LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Information Law, Data Privacy & Cybersecurity Practice

April 16, 2018 | Number 2301

California's Consumer Right to Privacy Ballot Initiative – What You Need to Know

California ballot initiative, Consumer Right to Privacy Act of 2018, gathers momentum for a November vote, spurring some telecom and internet businesses to organize opposition.

Key Points:

- The ballot initiative proposes to grant consumers an express "right to know" about all of their personal information that is collected, sold, or disclosed by a covered business, with the right to opt-out from having their personal information disclosed by a covered business.
- Businesses covered under the new law would be explicitly prohibited from charging consumers who have opted-out from data sharing a different price for the same goods or services offered to those who have not opted-out.
- The ballot initiative provides for significant new enforcement mechanisms – a private right of action (with statutory damages) for violations of the law, whistleblower incentives, and state attorney general enforcement.

Businesses are preparing to oppose a CA ballot measure that could impose new data privacy and security obligations, with the threat of significant civil liability for non-compliance. Signatures are being gathered to put the Consumer Right to Privacy Act of 2018 (the "CRPA Measure") on the November 2018 California ballot. The CRPA Measure, introduced by two California citizens, claims to give California consumers an "effective way to control their personal information" by providing them with (1) a right to request certain information about what personal information covered businesses have collected and sold or disclosed within the last year and (2) the right to opt-out from having their personal information disclosed by a covered business. The initiative also provides multiple avenues for enforcement (private civil actions; attorney general or local prosecutor enforcement; and whistleblower actions).

Procedural Posture In California, new laws can be adopted via the ballot initiative process, which gives California citizens a way to propose laws and constitutional amendments without going through the legislative process. At this early stage, whether the proponents of the CRPA Measure will secure the 365,880 signatures required to put the CRPA Measure on the November 2018 ballot remains unclear. The deadline to collect signatures is June 18, 2018.

As of February 6, 2018, proponents of the CRPA Measure reported having collected at least 25% of the required signatures. If the CRPA Measure obtains the necessary number of valid signatures, the measure

would appear on the November 2018 ballot. If a majority of Californians vote in favor of the CRPA Measure, the measure would become state law — having the same legal effect as if it had been passed by the state legislature and signed by the governor.

Background on California Consumer Privacy and Security Laws

The CRPA Measure seeks to impose additional data privacy and security obligations that build on the state privacy laws already on the books in California, including the following:

- **Shine the Light Law.** Enacted in 2005, "Shine the Light" requires covered businesses to disclose within 30 days of receiving a customer's request: (1) the types of personal information the business shared with third parties for the third parties' direct marketing purposes; and (2) the identities of the companies with which the covered business shared the information during the prior 12 months. Alternatively, a covered business may be exempt from the aforementioned disclosure requirements if it adopts a policy permitting customers to opt out of disclosing their personal information to third parties for the third parties' direct marketing purposes. *See* Cal. Civ. Code § 1798.83(a)(1)-(2).

- **California Online Privacy Protection Act (CalOPPA).** CalOPPA requires that any person or company whose website collects personally identifiable information from California consumers include a conspicuous privacy policy on their website stating what information is collected and with whom it is shared. *See* Business and Professions Code §§ 22575 – 22579. CalOPPA also requires the website operator or online service to comply with the site's privacy policy. *Id.* According to CalOPPA, conspicuously posting a privacy policy means any of the following:

    - The privacy policy is shown on the website's homepage.

    - A link — via an icon that contains the word "privacy" — appears on the homepage and directly takes consumers to the privacy policy. In this instance, the icon must be in a color different from the homepage's background.

    - The privacy policy is linked to the homepage via a hypertext link that contains the word privacy, written in capital letters equal to or greater in size than the surrounding text; is displayed in a type, font or color that contrasts with the surrounding text of the same size; or is otherwise distinguishable from surrounding text on the homepage.

- **California Data Breach Notification Law.** The California data breach notification law generally requires businesses to notify, without unreasonable delay, California residents whose personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person. *See* Cal. Civ. Code § 1798.82.

