California privacy law poised to alter US privacy landscape

Data Protection, Privacy and Security Alert

28 JUN 2018
By:

For decades, US state legislatures have taken an incremental approach to privacy regulation, passing legislation that addressed specific privacy issues (*eg*, a host of employee privacy laws, online privacy policy requirements, SSN privacy) but rejecting bills proposing broad-based creation of new privacy rights.

This pattern changed abruptly this week in California, where both houses of the legislature hastily passed the California Consumer Privacy Act of 2018 (AB 375), a long and confusingly drafted bill that would enshrine in California law a significant number of data subject rights found in the GDPR. Although this law does not take effect for 18 months and could change, it is a major development that companies should study carefully and develop plans for.

AB375/CA PRIVACY BALLOT INITIATIVE

The bill's provisions become operative only if the CA Privacy Ballot Initiative (No. 17-0039), a similar proposal with far greater class action enforcement risk, is withdrawn from the ballot, which is expected to occur by the time of passage.

EFFECTIVE DATE

Assuming the ballot initiative is withdrawn, the bill's provisions will become operative on January 1, 2020. AB 375's 33 page text was released with numerous drafting errors only a week before it was passed (in an effort to pass it by the state's deadline for withdrawal of the Initiative). The delayed effective date gives the legislature the ability to clarify the text of AB 375 before it goes into effect.

DEFINITIONS (§ 1798.140)

The bill applies to a broader range of "Personal Information" (PI) than found in any other US privacy law, broader even than the same term used in the GDPR. It defines **"Personal Information"** as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably linked, directly or indirectly, with a particular consumer or household." The definition consists of a long list of items, including IP addresses, persistent or probabilistic identifiers that can be used to identify a particular consumer or device records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies; Internet or other electronic network activity information, professional or employment-related information; or any consumer profile. The definition excludes public record information, but only if that information is used for a purpose consistent with the purpose for which the information was made publicly available.

It protects "consumers," who are defined as California residents, even if identified only by unique identifier.

It heavily regulates selling "personal information," and defines the term "sell" broadly, as any disclosure "for monetary or other valuable consideration."

REQUIREMENTS

Right to know (§§ 1798.100, 1798.110): At or before the point of collection, businesses collecting a California consumer's PI must inform the consumer as to the categories of PI to be collected, and the purposes for which the information will be used. Additional uses or collection of additional data require notice to the consumer. Consumers have the right to request that businesses collecting a consumer's PI disclose to the consumer the categories and specific pieces of PI the business has collected.

Consumers have the right to request that a business disclose, and, upon verification of the request, businesses have the obligation to disclose, the following: specific categories of PI, categories of sources from which the PI is collected; the business/commercial purpose for collecting or selling PI; categories of third parties with whom the business shares PI; specific pieces of PI it has collected about the consumer.

Right of access and data portability (§ 1798.100): Upon receipt of a verifiable request, a business must provide a consumer with access to this information held by the business and to obtain it “in a readily useable format” that allows porting the data to another entity “without hindrance.” Consumers may make this request to a business no more than twice in a calendar year. Businesses are not required to retain information that is obtained in a one-time transaction or to re-identify or link information that is not in identifiable form (although this limitation does not appear to apply to pseudonymized data, which may need to be re-identified).

Right to be forgotten (§ 1798.105): A consumer has the right to request that a business delete any PI about the consumer which the business has collected from the consumer, subject to certain exceptions (if it is necessary to provide a good or service the customer ordered; for security purposes; for law enforcement purposes, etc.). Businesses are required to notify customers of this right to request the deletion to the customer.

Disclosure of and choice regarding sale of PI to third party (§ 1798.115): Businesses must provide notice and opt-out consent prior to selling or disclosing PI to third parties. Consumers have the right to request, and businesses have the obligation to provide, the categories of PI about the consumer sold/disclosed.

Opt out right (§§ 1798.120; 1798.135): Consumers have the right to opt out of businesses selling their PI. A business must make available, in a form reasonably accessible to consumers: a clear and conspicuous link to the homepage, titled "Do Not Sell My Personal Information." The link must go to a webpage that enables a consumer to opt out of the sale of the consumer's PI.

