A Report on Businesses' Implementation of the California Consumer Privacy Act in the First Month

Holland & Knight

www.hklaw.com

California's landmark Consumer Privacy Act (CCPA) went into effect on January 1, 2020. A first-of-its-kind law in the United States, the CCPA grants California residents unique transparency into how covered businesses collect, use, and share consumers' online and offline personal information, and rights to access, delete, and object to the sale of their information.

Although the law passed in June 2018, businesses had to wait most of 2019 to see what the law would look like when it went into effect. Only in October 2019 did the Governor sign a series of amendments to add, *inter alia*, one-year partial exemptions for the personal information of employees and business-to-business situations. Just days later, the California Attorney General released draft regulations which significantly added to businesses' notice and recordkeeping obligations. On February 7, 2020, the Attorney General released a modified draft of the regulations. A final version of the regulations is still at least several weeks away.

Notwithstanding the lack of final guidance, the Attorney General begins enforcement of CCPA on July 1, 2020. In the meantime, businesses must balance the cost and resources of implementing the draft regulations, with the risk it could all be for naught if provisions are removed from the final requirements. Added to that uncertainty is a general lack of clarity around analytics and digital advertising technologies such as cookies and pixels, and particularly whether a company's ordinary use of those technologies on its website amounts to a "sale" of personal information under the CCPA.

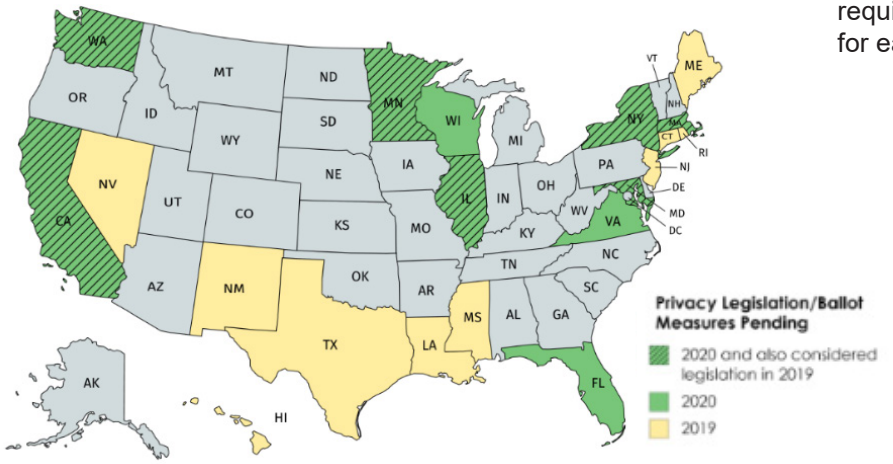
Two weeks after the law took effect, Holland & Knight conducted a survey of the websites of 125 of the country's largest public and privately-held companies to take stock of how businesses have operationalized CCPA.[1] The survey observed substantial differences in the approaches taken by companies, particularly in four key areas:

- Scope of Implementation
- Consumer Requests
- Do Not Sell
- Privacy Policy Updates

Scope of Implementation

Access and Deletion Rights Generally Exclusive to California

The passage of CCPA is directly traceable to the enactment of the General Data Protection Regulation (GDPR) by the European Union in May 2018. Similarly, CCPA inspired nearly twenty U.S. state legislatures to introduce equally comprehensive consumer privacy bills in 2019. So far this year, lawmakers in Florida, Illinois, Maryland, Massachusetts, Minnesota, New York, Virginia, Washington, and Wisconsin are all considering privacy legislation. Californians, of course, are likely to be considering Alastair Mactaggart's "CCPA 2.0" initiative on the State's November 2020 ballot.

