CCPA Update: Prioritizing Compliance with Two Months Until the CCPA Takes Effect

Alysa Z. Hutnik, Alexander I. Schneider

October 31, 2019

In exactly two months, the California Consumer Privacy Act (CCPA) takes effect. Many businesses are devoting resources to timely comply, but between the late rollout of the Attorney General's draft regulations, recent amendments to the law, and a lack of consensus in the industry on interpretation of key CCPA terms, tackling compliance can be daunting. Perhaps that's why in two polls released this year, businesses have overwhelmingly told the International Association of Privacy Professionals that they are not prepared for the CCPA.

The enforcement penalties support good faith and reasonable efforts to achieve compliance, but the CCPA grants the Attorney General the ability to seek civil penalties of $2,500 for each violation of the law, without defining "each violation." As with any new law, common sense typically prevails on what early enforcement will address. In general, such cases tend to be the obvious non-compliance, rather than the borderline cases.

Beyond penalties, the CCPA will set the standard for how businesses describe their data practices and privacy commitments to consumers. Non-compliant or confusing privacy messages or practices may have reputational and public relations costs as well. Importantly, the Attorney General cannot bring an enforcement action until, July 1, 2020, at the latest, but any such enforcement action can focus on noncompliance that began on January 1, 2020.

For businesses seeking to comply, and fast, we highlight considerations for prioritizing compliance efforts. Of course, each business is different, and consultation with legal counsel is the surest way to develop a plan to comply with the new law.

Priority: Consumer-Facing Obligations

The CCPA is laser-focused on providing consumers with the tools to exercise their rights to access, delete, or opt out of the sale of their personal information. In particular, the CCPA requires businesses to describe these rights and how they comply in their privacy policies and other required notices.

Companies can prioritize building consumer-facing processes and notices that demonstrate publicly that the business respects and complies with the CCPA. This prioritization includes:

- **Prioritizing Transparency:** Post plain language, straightforward consumer notices that address the current CCPA requirements in a manner that a consumer would actually understand (a challenge given reports that many privacy policies require a college reading level). Reviewing privacy policies is often the first step that a consumer – or regulator – can take to see if a

company is complying with the CCPA. Privacy policies are public representations and should be vetted to confirm that they accurately reflect a company's practices and do not contain allegedly false or deceptive statements.

- **Adopting a Privacy-Centric Company Culture:** Businesses can establish procedures for personnel, including customer service agents and others most likely to interact with California consumers, so they are prepared to handle privacy rights discussions, or escalate or transfer such requests to those who can. The more straightforward the process, the less likely consumers will become confused and complain. A spike in complaints can be a key source for regulators and others to scrutinize a company's practices.
- **Creating User-Friendly Options for Privacy Rights Requests:** Provide clear directions on how consumers can submit requests, and through which channels. In particular, the CCPA requires a toll-free number (except for online-only businesses) and, for companies that "sell" personal information, a link on the home page that enables consumers to opt out of the sale of personal information.
- **Setting the Right Tone:** As with all customer interactions, tone and responsiveness matter. When a consumer makes a privacy rights request, provide a brand-consistent, friendly response within 10 days that confirms receipt and provides information about how the request will be processed.

Priority: Protect Personal Information

The CCPA encourages implementing and maintaining reasonable security procedures and practices. In particular, the CCPA provides a private right of action to any consumer whose unencrypted and unredacted personal information is subject to a security incident due to a business's failure to implement and maintain reasonable security procedures and practices. Among other remedies, the CCPA provides for statutory damages of $750 per consumer per incident or actual damages, whichever is greater.

Given the significant potential for litigation and statutory damages, prioritizing cyber security is more important than ever. "Reasonable Security" includes:

- **Compliance with Reasonable Industry Standard Practices:** As described in a prior California Attorney General report, Critical Security Controls identified by the Center for Internet Security provide a "minimum level of information security that all organizations that collect or maintain personal information should meet." These controls include reviewing hardware and software connected to a company's network; implementing key security settings; limiting user and administrator privileges; assessing vulnerabilities and patching holes to stay current; securing critical assets and attack vectors; defending against malware and intrusions; blocking vulnerable access points; providing security training to employees and vendors with access to the network; monitoring accounts and network audit logs; testing defenses; and planning a response to security incidents. Importantly, businesses should document these efforts. Being able to demonstrate that it followed these controls, and how, will be a critical part of a company's defense.
- **Third-Party Liability for Vendor Compliance:** An important aspect of the business/service provider relationship is that a business that discloses personal information to a service provider "shall not be liable … if the service provider … uses it in violation of the [CCPA], *provided that, at the time of disclosing the personal information, the business does not have actual*

knowledge, or reason to believe, that the service provider intends to commit such a violation." Businesses can review vendor contracts, vendor-posted public terms, vendor descriptions of their services and how they use data, as well as vendor privacy policies and data processing addenda, to support that a vendor reasonably qualifies as a "service provider" and that there are no "red flags" that could provide a basis for third party liability. Depending on how many vendors a business has, it may be reasonable to tackle these efforts by tiered priority.

Priority: Plan for the CCPA's Impact on Your Digital Advertising

A key area of interest is how the CCPA defines the "sale" of personal information, and how the definition applies to Ad Tech relationships and different services, including the variety of ways your company may use interest-based advertising, enrich your existing data sets, use different types of data analytics services, use matching and re-targeting, or target your advertising to certain defined audience segments.

In particular, publishers may be considered to have "sold" consumer personal information when they pass along persistent identifiers to other Ad Tech participants depending on the relationship with such participants, and how such participants use the data. Just as important, companies that use service providers to assist with their advertising and data analytics efforts should evaluate and firm up such classifications. For partners that are not intuitively service providers or obvious recipients of data sales, more analysis and industry benchmarking on interpretations are likely warranted.

The Interactive Advertising Bureau proposes a framework that will enable publishers and their partners to comply with the CCPA's provisions on the "sale" of consumer data by providing publishers a technical solution to signal to partners that a consumer has opted out of the "sale" of their personal information. The framework will bind Ad Tech participants using a limited service provider contract. Through this arrangement, the framework maintains the availability of interest-based advertising, but restricts participants in their use of personal information to strictly business purposes.

Otherwise, for companies engaged in digital advertising and analytics, some priorities include:

- **Assessing the "Sale" of Personal Information:** Review any disclosure of personal information to other businesses and determine if that disclosure counts as a "sale" for purposes of the CCPA. If so, develop a plan to comply with the CCPA's requirements.
- **Cataloging Cookies and Pixel Tags:** Companies that have contracted with Ad Tech vendors to place cookies or fire pixel tags should catalog these activities and determine the extent to which they represent a "sale" of personal information, or if they reasonably qualify as service provider support. Alternatively, the Company may choose to block them from collecting personal information on the Company's sites.

If you have any questions about compliance obligations under the CCPA, please contact Alysa Hutnik or Alex Schneider.