COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 2, Number 11. June 13, 2019
US data privacy law talks reveal key differences and similarities between US and EU data security interests

By Sascha Matuszak

2019 started off with a lot of movement in the United States data protection sphere. The California Consumer Privacy Act of 2018 (AB-375) (CCPA) completed its period for public comments in March, and both the U.S. House of Representatives and Senate held several meetings regarding a potential federal data privacy law and the role of the Federal Trade Commission (FTC).

The CCPA and the European Union's General Data Privacy Regulation (GDPR) set off a ripple effect that has spread across the globe — new data protection regulations of various stripes have appeared in India, China, Japan, Brazil and South Africa — but it is in the U.S. that the ripple effect may have the greatest impact. The world's economy flows through the U.S., and any federal data privacy regulation will have an enormous impact on how organizations around the world manage their data. As the hottest commodity of the 21st century, the implications of data protection regulations that are similar to GDPR, or modeled on the slightly less stringent CCPA, are extraordinary. For the big tech giants like Alphabet Inc.'s Google and Facebook, Inc., that have enjoyed incredibly lax enforcement of data privacy in the U.S., the future promises to be very different.

Supply chain managers and compliance and ethics professionals will have their hands full ensuring the technologists on the team are keeping ahead of the regulations wave. Data is in general considered to be an information technology department concern, but as data becomes currency, commodity and liability all at once, multiple teams and departments are being forced to cooperate and face the challenges ahead.

CCPA comments

The public comments on the CCPA span some 1,400 pages and cover several aspects of the law that the major stakeholders (i.e., businesses, non-profits and consumer advocates) hope to clarify or amend. Some of the more common comments include suggestions that the California Attorney General:

- Provide clarification on the interaction between the CCPA and the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act of 1998, California's Shine the Light law, and the Family Educational Rights and Privacy Act.
- Develop a uniform opt-out logo modeled on the AdChoices icon for the "Do Not Sell My Personal Information."
- Provide clarification on the record types that businesses need to maintain to demonstrate they have complied with the CCPA in the event there is an AG action.
- Provide clarification on how a business can verify a consumer request if it has extremely limited information on a consumer, such as only having a device identifier.
- Clarify what is and is not considered a sale of personal information.

Other more pointed comments — from Apple Inc., the Association of National Advertisers, and the Nonprofit Alliance, for example — delve into issues such as:

- The cost of compliance and its effect on non-profits exempt under the current law.
- The issue of "discrimination" and how companies can reward users who provide greater access to personal data.
- Refining the term "personal information" to take into account a wide variety of possible identifiers, uses and types of data.

The Future of Privacy Forum published their comments online, and provided a helpful comparison between the GDPR and CCPA and "A Visual Guide to Practical De-Identification."

The major points of the Forum's comments revolved around the "gray area" that exists between identifiable and non-identifiable information, the effect of the CCPA on medical research by non-HIPAA entities, and a refined data subject access request process.

The comments were solicited by the California Attorney General's office, pursuant to Section 1798.185 of the CCPA, which gives the attorney general authority to seek public comment and also issue regulations in the following areas:

- Categories of personal information.
- Definition of unique identifiers.
- Exceptions to the CCPA.
- Submitting and complying with requests.
- Uniform opt-out logo/button.
- Notices and information to consumers, including financial incentive offerings.
- Verification of consumer requests.

The comments are in, and the attorney general is tasked with implementing the law by early 2020. In the meantime, the U.S. Congress is mulling over how to strengthen the FTC and what exactly a U.S. federal data protection regulation should look like.