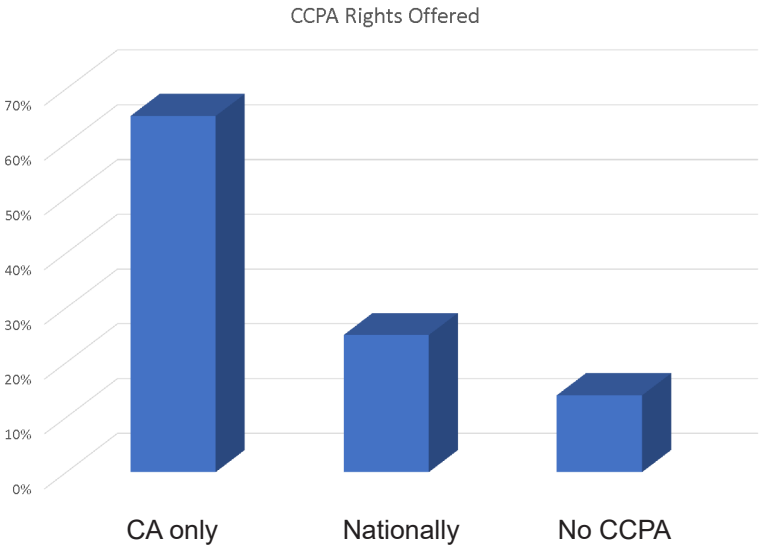


Despite widespread consumer interest in data privacy protections, and generally low expectations that the federal government could act to preempt state privacy laws in an election year, nearly 65% of companies surveyed limit the access, deletion and do not sell rights that form the core of CCPA to just California residents, rather than extend such rights voluntarily to additional jurisdictions that could adopt legislation but have not yet done so.

Just over 20% of companies give comprehensive access and deletion rights to consumers nationwide, regardless of residency. These include a diverse mix of retail, food and beverage, financial services, tech, and industrial businesses.

Nearly 15% of companies had made no website updates for CCPA at the time surveyed. These companies perhaps view the Act's July 1 enforcement date as the deadline for compliance. Any company that delays the rollout of CCPA's requirements, however, risks becoming a target for early and aggressive enforcement.

> "We will look kindly, given that we are an agency with limited resources, and we will look kindly on those [companies] that ... demonstrate an effort to comply … If they are not (operating properly) ... I will descend on them and make an example of them, to show that if you don't do it the right way, this is what is going to happen to you."
>
> - California Attorney General Xavier Becerra in an interview with Reuters on Dec. 10, 2019.



Consumer Requests

Submission Process

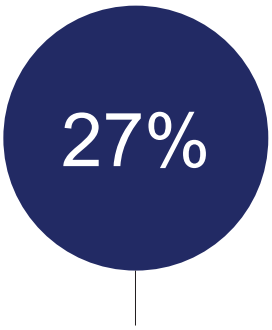
Even though only a small number of companies expressly grant access and deletion rights to consumers regardless of residency, in most cases, companies appear to lack a technical solution preventing non-California residents from submitting requests. Many rely on the consumer to self-confirm residency through a check box or statement of confirmation above the “Continue” button. Only one company was observed geo-fencing its CCPA request form to (presumably) California IP addresses.

The requirement in the October draft regulations that businesses provide a webform for submission of right to know requests was largely unexpected, and nearly a quarter of companies surveyed did not operationalize that requirement in January. Many instead provided consumers with only an email address for submission of requests. The choice appears to have paid off for some companies, as the modified regulations released in February eliminate the webform requirement and provide that email is an acceptable method for submission of requests. This change will particularly benefit companies with a global privacy program also covering GDPR, which only requires an email address for submission of consumer requests.

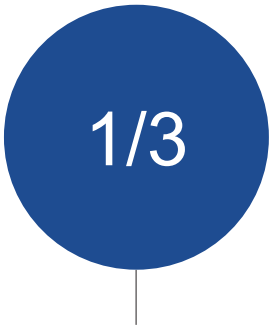
The requirement to provide a telephone option for consumers to submit requests received substantial feedback and commentary during the December 2019 public hearings held by the California Attorney General. This perhaps explains why 27% of companies do not currently offer a dedicated toll-free telephone number for submission of consumer requests. The February version of the regulations eliminates the telephone requirement for online-only businesses.

