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 offline 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 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

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