Corporate Counsel Business Journal
July ▪ August 2019
ccbjournal.com

CCBJ

# California Sets National Data Privacy Standard

**▶ Scott D. Schneider and Raj Shukla of the Commercial Bank of California, along with Travis Brennan of Stradling, discuss the impact of recently enacted privacy regulations in the U.S. and abroad.**

**CCBJ: The California Consumer Privacy Act (CCPA) becomes effective in January 2020. What are some of the key factors that corporations need to focus on to maintain compliance?**

There are at least six important things to keep in mind. First, and of particular significance to Commercial Bank of California and other financial institutions, the CCPA expressly exempts from its coverage "personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act." But this does not mean that financial institutions should ignore the CCPA. To the extent a financial institution is collecting personal information separate from its provision of financial services to customers (such as through its public website), that activity does not fit under the exemption. The CCPA provides similar partial exemptions for companies subject to the federal Health Insurance Portability and Accountability Act and some other industry-specific regulations.

Second, the word "consumer" masks the Act's true scope. A "consumer" is broadly defined as a California resident. In addition, the Act dramatically expands the definition of what constitutes "personal information." Under California's original information security law, "personal information" was limited to specific and sensitive data points, such as social security number, driver's license number, account numbers and login credentials and medical information. The CCPA protects those categories as well, but it doesn't stop there. "Personal information" now means any "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." These broad definitions mark a fundamental paradigm shift that has long been prevalent in Europe but is relatively new in the U.S.: data protection is no longer limited to helping avoid the tangible harms of identity theft; it's about preserving the intangibles of human dignity and autonomy in a digitally integrated world. That purpose should animate compliance efforts.

**Travis Brennan** is chair of Stradling's privacy and data security practice. Reach him at tbrennan@sycr.com.

Third, the CCPA is not limited to specific industries or activities; it will have some impact on most companies doing business in California. Any company with annual revenues of more than $25 million is a covered "business" under the Act. And regardless of revenues, a company will qualify as a covered "business" if it maintains a public website that averages 4,167 unique visitors from California per month. Furthermore, many companies who do not meet the Act's definition of a covered "business" will still meet the definition of "service provider" because their services involve processing personal information on behalf

of a customer who is a covered business. The Act requires businesses to impose certain obligations on their service providers via contract, so service providers will have their own compliance obligations.

Fourth, in terms of operational impacts, it helps to think of the CCPA as having two sides – the privacy side and the security side. On the privacy side, the Act creates four new rights for consumers: (1) the right to know, through a general privacy notice and with more specifics available upon request, what personal information a business collects, what it is being used for, and whether and to whom it is being disclosed or sold; (2) the right to require deletion of their personal information, subject to certain exceptions; (3) the right to opt out of allowing a business to sell their personal information – or in the case of minors under 16, the right to opt in; and (4) the right to exercise their rights under the Act without being discriminated against in terms of the services they receive. Covered businesses and their legal counsel will need to carefully map the flow of personal information through the organization, update privacy notices, make changes to the company website, develop a process for responding to consumers requesting to exercise their privacy rights, and develop other processes to implement requested deletion or transfer of personal information when required.

On the security side, the Act imposes a duty to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." If they have not done so already, covered businesses and their legal counsel should conduct security risk assessments to develop a written security policy, incident response plan, and administrative, physical and technical safeguards that are commensurate with the business's operations, risk profile and resources.

Fifth, the penalties for noncompliance can be severe. The Act empowers the Attorney General to institute civil enforcement actions against businesses or service providers who violate it, which can result in civil penalties of up to $2,500 for each violation or $7,500 for each intentional violation. The Act also gives consumers the right to sue for unauthorized use or disclosure of their personal information that results from a "business' violation" of its security duty and seek statutory damages up to $750 "per consumer per incident or actual damages, whichever is greater." The right to statutory damages makes a wave of class-action lawsuits likely, and the Act purports to render at least some consumer arbitration agreements unenforceable.

Sixth, some of the Act's requirements are subject to change before the end of this year, and others have yet to be written. There are a number of proposed amendments working their way through the legislature, including one to clarify that a business need not treat its California employees as "consumers" under the Act. Also, the Act delegates to the Attorney General's Office some very significant rule-making authority,

**Raj Shukla** is general counsel with Commercial Bank of California.

and some aspects of compliance will be difficult, if not impossible, until those rules are enacted. For example, some of the privacy rights are only triggered upon a business' receipt of a "verifiable consumer request," but the Act leaves it to the Attorney General to define what constitutes such a request. It's possible that those rules will not be published until shortly before, or even after, the Act's effective date of January 1, 2020.

