troutman pepper

California Consumer Privacy Act Enforcement Series

August 2020

troutman.com

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 Ofl ce 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:

  Conflrm 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 conspicuous.” 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 oflers 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.

  Conflrm 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 conflrm 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, conflrm that the business is oflering 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 eIective.

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 off ce. This privacy regulatory team has identiffed six areas of enforcement likely to catch the California Off ce 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 ffnalized, 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.flgueroa@
troutman.com

Lauren Geiser
Associate
804.697.1379
lauren.geiser@
troutman.com

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 ffag to the California Attorney General ("OAG") that the company is otherwise not meeting the requirements of the CCPA. Such privacy policy deffciencies 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-speciffc 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 off ce 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 ffnal 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 speciffc 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 veriffable 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 fffth 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 identiffed, provide the categories of third parties to whom the information was disclosed or sold." While what qualiffes 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 ffrst 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 deffned 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 speciffed 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. Veriffcation of the identity of consumers can be particularly challenging and it may be diff cult to create clear rules for all potential request scenarios. However, creating reasonable, documented rules of the road for identity veriffcation 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 veriffcation.
- 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 deffciencies 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 off ce. This privacy regulatory team has identiffed six areas of enforcement likely to catch the California Off ce 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 ffnalized, 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

CCPA Enforcement Area No. 3

Service Providers

Organizations that qualify as a "service provider" under the CCPA breathed a sigh of relief when realizing that most obligations imposed by the CCPA apply directly to "businesses." This includes, for example, providing the required notices (*i.e.*, Notice at Collection, Privacy Notice, Notice of Right to Opt Out, and Notice of Financial Incentive), implementing the "Do Not Sell" link, and ofiering methods for consumers to submit access, deletion, and opt-out requests. Of course, this does not mean the CCPA's sweeping compliance obligations left service providers free from regulation.

To qualify as service providers, organizations must agree in the data sharing contract to process personal information on behalf of covered businesses solely for the purpose outlined in the contract and further agree not to retain, use, or disclose the personal information for any other purpose. Service providers also likely agree to many compliance processes to assist such businesses with meeting their obligations under the law. From a practical perspective, this means that while service providers may not have visible fiags of CCPA-compliance on their websites or external-facing materials, compliance exists behind-the-scenes and should be appropriately documented through updated contractual provisions and robust policies and procedures. This is particularly important given that it would not be surprising to see OAG send "notice and cure" letters to organizations that *appear* to have ignored the requirements of the law, even though such organizations are acting as service providers and thus exempt from many of the CCPA's requirements.

In light of restrictions included in the data sharing contracts, service providers should routinely assess their operations to ensure that they do not behave in a manner or use downstream customer data (sent by "businesses" under the CCPA) in a manner that is in contravention of their service provider role. Indeed, any investigation of, or enforcement action against, a "business" could implicate service providers who have downstream access to customer data—especially where data use is not limited to a "specific purpose." To avoid the risk of the OAG suspecting unfair and deceptive trade practices by organizations falsely claiming to be service providers or improperly disclosing data practices, service providers should be prepared to explain why they have customer data and why their use of that data is proper.

Troutman Pepper tips

- **Review Vendor Contracts**

  To qualify as service providers, organizations must update their vendor contracts to include the conditions and limitations imposed by the CCPA. This includes, for example, identifying the nature and purpose of processing personal information on behalf of the business and prohibiting the service provider from retaining, using or disclosing the personal information for any purpose other than the specified purpose.[1] As with most of the CCPA's requirements, there are certain exceptions to the processing restrictions. For example, § 999.314 of the final text of the proposed regulations provides that service providers may use personal information "to detect data security incidents, or protect against fraudulent or illegal activity" or for "internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source." Despite the fact the CCPA allows for this type of processing by a service provider, it should still be expressly called out in the vendor contract. Failure to do so may limit the service provider in how it can use the personal information despite the allowance afiorded by the CCPA. Service providers also need to ensure that a strong contract management system has been implemented. Because service providers likely "service" more than just one customer, keeping track of the various (and perhaps confiicting) purposes permitted by the data sharing agreements will be critical.

[1] For additional information about updating vendor contracts in light of the CCPA, see our *Law360* article titled, *California Privacy Law Means New Approach to Vendor Contracts*, available here.

