Navigating CCPA Compliance in the Absence of Clear Rules

Since its enactment in June 2018, business leaders are well-aware that the California Consumer Privacy Act (CCPA) will impact the way they do business in the online economy, though the law’s compliance requirements remain murky. How can organizations prepare for CCPA compliance in the absence of clear guidance?
Since its enactment, the California Consumer Privacy Act of 2018 (CCPA) has become a source of confusion and anxiety for firms subject to the law’s requirements. As CCPA becomes operative on January 1, 2020, many business leaders struggle to determine how the bill will impact their organization. This hastily-drafted piece of legislation was driven by the advocacy of a wealthy Californian who leveraged the state’s ballot initiative process to force legislative action on the subject. As a result, the first version of the law contained errors, ambiguities and inconsistencies. Shortly after passing, the legislature amended CCPA by delaying attorney general enforcement of the privacy provisions of the law by six months, correcting technical errors, and exempting organizations currently subject to privacy provisions in a subset of federal and California state laws, including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). Though pending regulations and amendments may provide additional clarity for organizational leaders, some fear that uncertainty about the particulars of the statute may hinder companies’ ability to plan an effective compliance strategy on or before the California Attorney General’s enforcement date.

Business leaders may have good reasons to be concerned. Organizations around the country offer products and services to California residents; and this populous state often disproportionately represents companies’ overall customer portfolio. Those for-profit enterprises in scope of CCPA’s requirements face civil monetary penalties for non-compliance ($2500 per uncured violation, up to $7500 per intentional violation) and private right of action in response to consumer harms from data breaches (with monetary damages capped at $100 to $750 per impacted consumer). These factors provide organizations a strong incentive to ready themselves for CCPA compliance sooner versus later.
**Drawing Comparisons Between CCPA and GDPR**

For US-based companies doing business in the EU (including the United Kingdom, for now), most are aware of the General Data Protection Regulation (GDPR) and its strict standards for processing personal information (PI) about those in the Union. With myriad administrative and operational requirements, steep fines, and aggressive enforcement by European data protection authorities, GDPR sets the high mark for data protection in the EU and across the world.

**Similarities**

After CCPA passed, many experts noted similarities among GDPR’s core principles. For instance, CCPA and GDPR each provide new or enhanced rights designed to improve individuals’ control over the ways that organizations collect, use and share PI. Both laws require firms to improve transparency by offering detailed disclosures of their processing activities; and each requires organizations to enable prompt access to individuals’ PI, provide a detailed accounting of PI collected and shared with third parties and, erase individuals’ PI upon request. Other converging requirements relate to simple and accessible opt-out mechanisms, privacy rights for minors, data breach provisions, and the types of PI that organizations must safeguard. Lastly, both laws have extra-jurisdictional reach, as each focus on the act of processing personal information, regardless of where the processing occurs.
Differences

For all their similarities, the requirements of GDPR and CCPA vary in substantive ways. Each law addresses data privacy from perspectives grounded in unique histories and cultures. As a pillar of the EU’s Digital Single Market strategy, GDPR creates a uniform standard for data privacy regulation across its member countries. No such unified strategy exists in the US; and federal indecision on the development of comprehensive data privacy regulations compels states like California, Washington and others to add to the messy patchwork of privacy-focused laws across the country.

There are also differences in the scope of the laws. Under GDPR, any organization that processes PI (called a data “controller”) belonging to folks in the EU is subject to the law’s requirements. CCPA more narrowly covers the activities of “businesses” (which excludes non-profits and government agencies) who collect, use, or share Californian’s PI for commercial purposes. For third-party service providers doing business with in-scope firms, GDPR defines more rules for data “processors” than CCPA’s “service providers.”

Most privacy professionals agree that GDPR carries a heavier administrative burden than CCPA. Unlike the California law, GDPR requires organizations to develop an appropriate “legal basis” for processing PI. In order to meet this standard, business leaders must determine whether it makes sense to obtain consent from individuals prior to processing (the default option, which is a heavy lift for some) or find another legal option to meet GDPR’s standards. For organizations that transfer personal information from the EU to the US and elsewhere, GDPR has stringent rules and restrictions that company leaders must
address proactively. Other administrative requirements that set GDPR apart from CCPA include curiously prescriptive requirements for appointing a functionally-independent data protection officer (DPO), conducting regular data protection impact assessments (DPIAs) prior to deploying new products and services, and developing documented inventories of data processing activities.

