Related Attorneys: Sean Hoar Bryan Thompson
Related Practices: Data Privacy & Cybersecurity

California Enacts Sweeping, EU-Style Privacy Law

July 06, 2018
On June 28, 2018, California Governor Jerry Brown signed A.B. 375 into law, a robust bill that provides substantially broader...

By Bryan M. Thompson and Sean B. Hoar

On June 28, 2018, California Governor Jerry Brown signed A.B. 375 into law, a robust bill that provides substantially broader privacy rights to California consumers regarding how certain businesses can collect, use, sell, and disclose their personal information. The new law requires such businesses to be more transparent in their data collection and sharing practices.

Also known as the California Consumer Privacy Act of 2018 (the Privacy Act, or the Act), A.B. 375 was passed unanimously by the California Legislature, in part due to recent alleged instances of consumer data misuse and unauthorized disclosures, and to give Californians more control over their personal information. The Legislature passed the Privacy Act with the understanding that an even more stringent

measure would be removed from ballots in the November election. The proposed ballot measure would have granted California consumers a broader private right of action and allowed costlier penalties against businesses for violations.

The Privacy Act, which goes into effect on **January 1, 2020**, is reminiscent of the European Union's (EU) recently enacted General Data Protection Regulation (GDPR), which expanded the rights of EU residents to know and control the use of their "personal data" by businesses both within and beyond the EU's borders. Both the California Act and the GDPR grant individuals the right to access and delete their personal information held by a business under certain circumstances. Ultimately, compliance with one of the data privacy schemes will assist businesses comply with the other.

What Does the Privacy Act Do?

In summary, the Privacy Act expands California consumers' rights concerning their personal information:

- **Right to Information:** Consumers have a right to disclosure of the categories of personal information collected, the categories of sources from which the personal information is collected, the business purpose for collecting or selling the information, the categories of third parties to whom the information is shared, and the specific pieces of personal information that has been collected.
- **Right to Erasure/California "Right to be Forgotten":** Consumers have a right to request deletion of their personal information, and to have it deleted when the information is no longer necessary for legitimate business purposes.
- **Right to Opt-Out of Sale of Personal Information:** Consumers have a right to know whether a business has sold the consumer's information and to direct a business to not sell the information, or to "opt-out" of information sharing.
- **Minor Rights:** Businesses are prohibited from selling personal information of minors under 16 years old without valid "opt-in" consent.
- **Non-Discrimination:** Consumers have the right to not be discriminated against based upon the exercise of rights under the Act. This includes the right to not be denied goods or services, to not be denied levels of quality of goods or services, or to not be charged different prices or rates, due to the exercise of rights under the Act.

The Act also requires covered businesses to increase their transparency in their data collection and use practices. For instance, the Privacy Act requires such businesses to state in their online privacy policies the rights of California consumers' under the Act, and list the categories of personal information collected, disclosed, and sold over the past 12 months.

What Is "Personal Information" under the Privacy Act?

The Privacy Act expansively defines "personal information" to mean "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The Act includes a laundry list of data sets that fall within its scope, not limited to:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Any categories of personal information described in subdivision (e) of Section 1798.80 (any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including, but not limited to, his or her name, signature, social security number, physical

characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information);
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

However, the Privacy Act does not cover:

- Protected or health information covered under the California Confidentiality of Medical Information Act or the federal Health Insurance Portability and Accountability Act (HIPAA);
- Personal information sold to or from a consumer reporting agency if used in accordance with the federal Fair Credit Reporting Act (FCRA); or
- Personal information collected, processed, sold, or disclosed in accordance with the federal Gramm-Leach-Bliley Act (GBLA) or Driver's Privacy Protection Act.

Ultimately, this definition is substantially broader than how most states – including California – define personal information under their respective data breach notification statutes. This means that, to be in compliance with the Act, covered businesses must account for much more of the information they maintain on California consumers. In the end, businesses should review how much consumer "personal information" is necessary for their legitimate business purposes, and ensure they are not collecting or sharing more data than is necessary for legitimate business purposes.

What Types of Businesses Does the Privacy Act Apply To?

The Privacy Act does not apply to *all* businesses that handle California consumers' data. Instead, the Act applies to certain for-profit businesses that do business in California, control the collection or processing of consumers' personal information, and meet one of the following thresholds:

- Have annual gross revenues in excess of $25 million;
- Annually process personal information of 50,000 or more California consumers, households, or devices; or
- Derive 50 percent or more of its annual revenues from selling consumers' personal information.

How Will the Privacy Act be Enforced?

A.B. 375 contains a number of enforcement tools for both California consumers and the Attorney General. First, the Act creates a private right of action for any consumer whose unencrypted "personal information" – as defined under California's information security standard at California Civil Code 1798.81.5 – is acquired without authorization as a result of a business' failure to implement and

maintain reasonable security procedures to protect personal information. A consumer may institute a civil action to recover damages between $100 and $750 per consumer *per incident*, or actual damages, whichever is *greater*. A court may also order injunctive or declaratory relief, or any other relief it deems proper. Prior to initiating any action, however, the California consumer must provide the business 30 days notice to "cure" the violation unless the action is solely for actual pecuniary damages. A consumer bringing an action must also provide notice to the Attorney General within 30 days of the action being filed. This will then require the Attorney General to review the action and either prosecute the action in place of the consumer, allow the action to proceed, or attempt to stop the action.

Intentional violations of the Privacy Act may be assessed a $7,500 penalty for each violation.

Businesses and covered third parties concerned about how they can comply with the Privacy Act can seek an advisory opinion from the Attorney General. Such entities should note that, if an entity is put on notice by the Attorney General of alleged noncompliance, it will have 30 days to correct its actions and cure the violation, or it will be found in violation of the Act. Consequently, there may be a risk that by reaching out to the Attorney General for guidance, a business will be found to be non-compliant and required to take quick action to avoid penalties.

The bottom line is that the landscape just got much more expensive for businesses. Historically, the California Attorney General's office has carefully picked its battles. Now it will be required to scrutinize matters that would have otherwise flown below its radar.

What does this mean for Businesses?

Prior to the GDPR taking effect on May 25, many U.S.-based companies assessed if the regulation applied to them and, if so, took steps to comply with it. Businesses must similarly assess if their operations fall within the Privacy Act's requirements and plan accordingly.

Though the new law does not take effect until January 1, 2020, companies should take advantage of the opportunity and time to become compliant with the Act. Accordingly, businesses should take the following steps to operationalize the Privacy Act's requirements:

- Review their data collection and disclosure policies, including to what degree they sell or make California consumers' data available to third parties;
- Examine their data minimization practices to ensure that they do not collect personal information unnecessarily;
- Inventory the data that is currently collected and retained;
- Review their data retention policies, and consider revisions where appropriate to ensure that data is not kept longer than needed for legitimate business purposes;
- Consider appointing a "data protection officer" to manage its compliance with this and other data privacy requirements;
- Establish internal policies and procedures to respond to California consumer inquiries and opt-out requests in the timeframes mandated by the Act;
- Examine and update online privacy policies to include the Act's required disclosures; and
- Consult with experienced counsel about other measures that may be necessary to come into compliance.