- **Be Prepared to Explain Your Organization's Position**

  If a service provider receives a “notice and cure” letter from the OAG, the service provider should be prepared to explain how it reached the conclusion that it qualifies as a service provider under the CCPA and to provide documentation supporting its analysis. While the definition of “service provider” is somewhat circular, questions to consider include whether the entity is collecting or “processing” personal information on behalf of covered businesses for a specified “business purpose,” and whether the entity is restricted by contract from retaining, using, or disclose the personal information for any other purpose. Failing to adequately explain how the organization reached the conclusion that it qualified as a service provider could result in the OAG taking further action.

- **Ensure Proper Segmentation of Data**

  An organization contending it is a service provider must also be able properly segment the data it processes on behalf of covered businesses and implement the needed controls to avoid inadvertent violations of vendor contracts. This is especially critical for service providers who may be processing personal information for different purposes depending on the customer. Indeed, simply stating that personal information will not be used for any purpose other than that specified in the applicable vendor contract is likely insufficient. In addition, it would not be surprising for the OAG to “look under the hood” in the course of an investigation into either the service provider or a business it services, to confirm that the restrictions imposed by the vendor contract (and required by the CCPA to qualify as a service provider) are actually being complied with.

- **Review Marketing Materials and Privacy Disclosures**

  Service providers should review existing marketing materials and privacy disclosures to ensure that their position as a service provider is not being undercut by communications otherwise made by the company. For example, statements suggesting that the organization complies with the CCPA as a covered “business” (e.g., offering California consumers methods to submit CCPA requests) may raise confusion as to what role the entity has assumed. Though not required by the CCPA, service providers may consider including statements in privacy notices clarifying their position as a service provider, which may demonstrate the company’s limited role to consumers and OAG.

- **Responding to Consumer Requests**

  As a service provider, has your organization agreed to respond directly to consumer requests on behalf of the businesses you serve? If so, be careful. Your response to the consumer should continue to distinguish your organization as the service provider, as opposed to the covered business. Any confusion as to which role you have assumed may trigger follow up from OAG.

- **Wearing Multiple Hats**

  Proper data classification and mapping will be essential to determine an entity’s role under the CCPA, especially where an organization may be acting as a service provider on the one hand and a covered business on the other. Organizations will want to ensure they are properly classifying and mapping information to track when data is limited in use as a service provider or subject to the obligations imposed on a covered business. Without proper classification and mapping, the organization may be forced to apply the most restrictive rules across all data collected to comply with the CCPA (*i.e.*, treat the personal information if the service provider were actually a covered business). This would likely create additional compliance burdens and could also result in tension between the service provider and the business it is processing information on behalf of. Similar to the above, wearing multiple hats may also warrant adding language to public statements clarifying the organization’s position under the CCPA depending on the circumstance. For example, if an organization is acting as a covered “business” when collecting information directly from consumers but a “service provider” when collecting information from a third party, the company’s public statements may want to make that apparent. This may be accomplished, for example, by indicating that the role the organization assumes depends on the context of collection or the organization’s relationship with the consumer and then elaborating from there.

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 off ce. This privacy regulatory team has identiffed six areas of enforcement likely to catch the California Off ce 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 ffnalized, 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

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

Lauren Geiser
Associate
804.697.1379
lauren.geiser@
troutman.com

Anne-Marie Dao
Associate
858.509.6057
anne-marie.dao@
troutman.com

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 rebufied 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 off ce. This privacy regulatory team has identiffed six areas of enforcement likely to catch the California Off ce 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 ffnalized, 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

CCPA Enforcement Area No. 5

Failing to Provide Adequate Notice at Collection

The California Consumer Privacy Act's ("CCPA") notice at collection ("NAC") obligation requires certain regulated businesses to provide consumers with a privacy notice outlining what personal information they collect and how such information is used "at or before the point of collection." Failing to provide adequate notice at collection, both in terms of content and delivery, may attract the attention of the California Attorney General ("OAG"). As previous enforcement actions have shown, regulators go after businesses that do not effectively disclose how they use personal information. *See, e.g.*, our article on the recent $5 billion FTC-Facebook settlement based, in part, on allegations that Facebook engaged in a deceptive practice when it collected users' phone number to enable two-factor authentication without disclosing that Facebook would also use those numbers also for advertising purposes, available here.

Inconsistencies among privacy notices and other disclosures may also raise red flags. Proper CCPA compliance requires businesses to not only consider those disclosures mandated by the CCPA (*e.g.*, the NAC), but also any documentation that describe the business' privacy practices. In addition to enforcement and/or investigation concerns, privacy-based class action lawsuits are littered with allegations that businesses failed to accurately disclose the extent of their data collection and sharing practices (consider the *In re: Facebook Inc. Internet Tracking Litigation*, which we reviewed in our article, "Calif. Privacy Law Takeaways from 9th Circ. Facebook Case, available here). Drafting accurate privacy disclosures and implementing "just-in-time" notices (such as the NAC) will be the best way to defeat privacy-based claims and investigations and managing consumers' expectation of privacy from the onset.

