REPORT REPRINT

The California Consumer Privacy Act: not just 'America's GDPR'

MARCH 1 2019

By Paige Bartley

Going into effect in January 2020, the CCPA has frequently been compared with the EU's GDPR. While the regulations are similar in ethos, they have fundamental differences that reflect subtly divergent cultural attitudes and approaches toward data privacy and consumer rights.

Summary

The California Consumer Privacy Act was passed in June 2018, largely as a legislative compromise. Originally intended to become a ballot measure, the bill was put together in just seven days to avoid a public vote that likely would have resulted in greater restrictions on the processing and analysis of personal data: restrictions that many large, California-based technology companies opposed. The law goes into effect in January 2020, but before then, debate and industry lobbying will likely change some of the details and requirements.

In many ways, CCPA has been compared with the EU's landmark General Data Protection Regulation (GDPR), sharing many of the same principles. What GDPR aimed to achieve with the global economy – setting a gold standard – the CCPA aims to achieve with the US economy, urging other states to adopt similar standards in absence of concrete federal privacy legislation. The differences in the regulations for the enterprise mean that a 'one size fits all' approach will not suffice, necessitating a more nuanced data management strategy.

451 TAKE

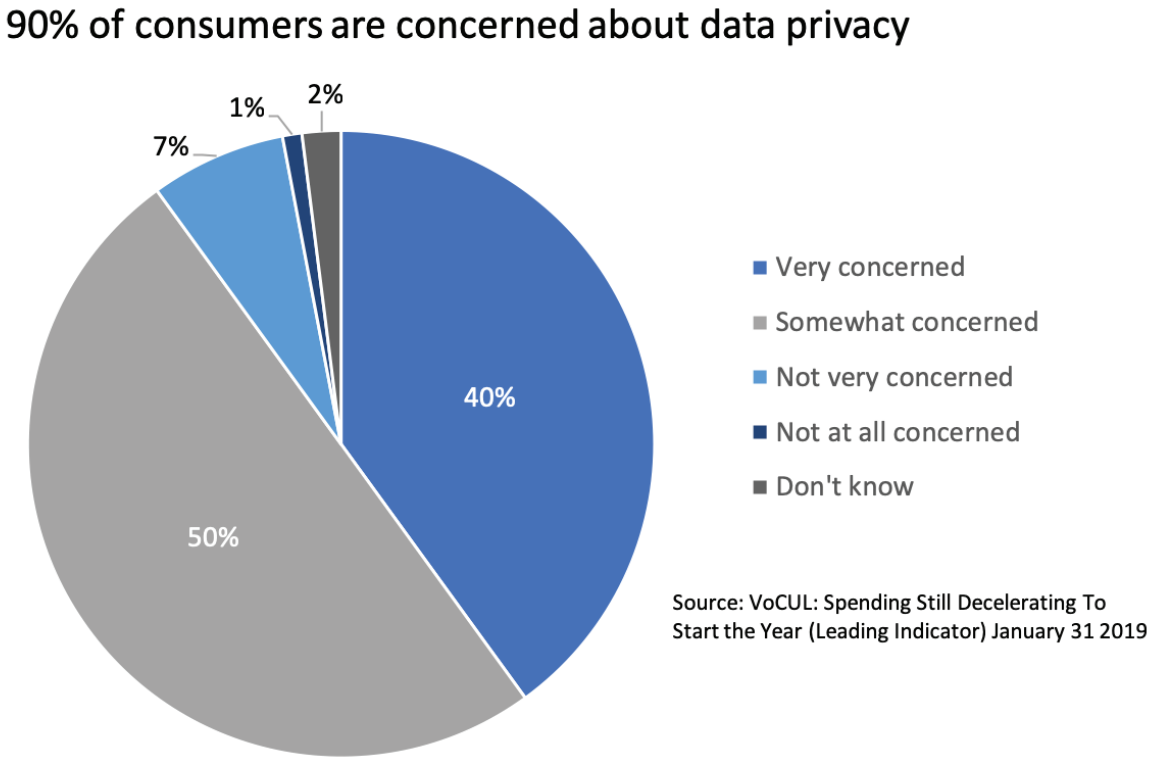
CCPA is trying to forge a de facto standard for data privacy in the US in the absence of federal legislation. With roughly 12% of the US population as its residents, and being the world's fifth largest economy, California has unique heft to enact consumer protection legislation that affects nearly any business with interstate operations in the country. In this sense, CCPA is similar to GDPR in that it uses economic presence to urge other regions – US states – to adopt similarly high standards. But GDPR and CCPA do have their own requirements and nuances, and a compliance program specifically architected to address GDPR will not necessarily translate. Troublingly, CCPA signals the beginning of 'balkanization' of data privacy regulation in the US. Businesses will need to take a more holistic and less regulation-specific approach to data management and compliance to remain competitively viable.

