

CCPA Enforcement Area No. 4

Businesses Collecting Children's Personal Information and Health-Related Data

The CCPA Will Not Sleep During COVID-19

Organizations who, just months ago, believed they were not collecting health-related data, or children's personal information, may now have to revisit those beliefs in light of the COVID-19 pandemic. Children are spending more time online, and businesses are collecting even more data from Californians in an effort to take precautions against the virus. Despite the concerns and fear COVID-19 has generated, businesses are still required to comply with the California Consumer Privacy Act ("CCPA"). In fact, California Attorney General Xavier Becerra has [rebuffed](#) any ideas that the CCPA should be delayed due to COVID-19.

Children's Personal Information

For businesses collecting personal information of minors under the age of 16, the CCPA extends several rights to minors by requiring businesses to obtain opt-in consent prior to the sale of a child's personal information, and by imposing an "actual knowledge" requirement on businesses who fail to comply with the consent provision. The CCPA provides the California Attorney General ("OAG") with a new enforcement tool, and it appears the OAG will follow the growing national trend of focusing on children's privacy, as evidenced by other enforcement actions brought by other states and the [federal](#) government. For example, the Federal Trade Commission ("FTC") and the U.S. Justice Department are [looking](#) into allegations that a popular application among minors, TikTok, has failed to protect children's privacy. The state of Washington also recently [settled](#) an investigation against a California-based technology company concerning children's privacy.

The FTC is also [considering](#) an update to the Children's Online Privacy Protection Act ("COPPA"). A coalition of 25 state attorneys general [urged](#) the FTC to update COPPA regulations, with Oregon Attorney General Ellen Rosenblum [submitting](#) her own call.

The OAG will continue, and now sharpen, its focus on this national trend. It appears the OAG will be an attentive watchdog in this space, as AG Becerra has previously [expressed](#) that enforcement will be "aggressive, early, [and] decisive."

Health Information

For organizations collecting health information, the CCPA's applicability is a bit more complicated because the CCPA provides an exemption for organizations collecting personal information that is otherwise covered by other regulations, such as the federal Health Insurance Portability and Accountability Act ("HIPAA"). This does not, however, mean that organizations should ignore the CCPA. Organizations will still be tasked with determining whether their data practices should be handled in accordance with HIPAA, the CCPA, or other privacy regulations.

Troutman Pepper tips

Organizations Need to Understand and Be Able to Distinguish Their Existing Obligations

- Before businesses seek to comply with specific regulations, such as the CCPA, they need first to identify how their data collection practices operate and how those practices may implicate other regulatory obligations. In the second part of our [CCPA Enforcement Series](#), we [discussed](#) the importance of performing an inventory on data collected by businesses, such as through data mapping. Identifying how a business collects and handles different types of personal information is a crucial preliminary step for businesses seeking to acquire a solid understanding of the kind of data it is handling, and how its handling may implicate the CCPA and other regulations.

Organizations Should Identify Their Existing Data-Handling Procedures

- Many businesses with years of experience handling either children’s information or health-related information may not need to drastically implement new systems to comply with the CCPA. However, businesses will not be able to make that determination without taking a close look at their existing procedures for handling this type of data.
- Take for example, how businesses operating primarily online and currently complying with the federal COPPA may only need to expand existing procedures by making a few tweaks to comply with the CCPA’s additional requirements. Other businesses collecting children’s information “offline,” however, may face a bigger task in implementing specific data-handling procedures to comply with the CCPA’s requirements.

Tips for Organizations Collecting Personal Information from Children

- Businesses should determine if they “sell” personal information of minors. For online content providers that utilize third-party digital advertising service providers, collection and disclosure of information to those third-party digital advertising service providers could be a sale under the CCPA.
- Businesses that desire to sell the personal information of minors under the age of 13 should develop a process for legal guardians to opt-in to such sales. The CCPA’s regulations describe that a business who has “actual knowledge that it sells the personal information of children under age 13” shall develop procedures for affirmative authorization of the sale of personal information, and that the authorization is provided affirmatively by a legal guardian. Businesses, therefore, are required to obtain opt-in consent for the sale of a minor’s personal information under the CCPA. Businesses collecting information of minors under the age of 13 online should evaluate their process for obtaining verifiable parental consent for such collection and supplement as needed to obtain any requisite consents for sale. For businesses interested in learning more about whether they “sell” personal information under the CCPA, consider reading our [first alert](#) in this series.
- Businesses that desire to sell the personal information of minors between the ages of 13 and 16 will need to develop a process to allow those minors to opt-in to the sale. Businesses should be especially mindful of their data collection practices online if the business has knowledge that minors between the ages of 13 and 16 use the business’s online service. Use of cookies and other automatic data collection tools to share data with third parties could inadvertently result in a sale of personal information by the business under the CCPA that could require the implementation of procedures to differentiate between minor and non-minor users.

Tips for Organizations Collecting Health-Related Data

- Develop systems for distinguishing between health-related information subject to the CCPA and “medical information” exempted by the CCPA. The CCPA exempts certain “medical information” when other laws, such as HIPAA, already govern that information. The CCPA’s exemption, however, requires businesses first to determine whether the health-related information it collects falls within the scope of another regulation. The HIPAA exemption for the CCPA does not fully protect healthcare institutions or their service providers if the patient data is not Protected Health Information (“PHI”) under HIPAA. PHI means all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. 45 C.F.R. § 160.103. For example, a hospital maintaining information about its employees is not PHI and is governed by other consumer protection statutes such as the CCPA. Also, health data provided by a patient wellness application may not be subject to HIPAA and thus regulated by the CCPA. Thus, businesses should create systems for distinguishing between the different types of health-related information it collects from consumers, as well as the statutes and regulatory schemes governing that information.

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



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



Sharon Klein
Partner
949.567.3506
sharon.klein@troutman.com



Ron Raether
Partner
949.622.2722
ron.raether@troutman.com



Alex Nisenbaum
Partner
949.567.3511
alex.nisenbaum@troutman.com



Lauren Geiser
Associate
804.697.1379
lauren.geiser@troutman.com



Edgar Vargas
Attorney
949.622.2473
edgar.vargas@troutman.com