Authorized Agents Infrequently Mentioned

Only around 1/3 of companies mention in their privacy policy that consumer requests may be submitted by an authorized agent, or detail a special process by which an agent may submit a request on behalf of a data subject. As this was a new requirement in the draft regulations released in October 2019, we expect more companies will add such language in the round of updates made after the regulations are finalized.



of companies do not currently offer a dedicated toll-free telephone number for submission of consumer requests



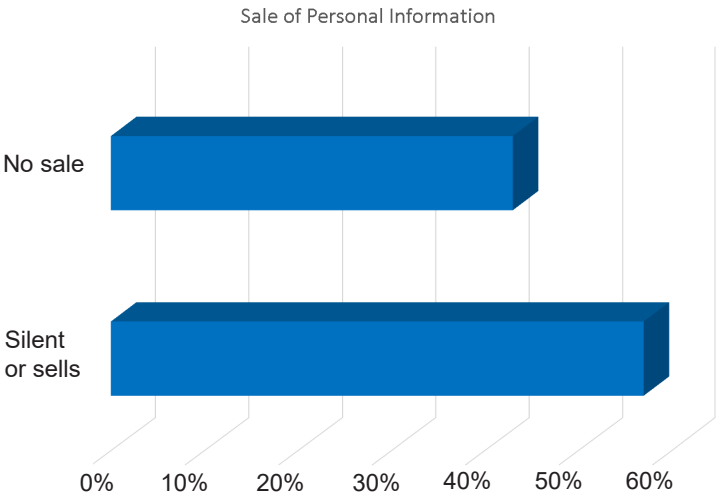
of companies mention in their privacy policy that requests may be submitted by an authorized agent

Do Not Sell

Approach Varies Widely — Blame Cookies

Navigating the ambiguity surrounding cookies and similar tracking technologies to operationalize CCPA's Do Not Sell requirement is one of the most challenging issues companies face and substantial differences were observed in implementation.

Only 22% of companies include a Do Not Sell link in their website footer at the time surveyed. In many cases, the link is connected to a GDPR-style self-serve cookie tool for consumers to manage cookie preferences on their own. In other cases, companies are effecting opt-out requests behind the scenes.



How and to what extent companies will utilize the Attorney General's newly-released CCPA button will be closely watched in the coming weeks.

While many companies (currently) do not have a CCPA opt-out link, less than 10% of companies actually state in their privacy policy that they "do not sell" personal information.[2] The remainder, 56%, are silent on the point, or more commonly, acknowledge they may sell personal information as defined under CCPA but do not provide consumers with a straightforward way to opt-out.

Cookies Policies Sporadically Used in the U.S.

Confusion around adtech is underscored by the fact that although no U.S. law requires a "cookie policy," 22% of companies provide consumers with a stand-alone cookie policy or policy on targeted advertising.

DNT = DNS

Further complicating matters, the modified regulations maintain the requirement that companies must treat user-enabled privacy controls as an opt-out of sharing. Under CalOPPA, businesses must state in their privacy policy whether they respect "do not track" signals or not. But because there is no industry standard for what amounts to "do not track," nearly all surveyed companies say they do not. The California Attorney General has now effectively eliminated that option, and companies will be forced to develop technical solutions to recognize and respond to "global" browser plugins, and privacy or device settings. Reg. § 999.315(d). How a company is expected to distinguish between California consumers' use of privacy controls versus other consumers' use, moreover, is a challenge that is likely to require significant industry resources to solve.

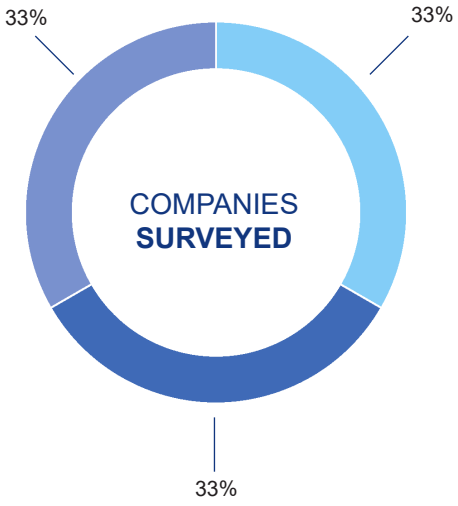
> The confusion around Do Not Sell is attributable to several factors: (1) a general lack of sophistication regarding third party behavioral advertising and website analytics on the part of the lawmakers, agency staff, and advocates who drafted the Act and regulations, and also by the lawyers and compliance personnel charged with implementing the law; (2) lack of real guidance from the California Attorney General on the opt-out process; (3) ambiguity in the law itself as to whether or when cookies-derived data constitutes a "sale" under the CCPA; and (4) technical and operational challenges that prevent a business from easily blocking third-party cookies on a user-by-user basis and communicating opt-outs to those third parties.