Data privacy and data protection, around the world, has reached a tipping point. The EU's GDPR, which went into effect in May 2018, is largely credited with triggering a domino effect of copycat regulations around the globe, as various countries sought to maintain close economic ties and simple transfer of data with the EU. The pressure to attain an 'adequacy decision' from the EU, deeming regional regulation sufficiently similar to GDPR's standards, was a primary motivating factor in nations closely copying or adapting the requirements set forth in the EU's regulation. The US, with no federal data privacy legislation of its own, started to become an outlier among developed nations.

Consumer awareness, too, has converged with global regulatory patterns to urge the discussion of data privacy in the US. Individuals are becoming more aware and more educated regarding the value and sensitivity of their data, with data breaches at consumer-facing companies now being regular headline news. Perceived privacy violations by major companies, particularly social media companies, receive increasingly vocal public backlash, even when business practices for sharing data with third parties or gaining consent for data collection were ostensibly legal in the US to begin with. 451 Research's Voice of the Connected User Landscape (VoCUL) monthly tracking of consumer trust and confidence in early 2019 shows that 27% total or 26% of US consumers are less trusting of US businesses than they were one year ago. When it comes to data privacy, nine in ten respondents are either very (40% total, 41% US) or somewhat (50%) concerned about the ability of the companies they do business with to adequately protect their personal data.

Figure 1

Source: 451 Research, LLC



With global economic pressure increasing to adopt more standardized data privacy practices and consumers becoming savvier toward violations, the US was lagging in adopting a cohesive national framework for data protection and data privacy. Traditionally in the US, data privacy legislation was very industry-specific. HIPAA, enacted in 1996, forged rules for privacy and portability of healthcare records. The Gramm-Leach-Bliley Act in 1999 created guardrails for the collection, use and disclosure of financial information. But at the federal level, the US was resistant to creating horizontal privacy rules that it perceived might limit broad economic and business opportunity. And as privacy issues came to the forefront with GDPR and increased consumer awareness, the political climate in the US did not facilitate progress. Between the 2016 presidential election and the 2018 midterm elections, gridlock between parties in Congress stalled productive discussions on bipartisan policy.

California saw this as an opportunity. Long known for progressive legislation and for being the most populous state in the nation, laws and rights that apply to California consumers or residents have overarching impact on nearly any organization that does interstate business in the US. The California Consumer Privacy Act in 2018 was a tactical move to advance a de facto national standard for data protection and privacy by establishing high standards that had extraterritorial reach. Most large businesses in the US have California residents as customers, thus pressing adoption of CCPA's standards elsewhere in the nation. But worryingly, California's legislation has spurred other states into action, drafting their own privacy laws. What could result, in absence of a federal standard, is the balkanization of privacy requirements in the US, with each state having different protections for its residents.

Key similarities, but also key differences

CCPA is inevitably compared with GDPR, and it is very similar in its core ethos. At its heart, they are both consumer protection law designed for the digital, data-driven economy. However, the exact mechanisms of how the individual laws function and enforce their requirements differ somewhat. Those distinctions often convey subtle cultural differences between the EU and the US. While detailed legal comparative analysis of the two regulations are well beyond the scope of this report, a high-level overview designed to help organizations craft more defensible data management strategy is within reach.

What they share in common

CCPA and GDPR, as well as most evolving data privacy regulations around the world, are built on core principles that are neither technical nor prescriptive. Common objectives tend to be high level in nature, and it is left to organizations to decide how to implement architectural and technical measures to comply with individual requirements. From this high-level perspective, both CCPA and GDPR are closely aligned in the following shared objectives:

- **The right to know:** Under both regulations, consumers and individuals are given bolstered transparency rights to access and request information regarding how their personal data is being used and processed.
- **The right to say 'no':** Both regulations bestow individual rights to limiting the use and sale of personal data, particularly regarding the systematic sale of personal data to third parties, and for limiting analysis/processing beyond the scope of the originally stated purpose.
- **The right to have data kept securely:** While differing in approach, both regulations give consumers and individuals mechanisms for ensuring their personal data is kept with reasonable security standards by the companies they interact with.
- **The right to data portability:** Both regulations grant consumers rights to have their data transferred in a readily usable format between businesses, such as software services, facilitating consumer choice and helping curb the potential for 'lock-in.'

How and why they differ

The devil is in the details. While CCPA and GDPR share the same broad objectives, their individual rules differ, creating trouble for the enterprise that is striving to comply with both. The US, even California, has traditionally taken a light-touch, free-market approach to business that generally views data privacy regulation as a hindrance to innovation and societal advancement.

Europe, on the other hand, has the historical perspective of WWII to shape its views on the potential systematic abuse of personal information and state surveillance. Regarding data privacy in Europe, consumers generally trust their modern governments more than they trust corporations. In the US, the opposite is true, with consumers having more faith in brands than they do in their own elected leadership. This has shaped the dynamics of the respective regulations.

