BCLP. Client Intelligent

Insights

ENFORCEMENT IS COMING – ARE YOUR PRIVACY POLICY AND COOKIES SOLUTION READY?

Apr 11, 2023

On January 1, 2023, the California Privacy Rights Act of 2020, which amended the existing California Consumer Privacy Act (collectively, the "**CPRA**") and Virginia's Consumer Data Protection Act ("**VCDPA**") went into effect. Regulatory enforcement for the VCDPA began on January 1, 2023 and enforcement for the CPRA will begin July 1, 2023. In addition, the first round of CPRA regulations was finalized and effective on March 30, 2023. Privacy laws in Colorado, Utah, and Connecticut will also come into effect over the course of this year, and new laws, such as that in Iowa, will need to be considered.

New privacy laws often translate to new requirements for businesses. This is especially true for businesses that deploy targeted advertising or analytics tools to collect consumer information from websites and mobile apps. Given competing demands for internal resources, most companies are not in a position to engage in a full-scale compliance effort for each new or pending privacy law. Rather, most businesses will find that adopting a well-developed risk-based strategy is the more attainable and sustainable approach.

We generally recommend that the first step in this risk-based analysis focus on the public-facing features of the business – namely, any websites or mobile applications, particularly because recent enforcement has focused on the content of online privacy policies and the use of advertising cookies.

With this in mind, we have compiled a list of key compliance measures businesses should consider when evaluating their cookie practices and online privacy disclosures. While we have focused our brief guidance here on addressing the requirements under California and Virginia law, these steps will apply more broadly to the other state privacy laws not yet in force as there is a great deal of overlap in their requirements.

1. **Understand what laws apply.** While tempting from an efficiency standpoint to address all of the requirements under US privacy laws, in your business's privacy policy, taking the time to really understand what laws apply can reduce risk associated with over-promising, and the operational burden of complying with laws that may not apply. For example, rather than simply implementing a "Do Not Sell or Share Button," ask yourself whether your business meets the threshold

requirements under CPRA. Even if an organization ultimately decides to take a jurisdiction agnostic approach, it is important to make these decisions strategically, rather than just assuming all laws apply in all circumstances.

a. **CPRA:** If your business meets any of the following criteria, it is likely covered by the CPRA, unless an exception applies (e.g., the Health Insurance Portability and Accountability Act or Gramm Leach Bliley Act carve-outs):

   i. Your business has an annual gross revenue of $25 million or more;

   ii. Your business earns at least 50% of its annual revenue from selling or sharing personal information; or

   iii. Your business buys, sells or shares (in this context, engages in cross-contextual behavioral advertising) with third parties the personal information of at least 100,000 California residents.

b. **VCDPA:** The VCDPA applies to any business that operates in Virginia or targets Virginia consumers, and controls or processes the personal information of 100,000 Virginians (or only 25,000 if the business makes more than 50% of its revenue from the sale of personal information).

2. **Review and update your business's privacy and cookie policies to include mandatory content and meet related structural requirements. To do so, organizations should consider and address the following steps:**

   a. Confirm that your privacy policy is ***easy to read and navigate***. In particular:

      i. Confirm that the privacy policy includes a table of contents with hyperlinks to each section for easier navigation;

      ii. Use straightforward language and descriptions so the average user can understand what information about them is being gathered and how it is being used and disclosed; and

      iii. Confirm all internal hyperlinks work properly.

   b. Ensure the privacy policy provides clear disclosures of the following:

      i. Categories of personal information your business collects;

      ii. The purposes for which the categories of personal information is collected;

      iii. The sources from which personal information is collected;

      iv. The categories of third parties to whom the business discloses, sells, or shares, personal information;

v. Description of consumer right of access, deletion, correction, and portability under applicable law;

vi. If your business collects sensitive personal information, a description of how this information is collected, used and disclosed (additionally, in California a mechanism to opt out of certain uses of sensitive personal information may be required, depending on how the information is used);

vii. Length of time your business intends to retain personal information; and

viii. If applicable, the reason that information is sold or shared (CPRA requirement) or disclosed for targeted advertisement purposes (VCDPA requirement) and how consumers can opt out of a sell or share/ disclosure for targeted advertisements (or other disclosures that would constitute a sale under applicable definitions).

c. Tailor descriptions of targeted advertising cookies and use of related technologies (collectively "cookies") to describe how the cookies are used and with whom the information is shared.

d. If your business has California employees or applicants, make sure your business addresses the notification obligations for employees and applicants. You may wish to consider the use of separate policies to satisfy these notice obligations.

3. **Review your cookie strategy and determine whether and what types of cookies are used. Consider the following if your business uses cookies:**

a. Both the CPRA and the VCDPA require that consumers be provided a mechanism for managing their cookie preferences when certain types of cookies are used. Providing an opt-out mechanism requires both an understanding of the cookies deployed on your business's website, as well as whether they qualify as advertising cookies (i.e, whether their use is a "sale" and/or "share" under CPRA or "targeted advertising" under VDCPA). Moreover, blocking cookies is technically complicated and may require deploying a third party cookie manager.

b. **CPRA**

i. Understand whether your business uses cookies.

ii. Consider using a third party cookie manager that can operationalize the consumer's choice regarding advertising cookies across digital properties.

iii. If advertising cookies are used:
1. Provide a mechanism for allowing consumers to opt-out of advertising cookies. This mechanism can take different forms depending on the needs of the business. A "Do Not Sell or Share My Personal Information" button is likely required; and

2. Ensure that your website honors the Global Privacy Control Signal (GPC) sent by a consumer through browser settings or an extension notifying the website of the user's privacy preferences. Most third party cookie managers claim to allow businesses to automatically detect and honor GPC signals.

c. **VCDPA**

i. If your business only has to comply with the VCDPA, provide Virginia residents with an opt-out mechanism for cookies. This can be in the form of a simple opt- out button, which will also have to be operationalized by a cookie manager. If CPRA and VCDPA both apply (and potentially other state laws, as they come into force), it will be important to determine how to conform the approach and make sure any options meet the obligations of all applicable laws.

d. Ensure that all the language in the cookie manager pop-up window is compliant with the CPRA and VCDPA (i.e., provides direct straightforward choices to accept or reject cookies rather than language that pushes consumers to accept and could be construed as a dark pattern).

4. **Make sure that your business honors the statements made in its privacy policy. For example:**

a. Ensure that the choices made by website visitors are honored across all the pages on your website, such as when a website visitor opts-out of cookies or clicks the "Do Not Sell or Share My Personal Information" button.

b. Honor the consumer rights outlined in your privacy policy if the consumer requests such consumer rights.

c. Ensure that descriptions about disclosures to third parties remain accurate.

d. Ensure that none of the options made available to consumers could be considered "dark patterns" under applicable law (i.e., as noted above, include language or other factors that push consumers to the desired result).

As privacy regulations proliferate, businesses will need to continue to monitor the various legal requirements and to meaningfully prepare for inevitable enforcement from state regulators. The steps described above are critical first steps in this process and in helping organizations achieve their privacy compliance goals.

RELATED CAPABILITIES

- Data Privacy & Security
- Retail & Consumer Products

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Andrea Rastelli

Boulder

andrea.rastelli@bclplaw.com
+1 303 417 8564