**The GDPR and the CCPA, while both designed to protect consumer privacy, are not one in the same. What differences and similarities should companies be aware of as they prepare for compliance with the CCPA?**

The differences shouldn't be overlooked. A defining feature of GDPR is its default prohibition against any processing of personal data unless a business has a "lawful basis" for the processing, which in many instances means obtaining specific, opt in consent from the consumer. The CCPA, in contrast, defaults to permitting processing of personal information subject to disclosures about the processing and a limited right to opt out. This fundamental difference means that the GDPR presents a set of compliance challenges that the CCPA does not.

That said, the GDPR clearly inspired some important aspects of the CCPA. Most prominently, the CCPA's definition of "personal information" is quite similar to the GDPR's expansive definition of "personal data." Indeed, the CCPA may have gone a controversial step further by including within the definition any "inferences drawn from" other personal information to "create a profile about a consumer." The implication appears to be that consumers will ultimately control not just their personal information but any commercially valuable insights a business develops using that information.

Another similarity is the CCPA's distinction between "businesses" and "service providers," which roughly mirrors the distinction between "data controllers" and "data processors" under the GDPR. But it is a little unclear whether some aspects of the CCPA apply to both business and service providers, or to businesses only.

**Scott D. Schneider** is executive vice president, CISO with Commercial Bank of California.

Under both the GDPR and the CCPA, the first step to compliance is careful mapping of how personal information flows through your organization. Companies that have achieved, or are working towards, GDPR compliance may have a head start in that regard, but the CCPA ultimately requires a dedicated compliance program given its unique privacy mandates.

**How does Stradling help companies prepare for the likelihood that a security incident will happen at some point?**

We encourage companies to start by thinking about the questions that regulators or plaintiffs would ask if an incident occured. For example: What was the nature of the vulnerability? Was it something you had anticipated, or should have anticipated? What steps had you

## GDPR has become a de facto standard for many multinational companies.

taken to minimize this risk? How can you be sure this hasn't happened before? As a litigator, I'm often investigating those types of questions on behalf of clients, and I bring that perspective to my compliance advice. The answers need to be backed up by an evidentiary record that shows what you did to assess and minimize risks in the weeks, months and years before an incident occurred. Building that record requires attention from the board and senior management, allocation of appropriate resources, regular risk assessments, development and implementation of a security program, and continuous updates to that program.

Assistance of outside counsel will be most effective if counsel is retained to lead a security incident investigation before an incident occurs. The investigative process needs to launch immediately and proceed quickly. If legal counsel is not leading that process, the communications exchanged in the hectic hours and days following detection of an incident – which may contain premature conclusions or statements based on incomplete information – will not be covered by the attorney-client privilege and will therefore be discoverable in any litigation arising from the incident.

We also encourage companies to put appropriate PR resources together in advance. The fact that a company suffers a data breach is not proof that it ignored duties to take reasonable care of personal information, but it often gets reported that way. The public narrative about an incident can harden very quickly, and good PR may keep any initial reputational hit from developing into an existential threat to the business.

**How will the CCPA impact doing business nationwide?**

The CCPA presumes that a business already has the means to determine whether any given individual, such as a visitor to its website, is a California resident. How else is a company to know whether it annually "receives for the businesses commercial purposes . . . the personal information of 50,000 or more consumers," and is therefore a covered business, when "consumers" means "California residents"? Companies will need to decide what changes they are willing to make to national operations for the purpose of determining how those operations impact California residents specifically.

For many companies who are not subject to federal data privacy laws, the CCPA may set a de facto national standard unless and until it is overridden by broader federal legislation. GDPR implementation provides some evidence for this theory – GDPR has become a de facto standard for many multinational companies because there are operational efficiencies and brand image benefits from applying the robust GDPR protections to all consumers, not just those residing in the European Economic Area. Given the size of California's economy relative to the rest of the United States, any companies that operate nationally might make a similar calculation as a result of the CCPA and simply treat all U.S. consumers as California residents as it pertains to data protection. ■