The business must wait a minimum of 12 months before requesting to sell the PI of a consumer who has opted out

Opt in right (§ 1798.120): The selling of a minor's PI who is less than 16 years of age is prohibited unless the minor explicitly opts in. In the case of a minor younger than 13 years of age, the parent/guardian is required to opt in.

Anti-discrimination (§ 1798.125): Businesses may not deny goods, charge different prices or rates, provide a different level or quality of service, or suggest that a consumer will receive different prices or service levels based on the consumer's exercise of his/her rights. In contrast to the Initiative, AB 375 added an exception if the different prices/rates /levels/quality of services provided are reasonably related to the value provided to the consumer by the consumer's data.[1] Financial incentives offered to the consumer for the collection, sale, or deletion of personal data are permitted only with prior opt-in consent by the consumer.

Method of consumer request/business response (§ 1798.130): A business must make available two or more designated methods for requests for information, including at a minimum, a toll-free telephone number and a website address (if the business maintains a website). The business must "disclose and deliver" to the consumer the required information within 45 days, inclusive of consumer request verification. There is a 45-day extension when reasonably necessary, subject to consumer notification. There is also a 90 day extension available to businesses "when necessary" (1798.145).

The disclosure must cover the prior 12-month period preceding the business's receipt of the request. It must be made in writing, and if the consumer maintains an account with the business, be delivered through that account. A business need not provide these disclosures to the same consumer more than twice in a 12-month period.

In order to comply with 1798.110, businesses shall associate the information provided by the consumer in the request to any PI previously collected by the business about the consumer.[2]

Privacy policy disclosures (§§ 1798.130, 1798.135): A business must disclose in its online privacy policy (if it has one), and update at least once every 12 months, a description of a consumer's rights as stated in this act, as well as the methods for submitting requests; a list of the categories of PI it has collected about consumers in the preceding 12 months; a list of the categories of PI it has sold about consumers in the preceding 12 months; a list of the categories of PI it has disclosed about consumers for a business purpose in the preceding 12 months.

Additionally, a privacy policy must also contain a link to a "Do Not Sell My Personal Information" part of its privacy policy, and in any California-specific description of consumers' privacy rights.

EXCEPTIONS (§ 1798.45)

AB 375 exempts entities or information collection/disclosure regulated by: (1) either California's Confidentiality of Medical Information Act or the federal HIPAA law; (2) sale of personal information to or from a credit bureau that is reported in, or used to generate a consumer report under the FCRA; (3) personal information regulated by the Gramm-Leach-Bliley Act and GLBA rules, to the extent AB375 conflicts; and (4) personal information regulated under the Driver's Privacy Protection Act, to the extent AB375 conflicts.

The bill does not restrict a business's ability to collect, use, retain, sell or disclose de-identified or aggregate consumer information, nor does it restrict "commercial conduct [that] takes place wholly outside of California," if that information was not collected while the consumer was in California.

Data breach expansion/private right of action (§ 1798.150): In contrast to the Initiative, which had very broad class action enforcement regardless of any proof of harm, the privacy provisions of AB 375 are enforced by the state AG. However, one section authorizes[3] a private right of action for data breaches involving PI under California's data security law without any proof of harm. The activity triggering enforcement is unauthorized access and exfiltration, theft, or disclosure of this information as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the business," a term which is undefined.

Statutory damages under this section are set at not less than $100 nor greater than $750 per consumer per incident, or actual damages, whichever is greater. Damages for a civil action brought by the Attorney General are set at up to $7,500 per violation for intentional conduct.

Enforcement (§ 1798.155): Businesses may cure alleged violations within 30 days of being notified of the violation – although curing a data breach may be difficult.

To learn more about this new measure, contact either of the authors.

---

[1] Note: § 1798.125(a)(2) states that "nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is **reasonably related** to the value provided to the consumer by the consumer's data." However, § 1798.125(b)(1) states in part, "A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is **directly related** to the value provided to the consumer by the consumer's data.

[2] However, § 1798.145 has a provision stating that 'this title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information."

[3] This provision is the subject of debate, as 1798.150(c) states, "Nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law." See also 1798.155, which states in part, "The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought…by the Attorney General."