Significant differences, though not an exhaustive list, include the following:

- **Who is protected by each regulation:** It goes almost without saying that GDPR and CCPA protect distinct audiences of individuals based on geography. GDPR protects identified or identifiable natural persons in the EU, 'data subjects,' whether they are legal citizens or not. CCPA protects 'consumers,' which can be individual California residents either within the state or temporarily traveling out of it.
- **What types of organization are regulated:** GDPR offers certain regulatory exemptions for businesses with fewer than 250 employees. CCPA, in general, is much more protective of small businesses and startups, exempting for-profit ventures with a gross revenue of under $25m, as well as exempting for-profit organizations that handle the personal information of less than 50,000 consumers, households, or devices for commercial purposes.

- **How personal information is defined:** Both regulations focus on data that can be either directly or indirectly linked to a living, breathing individual. However, CCPA specifies that data can also be linked at the household or device level, arguably offering a broader definition. CCPA excludes protection of certain government and public records, while GDPR offers strong protections for special defined classes of data, such as criminal records.
- **Consumer and/or individual consent:** CCPA grants California residents the right to explicitly opt out of the sale of their information to third parties. GDPR, while not giving this specific control, grants rights further upstream: in certain cases requiring explicit opt-in consent for personal data processing or analysis to occur at all. It is important to note that CCPA does not impose consent rules for data collection, only data sales. GDPR has robust rules around data collection and associated consent procedures.
- **Fine structure and civil penalties:** At first glance, GDPR's maximum 4% fine on global revenue (or up to €20m, whichever is greater) may seem to have sharper teeth, but CCPA's 'death by papercuts' approach fines individual violations. A fine of $2,500 per individual violation, or up to $7,500 per violation if intentional, is possible under CCPA.
- **Right to restrict (or object to) personal data processing:** Under many circumstances, GDPR gives individuals the right to restrict the processing and profiling of their personal data. CCPA does not provide for this mechanism; rather, it just allows individuals to opt out of the sale of their information to third parties.
- Right to rectification (correction) of personal data: Under GDPR, individuals may request that incorrect personal information held by a company be rectified, or corrected. Incomplete personal data may be completed. Under CCPA, no such explicit right exists.
- **Automated decision-making:** One very tricky area of regulation is the rules around quickly-evolving AI and ML technologies, which GDPR indirectly addresses with consumer protections and rights to object regarding the use of automated decision-making. CCPA does not address this subject, perhaps because it does not want to hinder the innovation occurring in this space, particularly with California-based technology companies.
- **Children and minors' rights:** The primary similarity between GDPR and CCPA regarding the treatment of minors is age. Both regulations use 16 as a common bar for 'adult' consent, and 13 as a bottom rung for possible independent consent. But GDPR requires adult consent for all data processing consent requests, whereas CCPA invokes adult consent only when the sale of data is involved. However, existing laws such as COPPA in the US provide additional online protection for minors.
- **Data security requirements and breach reporting:** CCPA is not prescriptive with security requirements, but it does establish a right of consumer action for certain data breaches that violate existing California law. GDPR mandates appropriate technical and organizational measures to protect data, and has an onerous 72-hour reporting window for suspected or detected breaches.

Business strategy amid proliferating regulatory requirements

While the list above may suggest there are more differences than commonalities between regulations, their core principles are largely identical. It is key for organizations is to tackle core, shared requirements at the architectural data management level and address individual nuances of each regulation with tools higher in the stack only as necessary. Such an approach allows for flexibility amid evolving regulations, and ultimately, cost savings.

As 451 Research discussed in the report 'Architectural data control: Turning privacy requirements into a blessing, not a curse,' strong, consistent and granular control of enterprise data is a shared requirement across all data-driven regulations. Just as a mother sauce in French cuisine can be adapted to meet the specific requirements of individual dishes, strong enterprise data control can be adapted to meet the individual requirements of individual regulatory requirements. In this sense, a bottom-up approach, focused on architectural control of data, is warranted. No number of custom compliance point solutions, implemented higher in the stack, can address or fix a lack of data control at the repository level.

It is important to note, too, that data privacy and data protection regulations are largely more process-oriented than they are technology-oriented. People, and the workflows they engage in to control data, must be orchestrated. Investment in platforms that help coordinate processes across various data protection and data privacy stakeholders can especially benefit the business, even when these platforms do not exert direct control on data themselves. In these cases, the enterprise must take care to evaluate the breadth and depth of integrations available because these are necessary for ensuring that specific data protection actions, such as encryption, are ultimately executed without disrupting the human workflow. Support for a broad variety of end-user stakeholders ranging from IT to data steward to privacy professionals is also needed.

Finally, enterprise perceptions today are still a hindrance to successful compliance strategy. Most organizations still view compliance as a reactive, costly and burdensome business function. That must change, given the reality of proliferating global requirements. Compliance requirements are an opportunity to reassess and optimize core data management architecture, for the ultimate benefit of all data-driven initiatives within the enterprise. To play Whack-a-Mole with compliance requirements, forging a new task force and new set of tools for each regulation, is not scalable or sustainable. The successful business in the data protection and data privacy era will focus on core competencies that are required and shared by all regulations, and customize only as needed in specific cases.