CRPA Measure Overview

As described below, the CRPA Measure codifies several broad privacy disclosure, consent, and security obligations. Technical compliance with these new obligations may require some effort and, in certain instances, implementation of new obligations (like the opt-out provision) may be difficult. However, in many respects, the CRPA's substantive requirements do not significantly depart from existing expected practices. Nevertheless, the CRPA Measure, if passed, could significantly impact covered businesses as a result of the new enforcement paradigm it creates by establishing a private right of action (with statutory damages), as well as a whistleblower enforcement mechanism.

CRPA Measure — Key Definitions

The definitions below are critical to interpreting the CRPA Measure. As a result of employing a somewhat limiting definition of the term "business," the CRPA Measure does not cover many smaller companies doing business in California. However, by adopting broad definitions of the terms "personal information" and "sell" (outlined below), the CRPA Measure expands the obligations on businesses that are covered by the CRPA Measure.

A. **Business** — The CRPA Measure limits the universe of affected companies by defining the term business to include only companies that (1) do business in California; (2) collect or **sell** consumers' personal information; and (3) either (a) have annual gross revenues of US$50 million or more; (b) derive at least 50% of their revenues from **selling** personal information; or (c) **sell** the personal information of "100,000 or more consumers or devices"[1] each year. The definition applies to both online and brick-and-mortar businesses that meet the above-mentioned criteria.

B. **Personal Information** — The CRPA Measure adopts an expansive definition of the term personal information (more expansive than under other California laws). The definition includes (in addition to expected contents like name and address): (1) biometric data; (2) internet activity (including interaction with webpages or ads); (3) purchase and consumption history; (4) geolocation data; (5) psychometric information; (6) professional or employment-related information; (7) IP address, and (8) inferences drawn about consumers from such data.[2] Publicly available information and de-identified information is excluded.[3]

C. **Sell, selling, sale, or sold** — Under the CRPA Measure, these terms are broadly defined to include "selling, renting, *releasing*, disclosing, disseminating, *making available*, *transferring*, or otherwise communicating orally, in writing, or by … other means, a consumer's personal information" to a third party for "valuable consideration." *See* CRPA Measure § 1798.106(q) (emphases added). The terms also include "sharing, orally, in writing, or [otherwise] a consumer's personal information with a third party, whether for valuable consideration *or for no consideration*, *for the third party's commercial purposes*."[4] *See id.* (emphases added).

The CRPA Measure Expands on Existing California Privacy Protections

The CRPA Measure meaningfully expands upon existing California privacy and security laws in the following ways.

A. **Expanded Consumer Right-to-Know and Opt-Out Requirement.** The 2005 California Shine the Light law required businesses to either (i) accommodate consumer requests about personal information disclosed for direct marketing purposes or (ii) provide a means for consumers to opt out of the disclosure of their personal information for direct marketing purposes. Under the CRPA Measure, consumers have an express "right to know" about all personal information collected (CRPA Measure § 1798.100(a)), sold (*id.* § 1798.101(a)), or disclosed for business reasons (*id.* § 1798.101(a)) by a covered business. Businesses must accommodate consumer requests for this information, regardless of whether the personal information was disclosed for direct marketing purposes or not. In addition, under the CRPA Measure, covered businesses must provide a means for consumers to opt out of the sale or disclosure of their personal information, regardless of the business reason for the sale or disclosure. *See id.* § 1798.102.

B. **Additional Website and Privacy Policy Disclosures.** As a result of CalOPPA and other sources of privacy regulation, businesses with a commercial online presence are expected to have already posted a privacy policy that describes the personal information the business collects, and the

categories of third parties with which personal information is shared. The CRPA Measure, however, adds to the list of specific items that a business must make available online, including but not limited to: (i) a requirement to post on the website homepage a link with the text "Do Not Sell My Personal Information;" (ii) a requirement to include text describing the consumer's opt-out rights; and (iii) three separate lists of personal information ((1) collected; (2) sold; and (3) disclosed) (unless there has been no sale or disclosure, in which case, that must also be stated).

C. **Non-Discrimination Based on Exercise of Privacy Rights.** Unlike the other California privacy laws currently in place, the CRPA Measure explicitly prohibits covered businesses from charging "opt out" consumers a different price for the same goods or services or providing such consumers with a different level of goods or services, as a result of their requesting information or exercising an opt-out right.