Privacy Policy Updates

Jurisdictional-Specific Disclosures

For companies with a global footprint, regional privacy regulations impose a unique compliance and operational challenge. Unsurprisingly then, the manner in which companies communicate jurisdiction-specific privacy disclosures to consumers varies widely.

One third of companies surveyed provide separate privacy policies applicable to consumers based on geographic region — generally the United States and Europe / Rest of the World. Another third take this jurisdiction-based approach a step further and provide a stand-alone California privacy notice, in addition to a U.S. privacy policy. At the other end of the spectrum, 1/3 of companies offer a global privacy policy intended to cover all applicable regulatory schemes in a single document.



provide separate privacy policies applicable to consumers based on geographic region

provide stand-alone California privacy notice, in addition to a U.S. privacy policy

offer a global privacy policy intended to cover all applicable regulatory schemes

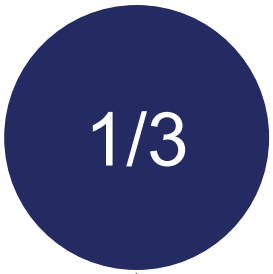
Nevada Disclosure

Fifteen percent of companies surveyed include language in their privacy policy in response to Nevada's new privacy law, NRS 603A.340. Interestingly, about half of those businesses say they do not sell under CCPA. The Nevada definition of a "sale" however, is encompassed within CCPA's broader definition of that term.

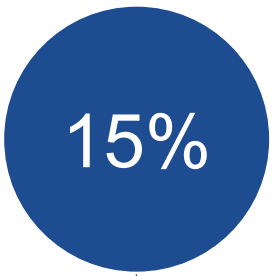
Notice of Financial Incentives

Just over half of the companies surveyed do not mention discrimination or financial incentives in their privacy policy. Of those that do, most address the new financial incentive language in section 999.307 of CCPA's draft regulations with a general statement that consumers will not be discriminated against for exercising their CCPA rights.

Fewer than ten companies acknowledge that they may charge a different rate or provide a different level of service. No surveyed company currently provides a "good faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference" and description of the method used to calculate such value, in its privacy policy. Reg. § 999.307(b)(5).



of companies mention in their privacy policy that requests may be submitted by an authorized agent



of companies surveyed provide Nevada opt-out

Conclusion

Most large companies committed significant time and resources towards CCPA compliance in 2019. But many businesses appear (reasonably) hesitant to expend additional resources implementing new requirements found in CCPA's draft regulations, or to make key decisions on the treatment of cookies, until the final form of the law is better understood.

The evolving regulatory landscape only complicates the challenges companies will face in the year to come. Federal action to preempt CCPA appears unlikely in the short term, and privacy advocates are pressing forward to have CCPA-author Alastair Mactaggart's "CCPA 2.0" initiative included on California's November 2020 ballot. At the same time, businesses are waiting to see what the State legislature will propose regarding the treatment of employees and other information exempted from CCPA for 2020. Outside of California, state lawmakers in some of the country's most populous states are considering comprehensive consumer privacy bills introduced during the first month of the year — several of which would be effective next year if enacted as currently drafted.

Practice Profile

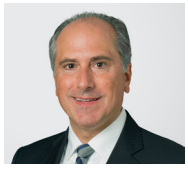
Holland & Knight's Data Strategy, Security & Privacy Team helps clients capitalize on data and tech capabilities while managing associated risks and incidents that arise. We have advised and represented clients on many of the largest public (and nonpublic) data issues and security incidents in the U.S.

We deliver: 1) pragmatic business-oriented solutions to address legal needs, 2) documentation you need for legal compliance and contracting, and 3) strategic representation during an incident, as well as in investigations and litigations that may follow. We do it efficiently, with transparent budgeting and billing.

How to Reach Us

Ashley L. Shively
Partner, San Francisco
415.743.6906
ashley.shively@hklaw.com

Mark H. Francis
Partner, New York
212.513.3572
mark.francis@hklaw.com



Mark S. Melodia
Partner, New York
212.513.3583
mark.melodia@hklaw.com

Paul Bond
Partner, Philadelphia
215.252.9535
paul.bond@hklaw.com

[1] It should be noted that this survey only reports on the publicly-available aspects of compliance and thus may not reflect the entire picture of a business's efforts to comply with the law.

[2] CCPA's draft regulations require a company that does not sell personal information state that fact in its privacy policy. Section 999.306(d)(2).