Given that the NAC must be provided "at or before the point of collection," businesses must also carefully consider the placement of such notices. This is especially important for businesses that collect personal information at brick and mortar locations as NAC requirements apply in the offline context as well. Even for businesses that collect personal information exclusively online, the final text of the proposed regulations implementing the CCPA ("Proposed Regulations") will require businesses to evaluate whether passive posting of a privacy notice is sufficient to meet the "timely notice" requirements.

Troutman Pepper tips

- **It Still Starts with Data Mapping**

  Evaluate all points of collection within the business to ensure an appropriate notice is being provided at each point. As we detailed in the second installment of our CCPA enforcement series, data mapping will be critical for this and other areas of CCPA compliance. For collection online or through a mobile app, a conspicuous link to a CCPA compliant privacy policy in accordance with the requirements of the Proposed Regulations will likely suffice. When developing mobile apps, instituting privacy by design principles to ensure delivery of proper notice could help avoid regulatory scrutiny and costly implementation of new in-app workflows.

- **Review Offline Methods of Collection**

  Businesses must take into account how a consumer interacts with the business at the point information is collected when providing the notice. For example, in a retail setting, collection may occur at the register, and prominent signage at the register or at the door of the retail establishment directing the consumer to a website where an appropriate notice can be found may be sufficient. When collecting personal information using physical paper forms, business may choose to present the requisite notice or link on the form itself. Businesses should consider whether tools such as QR codes can make it easier for consumers to follow the physical notice to any online notice it may reference. Over the phone, reviewing call center scripts to ensure representatives are providing consumers with notice or directions on where to obtain the notice online may be needed.

- **Anticipate Reasonably Foreseeable Collection Practices**

  The proposed regulations prohibit businesses from collecting categories of personal information other than the categories the business lists in the NAC. Businesses should make sure that the NAC contemplates all categories that may be required from an operational perspective currently and in the future to avoid compliance obstacles that could have otherwise been avoided.

- **Pay Attention to Explicit Consent Requirements**

  Create internal policies and procedures to ensure any proposed new uses of personal information held by the business, including any efforts to monetize data assets, are vetted by personnel responsible for privacy compliance. These processes should include reviewing proposed new uses of personal information against the historical privacy policies and statements, including all NACs. It is important that a business keeps track of when changes to privacy notices were implemented so it can ascertain the exact terms a user may have viewed at a particular time. Consistent with prior Federal Trade Commission guidance, the Proposed Regulations prohibit businesses from using personal information for a purpose materially different than those disclosed in the NAC without notifying the consumer and obtaining explicit consent. As we previous discussed here, the explicit consent requirements will continue to incentivize businesses to adopt broad notices that list all possible uses of personal information, regardless of whether such use is ever put into practice. For businesses that narrowly tailor their privacy notices, however, careful consideration must be given to the explicit consent requirements. When obtaining explicit consent is not practicable, alternative processes should be considered to allow the business to keep moving forward (e.g., segmenting databases, wiping data and starting over, and the like).

- **Employment-Related Information is Not Exempt from NAC Requirements**

  Personal information collected in the employment context is excluded from the scope of the CCPA, except with respect to the notice at or before collection requirements and the private right of action relating to data breaches. Practically, this requires every business with California employees to carefully consider whether, when and how best to provide the notice. Many businesses with California employees, independent contractors, and applicants provide for such notice of what is collected, the categories of information collected and the purpose for collection in an employee handbook or intranet portal. For in-person collection, consider providing the notice in paper form and documenting the fact that is has been provided. If collecting specific employee information by other means (*e.g.*, online or by phone) which was not disclosed previously, the minimum should be an email notice with a "read receipt" requested and logged.

- **Leverage the Exemptions**

  Businesses that do not collect personal information directly from consumers do not need to provide the notice at collection *if* they do not "sell" personal information. If the business sells personal information of consumers with whom it does not have a direct relationship, the business would likely qualify as a "data broker" under applicable California data broker registration law. Notably, data brokers are exempt from providing notice at collection to consumers *if* they have included in their data broker registration submissions a link to their online privacy policies that include instructions on how consumers can submit a request to opt out.

