identifies, relates to, describes, is ***reasonably*** capable of being associated with, or could reasonably be linked, directly, or indirectly, with a particular consumer or household." While this change may prove helpful for Covered Businesses that minimize data and rely on contractual prohibitions on associating data with known natural persons, it may have limited practical significance. The definition goes on to enumerate statutory categories of personal information, which include data elements often treated as pseudonymous or even anonymous, such as IP addresses or persistent identifiers. Thus, the impact of this useful limitation on the prior concept of information that is merely "capable" of being associated with a California resident or household is ambiguous for now.

- *Clarifies definition of "publicly available" information*: "Personal information" does not include "publicly available" information. AB-874 streamlines the definition of "publicly available" to mean "information that is lawfully made available from federal, state, or local government records." AB-874 also eliminates the caveat that information is no longer "publicly available" if it is used for a purpose not compatible with why it was publicly maintained.

- *Corrects a significant drafting error*: AB-874 clarifies that "personal information" does not include de-identified (as defined by the Act) and aggregate consumer information.

AB-1146: This amendment exempts from the Act certain vehicle and/or ownership information (as defined by the amendment) that is shared between a vehicle dealer and manufacturer for the purposes of effectuating a repair or recall.

AB-1564: This amendment eliminates, for certain businesses, the requirement specifically to provide a toll-free phone number for California residents to exercise their right to know. As amended, a Covered Business that operates "exclusively online" and has a "direct relationship" with the California residents from whom it collects personal information can provide its California residents with just an email address to exercise their rights. AB-1564 also moves and maintains the requirement that if the Covered Business maintains a website, a consumer must be able to submit a request via that website.

AB-1202: This (surprise, last-minute) bill adds an obligation that any data broker must register with the Attorney General or face a civil penalty. The Attorney General must also create a page on its website to list the registered data brokers. "Data broker" is defined by AB-1202 to include any business that collects and sells personal information of a consumer that the business does not have a direct relationship with. Given the broad definition of "sell" under the Act — "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration" — this amendment could encompass a large number of businesses that would not otherwise self-identify as data brokers. And failing to register (even unintentionally) could have enforcement and litigation consequences. Businesses should analyze their data practices and confirm whether they qualify as a data broker under AB-1202's broad definition.

Final Considerations

Compliance with the Act goes well beyond simply updating a privacy policy. Now that Covered Businesses have a concrete set of rights and obligations that they will have to follow, any business that has not started a data assessment, or that has only done so preliminarily, should immediately engage in a comprehensive compliance assessment and establish a project plan that will ensure material compliance by 2020.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Michael H. Rubin
michael.rubin@lw.com
+1.415.395.8154
San Francisco

Robert Blamires
robert.blamires@lw.com
+1.415.395.8142
San Francisco

Scott C. Jones
scott.jones@lw.com
+1.202.637.3316
Washington D.C.

Marissa R. Boynton
marissa.boynton@lw.com
+1.202.637.3307
Washington D.C.

You Might Also Be Interested In

4 Questions to Consider When Dealing With Children's Data in the US

FTC Hearings Discuss the State of Data Security in the 21st Century

Deep Dive on Deep Learning: FTC Considers Artificial Intelligence