D. **Requirement to Maintain Reasonable Security Procedures and Practices.** Under current California law, a data breach is not a statutory violation subject to civil penalties (although security practices may be scrutinized under other laws, *e.g.*, as an unfair practice). The CRPA Measure makes a data breach a violation of state law, unless the covered business has "implement[ed] and maintain[ed] reasonable security procedures and practices, appropriate to the nature of the information, to protect [] personal information from unauthorized disclosure." *See* CRPA Measure § 1798.112.

Companies covered by the CRPA Measure must comply with these obligations with limited exception. Businesses may be exempt to the extent they are cooperating with law enforcement or altogether avoiding California jurisdiction in the process of collecting, selling, and/or disclosing consumer information. In addition, the CRPA Measure does not apply to information covered by HIPAA, or information sold to or from a consumer reporting agency if the information is to be reported in, or used to generate, a consumer report.

The CRPA Measure Includes Potentially Significant New Enforcement Provisions

The CRPA Measure establishes new mechanisms and rights to enforce the CRPA Measure, including a private right of action. Under the CRPA Measure, consumers who suffer a violation (such as having their personal information sold despite opting out or being the victim of a data breach at a covered business) may pursue civil statutory damages. The CRPA Measure sets statutory damages at US$1,000 or actual damages (whichever is greater) for each violation by a covered business. The statutory damages for knowing or willful violations increase to US$1,000 - US$3,000 or actual damages, whichever is greater, per violation. *Id.* § 1798.108.

In addition to the private right of action and enforcement by public entities (such as the California Attorney General or local prosecutors),[5] the CRPA Measure also permits whistleblowers to file a written request with the California Attorney General for the Attorney General to commence an action for civil penalties (up to US$7,500 per violation). If the Attorney General takes up the action, a whistleblower may receive 15% of the ultimate penalty (if any). If the Attorney General does not act within 90 days of the whistleblower's written request to commence the action, the whistleblower may prosecute the case and may receive 25-50% of the ultimate award. *Id.* § 1798.111.

Both the private right of action and whistleblower provision appear to create the possibility of significant civil liability risk for covered businesses with large stores of consumer data.

Final Considerations

It is too early to tell if the CRPA Measure will receive enough signatures to earn a vote in the 2018 California State elections. However, if the CRPA Measure is put to a vote, businesses operating in California would face significant risk. Notably, in mid-February 2018, a coalition of telecommunications and internet companies formed and funded a committee to oppose the CRPA Measure.

Affected businesses would likely incur immediate compliance costs in order to update website and privacy policy disclosures, and to develop and implement compliant opt-out mechanisms to conform to the technical specifications in the new law. Fortunately, the law provides a nine-month grace period, during which businesses will not be subject to the CRPA Measure's provisions regarding the collection or sale of personal information. Unfortunately, how certain provisions and terms would be interpreted (in particular the phrase "for valuable consideration" in the definition of sale and the non-discrimination provision) is unclear, and businesses will be required to apply their own best judgment in interpreting these words as they would work to meet the CRPA Measure's new standards.

At this early stage, "wait and see" may be the right approach. But if the CRPA Measure obtains enough signatures to earn a spot on the California ballot, businesses should begin preliminary assessments about what changes might be in order for them, should the CRPA Measure pass in November.

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:

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

Roxana Mondragón-Motta
roxana.mondragon@lw.com
+1.202.637.1066
Washington, D.C.

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

You Might Also Be Interested In

New DoD Cybersecurity Requirements Go Into Effect

Call for Cybersecurity Guidelines in International Arbitration

How Can Healthcare Organizations Prepare for the Next Cyberattack?

New Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

Endnotes

[1] "Devices" is undefined in the CRPA Measure.

[2] *Compare* CRPA Measure § 1798.106 (m), *with* Cal. Civ. Code § 1798.80 *et seq.*

[3] "De-identified" is defined as "information that cannot reasonably identify, relate to, describe, reference, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer or device…" CRPA Measure § 1798.106(h).

[4] "Commercial purposes" is defined as "to advance a person's commercial or economic interests, such as by inducting … or enabling or effecting, directly or indirectly, a commercial transaction." CRPA Measure § 1798.106(e).

[5] *See id.* § 1798.109.