California Brings GDPR to the USA

Michael R. Cohen*
CIPP/US, CIPP/E
Gray Plant Mooty

80 South Eighth Street
500 IDS Center
Minneapolis, MN 55402

American businesses were just getting used to compliance with the European Union's General Data Protection Regulation (GDPR) when, on June 28, 2018, California Governor Jerry Brown signed into law the California Consumer Privacy Act (CCPA).

While the CCPA does not go into effect until January 1, 2020 and will likely be amended and modified, some form of the law will take effect in less than two years. Businesses who may have felt safe and immune from GDPR are now faced with getting ready for the American version.

Violating the CCPA exposes businesses to potentially large civil penalties and statutory damages. The CCPA authorizes a civil penalty of up to $7,500 per violation and will be enforced by the California Attorney General. The CCPA also includes a private right of action to Californians so we are likely to see class action lawsuits based on CCPA violations. This private right of action is a game changer when it comes to enforcement of data privacy and security laws.

California has always been the bellwether when it comes to data privacy law so the CCPA will heavily influence data protection practices nationwide. For a detailed and intriguing account of how the CCPA became law with little debate see https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html

What Steps Should a Business Take Now to Get Ready for CCPA?

Data Inventory – Perform data mapping as necessary to inventory the personal information collected on California residents, households, and devices. While the CCPA does not explicitly require businesses to maintain a data inventory, it will be practically impossible for businesses to comply with CCPA without one. Businesses will need a database that tracks all the business processes, third parties, products, devices, and applications that process California residents' personal data and keep it up to date as all of these things change.

Business Processes – Business processes may need to be re-engineered to function effectively once California residents start expressing their rights to opt out of data monetization and to delete their data. Some processes that inherently 'sell' data will need to be either discontinued or unwound so that opted-out consumers can continue to be served. Other processes that depend on consumer transactional data will need the 'delete' action designed so that system-critical, de-identified data is not also deleted.

Privacy Policy Updates – Businesses may have to update privacy policies with new disclosures regarding data access and deletion. CCPA requires notice to consumers and employees indicating the categories of personal information collected and the purposes for which they are used. The notice must explicitly indicate the categories of their personal information that are collected, disclosed, or 'sold'—using a broader definition of 'sold' than seen before—and that they have a new right to opt-out of this selling. Businesses may not collect additional categories of information or use information for additional purposes without providing consumers with an updated notice. Similarly, businesses may need to update their privacy policies to include a description of the other new consumer rights afforded by the CCPA. Before making these updates, businesses will need to step back and determine if they will maintain one privacy notice for California residents and one for everyone else, or stick with one unified notice.

New Disclosures and Right to Opt-Out

Consumers must be able to opt out of the sale of their personal information and businesses are required to notify consumers of this right. The opt-out notification must list the categories of information collected about consumers in the past 12 months and identify whether the business sells or discloses personal information. This will allow the CCPA to impact data collected before the 2020 enforcement date.

These disclosures must appear in the online privacy policy. Businesses must also provide a clear and

conspicuous link on their website that says "Do Not Sell My Personal Information." The link must allow consumers to actually opt-out of the sale of their personal information.

Right of Data Access and Deletion

Similar to the GDPR, CCPA states that consumers "shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected." The CCPA also gives consumers a broad license to request deletion without formally withdrawing consent for processing or satisfying any other contingencies. It states consumers "shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."

To comply with the CCPA businesses must disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer. Businesses may have to implement new systems and procedures for handling such data access requests from consumers.

Data Security – The CCPA, like the GDPR, requires covered businesses to protect personal data with 'reasonable' security. The Federal Trade Commission's enforcement of the FTC Act similarly holds businesses accountable to providing a reasonable standard of due care for the protection of personal data. In practice, this 'reasonable' standard has led businesses to take a risk-based approach toward addressing threats to the confidentiality, integrity, and availability of personal data.

CCPA and the potential of a private right of action escalates the need for remediating any gaps in data security. If "nonencrypted or nonredacted" California consumer information is compromised through a breach or some other unauthorized disclosure resulting from a failure of reasonable security, the CCPA allows for a legal action for statutory or actual damages.

The CCPA further promotes the need for incident response plans and teams as necessary to handle unauthorized access and potential data breach notification requirements.

Training and Awareness – CCPA compliance will require a team effort and is not the sole responsibility of legal or IT. Training and educating employees regarding any new systems or processes will be necessary. Because of the significant penalties allowed by CCPA, businesses may want to consider deploying a more robust training program as necessary to be ready in January 2020 for each relevant corporate function and line of business.

Strategic Decision-Making – The CCPA poses some strategic questions for businesses. Do they afford CCPA rights to only Californians, or do they offer the same enhanced rights to their entire base of customers, consumers, and employees? Is it more cost effective to offer a single level of service to everyone? If CCPA becomes the standard to be followed by other states does the business become an early adopter of these requirements? Consumer may expect to see these same or similar rights. Does CCPA compliance provide a competitive advantage in the marketplace by demonstrating robust data privacy and security compliance? Should a business wait until the CCPA is further amended or clarified by California legislators by January 2020 or start now by taking some of the steps noted above?

*Michael is a Principal and the Privacy Officer at the Gray Plant Mooty law firm. He is the primary author of ***A Legal Guide to Privacy and Data Security*** and holds CIPP/US and CIPP/E certifications from the International Association of Privacy Professionals in recognition of passing examinations in the areas of United States privacy laws and an advanced concentration in European data protection laws, standards and practices.