Pre-Implementation Strategy for Compliance with the CCPA and other Consumer Privacy Statutes

Ryan D. Levy & Dominic A. Rota

The current trends in information security and data privacy are (1) the growing consciousness surrounding the purported right to privacy of individuals, and their related information and data attached thereto, and (2) the unprecedented, continuous escalation in cyber-attacks, executed by nation-state (or nation-sponsored) organizations or rogue actors. While most businesses are aware of the high probability of a data breach and the necessary implementation of safeguards, businesses continue to struggle with the rapid changes in data privacy regulations, both domestically and abroad. Complicating matters further, much of privacy law within the United States is industry-specific, thereby requiring knowledge of a piecemeal set of laws: Federal Trade Commission Act ("FTCA"), Gramm-Leach-Bliley Act ("GLBA"), Health Insurance Portability and Accountability Act ("HIPAA"), Children's Online Privacy Protection Act ("COPPA"), Family Educational Rights and Privacy Act ("FERPA"), Electronic Communications Privacy, and state laws, such as the Tennessee Consumer Protection Act ("TCPA"). And now, qualifying entities must comply with the European Union's ("EU") General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"), both of which present all-encompassing, wide-sweeping privacy reform.

Since the GDPR took effect on May 25, 2018, many businesses have already experienced the harsh penalties of the EU's GDPR, for failure to ensure the privacy and security of consumer personally identifiable information ("PII"). Google experienced approximately $55 million in fines for a failure to obtain consent in personalizing advertisements. British Airways was fined approximately $200 million for a data breach of about 500,000 individual consumer records. And Marriott was required to pay approximately $110 million in fines for a data breach of approximately thirty (30) million individuals.

Mirroring the tenets of the GDPR, California became the first state to codify a comprehensive privacy regime with an expected implementation of the CCPA on July 1, 2020. As we anticipate California's final regulations, businesses have until the implementation date to achieve compliance.

Businesses should carefully consider if they fall within the anticipated legislative mandates of the CCPA. An organization is subject to the CCPA if the business (i) does business in the State of California, (ii) collects personal information of California-resident consumers; ***and*** (iii) satisfies any one of the following three: (a) has annual gross revenue in excess of $25 million, (b) annually engages in the sale of 50,000 or more California-resident consumers, or (c) derives fifty percent (50%) or more of its annual revenues from selling California-resident consumers' personal information.[1] Furthermore, the CCPA is anticipated to have a broad reach as it applies to *any* entity that controls, or is controlled, by a CCPA-covered business, or shares common branding with a CCPA-covered business.[2]

Upon determining whether the business falls within the ambit of the CCPA, businesses must then ascertain the personal data and information it collects, in conjunction with its legitimate business needs. Whereas most states define PII to include those conventionally covered items (e.g., name, address, social security number, driver's license), the CCPA's coverage is ***tremendously*** broad.

[1] *See* Cal. Civ. § 1798.140(c)(1).
[2] *See* Cal. Civ. § 1798.140(c)(2).

The statute defines PII as information that is reasonably capable of being associated with, or could be reasonably linked with, a particular consumer, such as (i) biometric information; (ii) geolocation data; (iii) internet or other electronic network activity information; (iv) audio, electronic, visual, thermal, olfactory, or similar information; (v) education information not covered under FERPA; and (vi) other information under which inferences could be drawn to create a profile about a consumer and its preference, characteristics, psychological trends, predispositions, behavior, intelligence, and aptitudes.[3] Thus, businesses will be tasked with the challenge of reviewing data collection protocols for both discrete, particularized identifiers and data pieces in which inferences can be drawn as to the identity of the California-resident consumer.

One noteworthy difference between the GDPR and the CCPA is the notice of privacy (or "information right") afforded to the California-resident consumer. Unlike the GDPR, which demands its covered entities to require consumers to *expressly* "opt-in" for the sale or use of personal information or data, the CCPA requires specific privacy notices, with a right to "opt-out" of the sale or use of information.[4] To provide a California-resident with the opportunity to *expressly* "opt-out," businesses must present to the consumer, in a form reasonably accessible to the consumer, the following: (i) a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information";[5] and (ii) a description of a consumer's rights under the CCPA.[6] Because many sophisticated business entities' "privacy policies" and "terms of use" are inadequate with respect the CCPA's prescribed disclosures, it will become incumbent upon businesses to review their privacy policies to ensure they have adopted and adapted language from the CCPA, with additional scrutiny as to whether the following data processes are sufficiently outlined and described therein: collection, automatic collection, retention, use, transfer, disclosure, and third-party facilitation.

Compliance with the CCPA will not be a one-stop check-box. It will require routine monitoring of all modifications to current data processing and security systems. More specifically, the CCPA requires covered businesses to ensure that California-resident consumers' requests to exercise their rights are acknowledged and resolved by an individual operating on behalf of the business. Following such a request, the CCPA demands that businesses neither continue to sell or use California-resident consumers' personal information nor discriminate against said California-resident consumers for exercising their statutory-afforded rights.[7]

As was the case with the enactment of the GDPR, businesses must achieve compliance *prior* to the implementation date of July 1, 2020. Regarding enforcement, the CCPA affords the State of California (and its injured residents) the ability to heavily penalize those organizations violating the CCPA. Fines for ***each*** violation include: (i) $2,500 for unintentional and $7,500 for intentional violations of the CCPA, wherein such action is brought by the California AG;[8] and (ii) the higher of $100 to $750 or actual damages, per incident/violation, wherein such action is brought by

[3] *See* Cal. Civ. § 1798.140(o)(1)-(3).
[4] *See* Cal. Civ. § 1798.120(a).
[5] *See* Cal. Civ. § 1798.135(a)(1).
[6] *See* Cal. Civ. § 1798.120(a)(2).
[7] *See* Cal. Civ. § 1798.125(a)(1).
[8] *See* Cal. Civ. § 1798.155(b).

California-resident consumers.[9] These fines can very quickly stretch into the millions of dollars, as these fines are imposed on a per-violation basis. Accordingly, a prospective approach is critical to avoid significant financial penalties.

Given that the CCPA is a fairly nascent statutory construct with no guidance as to the enforcement efforts of the State of California, the best practice is likely to adopt the "belt-and-suspenders" approach. This approach would generally include the following steps: (i) conducting an internal audit of the data collected, used, retained, or otherwise processed; (ii) making available on a business's website a clear and conspicuous link titled "Do Not Sell My Personal Information"; (iii) drafting (or re-drafting) a CCPA-compliant privacy policy; and (iv) constructing a routine monitoring program, wherein corporate counsel directs the organization to ensure that it has a program affording California-resident consumers the opportunity to exercise their rights afforded to them.

Going forward, businesses must continue to remain up to date on the regulations promulgated by the AG of the State of California. Following the implementation of the CCPA, businesses should carefully watch the enforcement efforts of the State of California and be aware of those statutory provisions and regulations most aggressively pursued by the AG. Lastly, businesses should remain abreast of the rise of legislation on information security and data privacy within the United States. Not only have some states enacted new laws enforcing consumer rights in data breaches (e.g., New York Stop Hacks and Improve Electronic Data Security Act), other states have promulgated legislation loosely modeled after the CCPA, including the Nevada Senate Bill 220 and the Maine Act to Protect Privacy of Online Consumer Information. Until uniform legislation is passed, businesses will have to pay close scrutiny to their use of individuals' information, as each individual will carry with it the tether of the state law governing its data privacy and consumer protection.

[9] *See* Cal. Civ. § 1798.150(a)(1)(A).