SADDLE UP AMERICA: California Aims to Pass its Own GDPR Law

Dana B. Rosenfeld, Alysa Z. Hutnik

June 7, 2018

Just when you think you've tackled the Wild, Wild West of GDPR and privacy compliance, California decides to mix it all up again.

This November 6th, California voters will decide on the California Consumer Privacy Act ("Act"), a statewide ballot proposition intended to give California consumers more "rights" with respect to personal information ("PII") collected from or about them. Much like CalOPPA, California's Do-Not-Track and Shine the Light laws, the Act will have broader consequences for companies operating nationwide.

The Act provides certain consumer "rights" and requires companies to disclose the categories of PII collected, and identify with whom the PII is shared or sold. It also includes a right to prevent the sale of PII to third parties, and imposes requirements on businesses to safeguard PII. If passed, the Act would take effect on November 7, 2018, but would apply to PII collected or sold by a business on or after nine (9) months from the effective date – *i.e.*, on August 7, 2019.

Who is Covered?

The Act is intended to cover businesses that earn $50 million a year in revenue, or businesses that "sell" PII either by (1) selling 100,000 consumer's records each year, or (2) deriving 50% of their annual revenue by selling PII. These categories of businesses must comply if they collect or sell Californians' PII, regardless of whether they are located in California, a different state, or even a different country.

What is Considered PII?

The term "personal information" is broadly defined as "information that identifies, relates to, describes, references, is capable of being associated with, or could reasonable be linked, directly or indirectly, with a particular consumer or device." The term expressly includes, but is not limited to:

- Typical personal or contact information (such as name, address, email, account name, SSN, driver's license number, or other similar identifiers);

- Any persistent identifier that can be used to recognize a consumer or a device over time and across different services (such as IP address, device identifier, cookies, beacons, pixel tags, mobile ad identifiers, or similar technology, customer number or user alias);
- Internet or other electronic network activity information (such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement), or geolocation data;
- Commercial and purchasing information (such as records of property, products or services that have been provided, obtained or considered, or other purchasing or consuming histories or tendencies);
- Biometric data, or audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information, information relating to characteristics of protected classifications under California or federal law (such as race, ethnicity, or gender); and
- Any inferences drawn from any of this information.

PII does not include information that is publicly available or that is de-identified.

What are the Consumer "Rights"?

The Act enumerates four specific consumer "rights":

- **"Right to Know" What PII is Collected**: Consumers would have the right to request that a business that collects PII disclose the categories of PII that it has collected about the consumer.
- **"Right to Know" Whether Information is Sold or Disclosed**: Consumers would have the right to request that a business that sells PII or discloses it for a business purpose identify the categories of PII that the business sold or disclosed about the consumer and the identity of the third parties (name and contact information) to whom it was sold or disclosed (whether or not it was sold or disclosed for marketing purposes).
- **"Right to Say No" to Sale of PII**: A consumer shall also have the right to direct a business that sells PII about the customer, not to sell the customer's PII. Businesses must provide notice on the website or app homepage and privacy policy that such information may be sold and that consumers have a right to opt out of such sale.
- **"Right to Equal Service and Price"**: The Act provides that a business is prohibited from discriminating against a consumer for exercising these rights. This includes prohibiting the business from denying goods or services to the consumer, charging different prices or rates (including through the use of discounts or other benefits or imposing penalties), providing a different level of quality or services, or suggesting that the consumer will receive a different price or rate, or level of quality or service, for exercising these rights.

How Do Businesses Comply?

The Act provides very specific compliance obligations for each of the consumer rights, and enumerates certain disclosure requirements for online privacy policies. This includes:

- **Contact Designation**: Business must designate two or more methods for submitting requests, including at a minimum a toll-free telephone number, and if the business maintains a website,

the website address.

- **Timeframe for Response**: Business would be required to provide the requested information free of charge and within 45 days of receiving a verifiable request from the consumer. Businesses must take steps to verify the request, but this verification shall not extend the 45 day time period to respond. The disclosure must cover the information collected, sold, or disclosed in the preceding 12 months.
- **"Right to Say No"**: Business must provide a clear and conspicuous link on the homepage *and* in the online privacy policy, titled "Do Not Sell My Personal Information," that provides consumers a link of where to opt out of the sale of the consumer's PII.
- **Privacy Policy Requirements**: The Privacy Policy must contain the following information, and must be updated *at least* once every 12 months:
    - A description of the consumers' "rights."
    - A list of the categories of PII it has collected about consumers in the preceding 12 months by reference to one or more of the enumerated categories in the Act.
    - A list of the categories of PII that it has sold about consumers in the preceding 12 months by reference to one or more of the enumerated categories, or if a business has not sold consumers' information, the business shall disclose that fact.
    - A separate list of the categories of PII it has disclosed about consumers for a business purpose in the preceding 12 months by reference to one or more of the enumerated categories, or if a business has not disclosed consumers' information for a business purpose, the business shall disclose that fact.
- **Reasonable Security Measures**: Businesses must implement and maintain reasonable security procedures and practices, appropriate to the nature of the information, to protect the PII from unauthorized disclosure.

What are the Penalties for Failing to Comply?

The Act provides a private right of action for any consumer suffering a violation of the Act, and permits statutory damages in the amount of $1,000 per violation or actual damages (whichever is greater), or up to $3,000 or actual damages (whichever is greater) per knowing and willful violation.

The Act also permits a number of public entities (including the Attorney General, any district attorney, and certain county counsel, city attorneys, or city prosecutors) to bring an enforcement action and issue a civil penalty of up to $7,500 for each violation.

The Act contains a whistleblower provision allowing any person who becomes aware, based on non-public information, that a person or business has violated the Act to file a civil action for civil penalties, provided that notice is first given to the Attorney General.

* * *

For companies around the country, this California proposition will be one to watch during the November 2018 general election.