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.

One ring to rule them all?

On May 8, 2019, the House of Representatives Committee on Energy and Commerce held a hearing, "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security," that put in the spotlight the FTC's role in protecting data security. Committee Chairman Frank Pallone, Jr., provided a clear rundown of what the FTC is and is not empowered to do.

According to testimony given during the hearing, the FTC does most of its work investigating "unfair or deceptive acts or practices" under Section 5 of the Federal Trade Commission Act. The FTC also enforces a variety of more specific laws related to its consumer protection mission, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act. In total, its enforcement and administrative responsibilities derive from more than 70 laws. The committee came to the conclusion that the U.S. citizen is underserved by the current system.

"The FTC can and should be doing more to protect consumers, and Congress needs to give the FTC the tools it needs to be more effective," Pallone said. "That starts with resources. The FTC has fewer employees today than it did in the 1980s when the Internet did not exist. It has just 40 employees responsible for protecting the data of 300 million Americans. That's unacceptable – particularly when you consider that the United Kingdom, which has a much smaller population, has more than 500 people who protect the privacy and data of its residents. … The FTC also needs more authority to prevent privacy abuses from happening in the first place and to ensure that companies properly secure the personal data entrusted to them."

The scrutiny of the FTC comes as the commission is considering a landmark fine against Facebook, Inc. for violating a 2011 consent order by failing to protect the personal information of millions of users. The repeated breaches and failures to protect data, as well as the brazen commodification of personal data, has led U.S. politicians to consider an overhaul of the FTC in order to create a U.S. equivalent of the European Data Protection Board, the body that has the last say over GDPR matters.

The U.S. Senate on data protection

The U.S. Senate Committee on Commerce, Science, and Transportation (or the Senate Commerce Committee) also held several hearings on the topic of a federal data protection regulation:

- "Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act," in Oct. 2018.
- "Policy Principles for a Federal Data Privacy Framework in the United States," on Feb. 27, 2019.
- "Small Business Perspectives on a Federal Data Privacy Framework," on March 26, 2019.
- "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework," on May 1, 2019.

During the Feb. 27 hearing, Committee Chairman Roger Wicker reiterated the need for a federal data law and continued the thread of giving the FTC authority to regulate data privacy and protection:

> Congress needs to develop a uniquely American data privacy framework that provides consumers with more transparency, choice, and control over their data. This must be done in a manner that provides for continued investment and innovation, and with the flexibility for U.S. businesses to compete domestically and abroad. It is clear to me that we need a strong, national privacy law that provides baseline data protections, applies equally to business entities – both online and offline – and is enforced by the nation's top privacy enforcement authority, the Federal Trade Commission.

One of the most repeated concepts during these hearings is the concept of "consumer trust," and how that trust has been broken by the numerous data breaches in the last few years. In his statement prior to the May 1 hearing, Senator Wicker wrote, "Consumer trust is essential. To maintain trust, a strong, uniform federal data privacy framework should adequately protect consumer data from misuse and other unwanted data collection and processing."

The committee heard from many witnesses, including Helen Dixon, the commissioner of Ireland's Data Protection Commission. She made several interesting distinctions between the GDPR and the discussions revolving around a U.S. federal law, including the fact that the GDPR applies to "*any* organisation collecting and processing information that relates to an identified or identifiable person" (italics in original), and also a slight but perhaps significant difference in terminology: In Europe, the GDPR refers to the people covered by the law as "data subjects," whereas in the U.S. they are, as of now, referred to as "consumers."

"[Data subjects] is a concept far broader than consumers given that the GDPR concerns itself with any personal data processing and not merely that which occurs in commercial contexts," Dixon said.

This is an interesting difference, and one that may be part of the defining characteristics of a pending U.S. federal data protection regulation.

Takeaways

- There is strong bipartisan support for a United States federal data law that takes on aspects of the GDPR and the California Consumer Privacy Act of 2018.
- The Federal Trade Commission looks to become the top regulating and enforcement body for any U.S. federal data law that emerges.