**Lessons Learned from GDPR/CCPA Comparisons**

For organizations that invested in GDPR-focused compliance efforts, the dust was only beginning to settle when CCPA suddenly emerged. Luckily, the similarities between the laws make the job of complying with both a little easier. For instance, the muscle-memory developed in support of GDPR’s rights for individuals will boost process efficiency when addressing CCPA’s mandates separately. That said, GDPR compliance does not guarantee full conformity with CCPA’s requirements. Business leaders should act urgently to understand where the similarities end, and the differences manifest into additional legal obligations for those subject to both laws.

**Addressing CCPA’s Ambiguities**

Unsurprisingly given its breadth and depth, CCPA has its fair share of ambiguity. One should expect this when legislators attempt to address a topic that is far from black and white. It appears that California’s legislative response to the actions of certain industries – namely the social media giants, online advertisers, and other firms whose profits are dependent on the processing of personal information – makes for a set of requirements that can be especially perplexing for firms with a modest online presence.
In their haste to pass the law, California policymakers acknowledged CCPA’s imperfections. In response, the law directs the state’s Attorney General to draft supporting regulations. At present, the AG’s office is conducting listening sessions for feedback from citizens, industry representatives, and other stakeholders.

Transcripts of these events reveal that participants are eager to understand the more nebulous parts of the law. Everything is on the table during these sessions: from CCPA’s definitions of “personal information,” “selling” and “households” to the finer points of the law’s anti-discrimination mandates. Naturally, industry representatives are using uncertainties in the law to lobby for refinements that move in their favor.

Preparing for the Unknown

Until California publishes its regulations and/or policymakers pass amendments to the law, business leaders looking for definitive answers about CCPA’s impact will be disappointed by lawyerly caveats and cautious estimates. Lack of clarity should not translate to lack of action however, as there are many things organizations can do today to prepare for the effective date.

As with any new compliance effort, business leaders should undertake an assessment of the firm’s CCPA readiness. Companies that completed a readiness assessment in the runup to GDPR compliance can leverage many of the lessons learned in preparation for CCPA. For those companies that have not begun the process of identifying gaps between CCPA’s requirements and current business practices, time is running short. We recommend a four-step approach (illustrated and described below):
Step One: Understand Context

Organizations should seek an understanding of business context to identify the factors that will influence decision-making throughout the CCPA readiness process. Some key questions to consider during this step include the following:

- What are our business objectives and values?
- What proportion of our customers are California residents?
- How do we collect PI and from whom?
- What do we sell and how do we sell it? To whom? Through what channels?
- How do we market to consumers? Through How critical is our brand identity?
• Can we leverage sound privacy practices to differentiate ourselves in the market?
• Do we have a data privacy program in place? How can we leverage these controls?
• Do we have the internal resources and expertise to implement enhanced privacy controls?

With an understanding of business context, firms can identify potential compliance roadblocks and opportunities, focus on areas of greatest exposure, and develop the most effective approach to implementing CCPA-focused controls and processes.

**Step Two: Validate Scope**

Determining which parts of the business are in scope for CCPA’s requirements helps organizations minimize compliance-related costs and business disruptions. The scope validation step starts with a disciplined approach to identifying data flows and inventorying data elements. Though not an explicit requirement in CCPA, this is a critical step towards an efficient compliance program. Without an understanding of the location of PI, companies will find it difficult to efficiently facilitate an individual’s request for access to or erasure of PI. To begin the process of data discovery and classification, focus on key business processes. For each process, organizations should map the flow of PI from its origination point to its final disposition. Once completed, firms should regularly update data flow mappings and make them readily available to those who can benefit from this information.
Step Three: Conduct an Assessment

The next step is conduct a thorough assessment to identify and prioritize gaps between CCPA’s requirements and existing controls. Despite the lack of clarity in some of CCPA’s more detailed requirements, organizations can rely on the foundational principles of CCPA to frame the assessment. For those subject to GDPR, firms can also leverage some of the similarities between the two laws.

Step Four: Plan Mitigation Strategy

Use the results of the assessment to communicate gaps to stakeholders, seek executive support, and secure budget. Include estimates for mitigating gaps, measured in time and resources. Develop a strategic plan that outlines milestones and provides room for changes after publication of CCPA’s regulatory guidance.

About the Author

Adam Stone is Vice President of Consulting Services and Chief Privacy Officer for Minneapolis-based Secure Digital Solutions, Inc. (SDS). SDS partners with businesses to efficiently navigate complexities of today’s privacy and cyber security challenges. Our team of practitioners provides leadership, oversight and guidance necessary to develop sustainable risk and compliance programs aligned to business mission and objectives. For information about how your organization can prepare for CCPA compliance, contact us at 952-544-0234 or info@trustsds.com.