CCPA Enforcement Area No. 1

The Infamous "Do-Not-Sell" Button

It should come as no surprise that the absence of a “Do Not Sell My Personal Information” button on a website may attract unwanted attention from the California Office of the Attorney General (OAG). This requirement, imposed on businesses that “sell” personal information, has generated much press, as well as concerns about a company’s ability to automate, track, and ultimately prove compliance with do-not-sell requirements.

Because the CCPA requires businesses who sell personal information to post a “clear and conspicuous link” on the business’s internet homepage titled, “Do Not Sell My Personal Information,” the absence of such a link will likely be the low-hanging fruit for the OAG when it comes to selecting initial enforcement targets.

Troutman Pepper tips

- If a business has taken the position that it does not “sell” personal information, then its actions and statements should communicate that same message. This requires businesses to not only consider those disclosures mandated by the CCPA (e.g., the CCPA Privacy Notice and Notice at Collection), but also any documentation that describes the business’ privacy practices. For these businesses, it is also critical to have in place controls to assure that that data usage practices of the business align with the disclosures provided to consumers. For many companies, it would not be surprising to learn that the functionality of the product got ahead of the statements made in the privacy policy and other consumer-facing documents. Privacy by design and coordination between the business and regulatory compliance remains critical.

- For businesses that do sell personal information:

  Confirm that you have included a link titled “Do Not Sell My Personal Information” on the introductory page of your internet website and on any internet webpage that may be collecting personal information. For businesses seeking to comply with the proposed regulations, the link may also be titled “Do Not Sell My Info.”

  Review whether your link is “clear and conscious.” For a discussion as to what constitutes “clear and conspicuous,” consider referring back to the OAG’s guidance on developing a meaningful privacy policy, “Making Your Privacy Practices Public,” available here.

  If your business offers a mobile application, consider whether consumers can access the “Do Not Sell” link through the application’s download page or within the mobile application itself.

  Confirm that consumers are not required to create an account in order to direct the business not to sell the consumer’s personal information.

  Review the functionality of the “Do Not Sell” link and confirm that clicking it enables the consumer to opt out of the sale of the consumer’s personal information. For businesses seeking to comply with the proposed regulations, there may be additional requirements to consider. For example, the proposed regulations introduce the concept of a “Notice of Right to Opt Out,” which does not exist under the statute. The proposed regulations impose certain content requirements for the Notice of Right to Opt Out and also specify that consumers should be directed to the notice after clicking the “Do Not Sell” link.

  In addition to the “Do Not Sell” link, confirm that the business is offering one additional method for consumers to exercise the right to opt out (e.g., telephone number, email address, postal address, etc.).

  Verify that there are processes and procedures in place to timely honor requests once they have been submitted. Although the proposed regulations suggest that a response is timely if complied with within 15 business day of receipt, the statute appears to be silent on this issue.

Consider how the use of online tracking technologies impacts your position on whether you sell personal information and whether there are processes in place to flow down opt out requests to such technology vendors. The OAG has stated that whether the use of website cookies to collect information that is shared with third parties is a "sale" is a fact specific determination that requires a business to determine whether a cookie can be linked to a consumer or household, over time and across services, and whether a third party advertising services vendor is prohibited from using the information for purposes other than providing services to the business.

If your organization has determined that it's use of third-party cookies results in a "sale" of personal information, consider whether the consumer needs to take additional steps (e.g., providing functionality to disable third-party cookies for each browser and device that the consumer uses in connection with the company's websites) in order for their opt out request to be effective.

CCPA: The Enforcement Series

Enforcement of the California Consumer Privacy Act ("CCPA") began July 1, 2020. Our privacy team at Troutman Pepper includes several attorneys who worked in an attorneys general office. This privacy regulatory team has identified six areas of enforcement likely to catch the California Office of the Attorney General's (OAG) attention, which arguably holds sole regulatory enforcement authority under the Act. This six-part series will focus on those areas of the law. Building on the experience of advising clients on the CCPA since its passage, our privacy compliance team will then discuss discrete strategies to minimize enforcement risk and bolster compliance efforts.

Key Enforcement Issues to Note:

- *Prior to initiating an enforcement action for an alleged violation of the CCPA, the OAG must provide businesses with a notice of alleged noncompliance and a 30-day opportunity to cure ("Notice and Cure Letter").*
- *As of July 1, 2020, certain businesses have received Notice and Cure Letters. Given the 30-day window to cure, it is likely that nothing will be made public about these early enforcement targets until August 1st (i.e., once the cure period elapses), at the earliest.*
- *The OAG may be selecting early targets for enforcement actions in various ways including, for example, based on consumer complaints submitted directly to the OAG or those made public on social media platforms (e.g., Twitter), or simply by scanning business' websites for noncompliance.*
- *Because the proposed regulations implementing the CCPA have not been finalized, the OAG can only bring an action based on an alleged violation of the CCPA (i.e., the statute) or a data breach, which went into effect January 1, 2020. It would not be surprising to see, however, the OAG argue a violation of the CCPA and seek remedial measures based on its interpretation as stated in the draft regulations. For additional information on the status of the proposed regulations, click **here**.*
- *If a company receives a Notice and Cure Letter from the OAG, we advise seeking legal counsel on how to respond to the OAG's request in a manner that minimizes business disruption but demonstrates a willingness to comply. Early and frequent communication and transparency will be key.*

Contacts

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

Ashley Taylor, Jr.
Partner
804.697.1286
ashley.taylor@
troutman.com

Sharon Klein
Partner
949.567.3506
sharon.klein@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

Oscar Figueroa
Associate
949.622.2743
oscar.figueroa@
troutman.com

Lauren Geiser
Associate
804.697.1379
lauren.geiser@
troutman.com