CCPA Enforcement Area No. 2:

Treating the CCPA Like a Check-the-Box Exercise

AG Enforcement Risk: Take it Seriously

Conspicuously posting a privacy policy that complies with the requirements of the California Consumer Privacy Act ("CCPA") is perhaps the most obvious outward sign of a business's compliance with the CCPA. A company with a privacy policy that fails to track the requirements of the CCPA will present a red flag to the California Attorney General ("OAG") that the company is otherwise not meeting the requirements of the CCPA. Such privacy policy deficiencies will make the company a prime target for a civil investigative demand and possibly an enforcement action.

Companies need to avoid simply treating CCPA compliance like a simple check-the-box exercise in updating an existing privacy policy or posting a new CCPA-specific privacy policy. In addition to developing meaningful disclosures that are CCPA compliant, companies must follow through on complying with these policies and other CCPA requirements.

The risk of such noncompliance is steep, as AG Xavier Becerra has stated that his office fully plans to "descend on" and "make example[s]" of companies that are not operating properly under the CCPA. Accordingly, companies should make every effort to keep in step with the CCPA's requirements and should assume that anything short of that may lead to a dreaded "notice and cure" letter from the AG. If not handled properly, such a letter could lead to a civil investigative demand, investigation, formal enforcement proceeding, and/or steep penalties for violations.

Troutman Pepper tips

Inventory Data Collected by the Business

- The final text of the proposed regulations implementing the CCPA ("Proposed Regulations") require that privacy policies provide consumers with a "meaningful understanding" of a business's data collection and sharing practices. Thus, while the CCPA allows certain disclosures to be made in terms of "categories," businesses should give careful thought to what level of detail should be included. This is true especially in connection with personal information that business may collect passively and that consumers may not be aware of, unless adequately disclosed in the privacy notice. As a starting point, conducting a thorough data mapping exercise to understand the lifecycle of personal information collected will be key to providing adequate disclosures.
- Effective data inventory is also key to understand in what systems and formats the personal information is stored some of which may be in the hands of third parties such as cloud vendors. This allows a business to identify the specific technical and organizational challenges to data retrieval and deletion faced by the business and delegate clear responsibilities to internal departments with accountability for action plans relating to verifiable consumer requests, which is critical for a business to respond to such requests within the requisite time frames.
- Data mapping will also help the business understand each collection point and comply with CCPA requirements to provide appropriate notices at or before the point of collection, which we will detail further in the fifth installment of our CCPA enforcement series.

Privacy Policies

- The CCPA requires businesses to identify the categories of personal information disclosed for a business purpose or sold within the previous 12 months. The Proposed Regulations further require that "for each category of personal information identified, provide the categories of third parties to whom the information was disclosed or sold." While what qualifies as a "sale" remains unclear, disclosure for a "business purpose" would generally include disclosures to third-party service providers who process personal information on behalf of the business. Failing to note these details in your privacy policy could generate unwanted attention even if you are otherwise in compliance with the CCPA.

- For businesses that do sell personal information, ensure that the business's privacy policy and website include required disclosures, as well as links to web forms and other opt-out request submission methods that provide consumers with the ability to opt-out of the sale of personal information. For more information on CCPA requirements related to the sale of personal information, including providing a "Do-Not-Sell" button on websites, see the first installment of our CCPA enforcement series.

- In addition to adhering to the requirements of the Proposed Regulations, when developing CCPA privacy policy disclosures businesses may consider referencing the recommended practices and principles in the OAG's guidance on developing a meaningful privacy policy, "Making Your Privacy Practices Public."

Additional Operational Compliance Tips

- Assess the security of the personal information used by the business and ensure that appropriate information security controls are implemented and documented. The CCPA allows consumers to bring individual and class action lawsuits following breaches of certain types of personal information that are caused by a business's failure to use reasonable security procedures and practices to protect that personal information. While California law does not detail what constitutes "reasonable" security, the OAG provided guidance on this issue in its 2016 Data Breach Report. In that report the OAG cited the 20 controls defined by the Center for Internet Security's Critical Security Controls as the "minimum level of information security" that all businesses should meet and also recommend use of multi-factor authentication and encryption of personal information on laptops and other portable devices. The controls required by many information security standards such as NIST 800-53, the NIST Core Framework and ISO 27002 can be mapped to the CIS Critical Security Controls and so effective implementation and documentation of compliance with such information security standards up front can pay dividends to mitigate risk downstream in the event of a security incident. What is "reasonable" security should also be viewed in light of what the OAG has required of businesses in settlement terms for previous OAG enforcement actions.

- Given the limitations imposed on "service providers" under the CCPA, implementing vendor management policies and procedures will be key to ensure your disclosures accurately represent your practices. Additionally, to help mitigate the risk of liability from data breaches, businesses should have in place clear and consistent policies and procedures to diligence service provider information security controls, conduct periodic (at least annual) reviews of such controls and put in place and enforce appropriate contractual restrictions, including with respect to use of personal information collected or received on behalf of the business. We will focus on areas of potential OAG enforcement and best practices with respect to the use of service providers in next week's installment of our CCPA enforcement series.

- Provide CCPA training to appropriate employees and document attendance. The Proposed Regulations submitted by the OAG require businesses to "establish, document, and comply" with a training policy for individuals that are responsible for handling consumer requests and those responsible for the business's compliance with the CCPA. This requires businesses not only to develop policies, but also to create or obtain appropriate training programs and materials and document attendance through the use of training logs or other appropriate tools. Such training should be part of onboarding employees and required at least annually.

- Maintain records of consumer requests for at least 24 months. The OAG's Proposed Regulations require these records be maintained and include certain specified details. Accordingly, any request for documentation received by a business from the OAG relating to CCPA compliance is likely to include a request for such documentation.

- Establish and document the plan for verifying consumer requests and include a general description of it in your CCPA Privacy Policy. Verification of the identity of consumers can be particularly challenging and it may be difficult to create clear rules for all potential request scenarios. However, creating reasonable, documented rules of the road for identity verification in accordance with the requirements of the OAG Proposed Regulations is an area that could come under scrutiny in an OAG enforcement action, especially if prompted by a consumer complaint related to consumer request response and verification.
- Make the privacy policy and other notices provided under the CCPA reasonably accessible to consumers with disabilities. The OAG's Proposed Regulations require, for example, that online notices must follow generally recognized industry standards such as the Web Content Accessibility Guidelines, version 2.1 which require online content to be perceivable, operable, understandable and robust. Simply posting an otherwise compliant CCPA privacy policy that is not usable by screen reading programs or other accessibility technologies is unlikely to meet this requirement. In addition to these deficiencies being readily apparent to the OAG, the accessibility requirement adds fuel to the active area of web accessibility litigation in California that we have covered previously here and here.

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

Wynter Deagle
Partner
858.509.6073
wynter.deagle@troutman.com

Alex Nisenbaum
Partner
949.567.3511
alex.nisenbaum@troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@troutman.com

Lauren Geiser
Associate
804.697.1379
lauren.geiser@troutman.com