- **Make the NAC Reasonably Accessible to Consumers with Disabilities**

  The OAG's Proposed Regulations require that online NACs 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. For more information about CCPA requirements relating to accessibility standards and web accessibility litigation in California, see the second installment of our CCPA enforcement series and our previous coverage of such litigation here.

- **Don't Forget the DNS Link**

  To the extent a business sells PI, include in the NAC a link to or, for offiine notices, the website where the business's "Do Not Sell My Personal Information" link is provided. For more information with respect to the Do Not Sell My PI Requirement, refer to the first installment of our CCPA enforcement series.

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 off ce. This privacy regulatory team has identiffed six areas of enforcement likely to catch the California Off ce 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 ffnalized, 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

Alex Nisenbaum
Partner
949.567.3511
alex.nisenbaum@
troutman.com

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

Brett Dorman
Associate
949.567.3541
brett.dorman@
troutman.com

CCPA Enforcement Area No. 6

California Privacy Rights Act (CCPA 2.0)

CCPA 2.0: A Refresher

Just as the dust from the CCPA began to settle, on June 24, 2020, the California Secretary of State released a memorandum (available here) stating that the California Privacy Rights Act (the "CPRA"), also known as the CCPA 2.0, passed the threshold of signatures to be on the November ballot for California's General Election. The CPRA, which was introduced by Californians for Consumer Privacy, the group behind the CCPA, would expand upon the CCPA's consumer privacy rights and move California privacy law closer in the direction of the EU General Data Protection Regulation ("GDPR").

If the CPRA passes, it will go into efiect January 1, 2023 and create new privacy rights in connection with certain types of information. Such rights may include, for example, a right to correct inaccurate personal information and a new right for consumers to opt out of the use or disclosure of "sensitive personal information" for advertising and marketing purposes. The law would also establish a "California Privacy Protection Agency" to enforce the CPRA.

The new obligations and requirements imposed by the CPRA will also likely require additional rulemaking from the California Ofi ce of the Attorney General ("OAG"). As demonstrated by the CCPA rulemaking process, this is certainly no easy task. As we previously reported here, the final proposed regulations implementing the CCPA have not even been approved yet, leaving many businesses and industry groups wondering how the OAG may react to the CCPA 2.0 referendum.

What to Expect from the OAG

It is no mystery that Attorney General Becerra aggressively supports the implementation and enforcement of CCPA 1.0. He has long demonstrated his commitment to having California "lead the way [in] putting people first in the Age of the Internet." AG Becerra himself announced the title and summary of CCPA 2.0, and—if the referendum is successful—entities should expect him to pursue its implementation and enforcement with the same gusto he has demonstrated for its original counterpart.

It is daunting to consider CCPA 2.0 while CCPA 1.0's dawn over California is just beginning. However, CCPA 2.0's looming presence should not be a cause for panic:

- First, the OAG has its hands full navigating the very new landscape of CCPA 1.0 which is in efiect. The Ofi ce will need to strategize and reallocate its efiorts to undertake CCPA 2.0 which is years down the road. If CCPA 2.0 is successful, the OAG will likely handle the implementation process carefully in an efiort not to make mistakes or sufier from any oversights.
- Second, the OAG knows it cannot force compliance or threaten enforcement overnight. Just as it gave covered entities time to prepare for CCPA 1.0, similar time will be required for CCPA 2.0. The OAG has no interest in watching covered entities struggle to draft and implement rushed and haphazard compliance policies and procedures.
- Third, if the referendum is successful, it will require immense legislative and budgetary efiorts to get ofi the ground. While it is currently set to go into efiect in 2023, that date is not set in stone and may be delayed. Some pundits believe this long timeframe may allow for national privacy legislation-an assumption made more likely if Kamala Harris, former California Attorney General and champion of privacy rights, is elected as Vice President.

Troutman Pepper tips

- **Don't Get Distracted from CCPA 1.0:** Keep a good thing going. Entities have worked very hard to achieve and maintain compliance with CCPA 1.0—this requirement is not going to change or go away. CCPA 2.0 has not even passed the referendum stage yet, so while it is important to be aware of it, covered entities should not let compliance with CCPA 1.0 Put difierently, CCPA 1.0 is real, while CCPA 2.0 has not yet materialized.
- **Stay "In the Know":** While covered entities should not become distracted by CCPA 2.0, they should closely monitor its developments to prevent being blindsided if and/or when the referendum passes.
- **Ask Questions Now, Not Later:** Covered entities should raise key compliance questions and concerns now, not later. It is better to have peace of mind and a plan now, than to panic and be subject to regulatory scrutiny later.

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

Lauren Geiser
Associate
804.697.1379
lauren.geiser@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com