COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 3, Number 1. January 09, 2020
California's privacy law went into effect Jan. 1; have you spoken to IT yet?

By Sascha Matuszak

California's new data privacy law went into effect Jan. 1, 2020, but the date is largely symbolic. Companies should already have a data management plan in place by now, as certain provisions within the new law call for companies to be able to provide data going back 12 months, and California's attorney general has stated that full enforcement will not be likely until after July 2020.

Since the California Consumer Privacy Act of 2018 (AB 375)[1] was passed in the summer of 2018, companies, interest groups, consumers and government actors have been discussing what the law actually does and how it will be enforced. Several amendments were passed in September 2019,[2] putting to rest a host of questions, but despite this and several public discussion forums,[3] companies' interpretations of the law and how to comply with it widely differ.

The problem with nonstandard application of the law rests on both sides. The law itself grants the courts and the attorney general broad freedoms to enforce it as they see fit, and several provisions within the law will be clarified through enforcement actions. The law grants consumers the right to request their personal data be deleted, for example, but also grants companies several exemptions to this clause, including a variety of business purposes that provide ample wiggle room.

This means companies are currently complyingas far as they feel they need to. Facebook, Inc. is punting compliance off to its many vendors, claiming it merely *provides access* to users' data through its targeted advertising service; and Evite has taken an aggressive approach to compliance by giving users information and quick access to choices on how their data is collected and shared.[4]

Read the law, talk to IT

This bill grants Californians the right:

1. To know what personal information is being collected about them.
2. To know whether their personal information is sold or disclosed and to whom.
3. To say no to the sale of personal information.
4. To access their personal information.
5. To equal service and price, even if they exercise their privacy rights.[5]

The full text, as amended, of the California Consumer Privacy Act of 2018 is available online. It is not a long document and includes a list of definitions that help to clarify several misconceptions. The regulatory burden is not enormous, the fines are reasonable and easily avoided, and the consumer's right to file a lawsuit is limited. It

is not hard to understand the five basic rights granted to Californians under this law and why those rights are important in the digital age.

The real burden is the cost of gaining control over data flows. For-profit organizations doing business in the U.S. have enjoyed more or less free rein with personal data, which, together with powerful data mining and collection tools, has led to petabytes of personal data being stored, managed and analyzed on servers and then shared into a more or less unregulated third-party ecosystem. Companies are now being asked to meticulously map those flows and be able to reproduce them when asked, within a certain time frame.

This quote from a CSO article hints at the challenge:

> "Most file search tools lack the ability to search across the modern file repository ecosystems so prevalent today," says Aaron Ganek, CEO of Cloudtenna. "Cross-silo file management is a major challenge. It is difficult to understand context for each file if they are scattered inside different repositories." Plus, compliance issues are associated with pulling together data, he says. "Legacy enterprise tools struggle to observe the disparate permissions and security models, violating the very laws and regulations they're being used to satisfy."[6]

As we have discussed before in regard to data transparency[7] and the role of artificial intelligence in supply chains,[8] the real challenge going forward is not regulatory compliance as much as the technical ability to comply, and what those solutions might look like.

Waiting for that big case

California Attorney General Xavier Becerra told National Public Radio that although he won't enforce the law until July of 2020, he considers it in effect as of Jan. 1. It seems as if the attorney general will seek out big cases to send a message, rather than seek to enforce every possible violation, no matter how small:

"[T]he bigger the company, the bigger the problem," Becerra said. "The bigger the universe that has data that is used in certain ways, that could lead to that violation, the bigger the case will be."[9]

Like the EU's tactic with the GDPR,[10] California's authorities may choose to take on big players such as Facebook, Alphabet Inc.'s Google or Amazon. Forcing those major companies to ensure data transparency will have downstream effects that could, eventually, create global standards for the digital world that companies, consumers and public officials are hoping for.

Takeaways

- California's data privacy law presents a formidable challenge for companies in the business of collecting and sharing data: gaining transparency over data flows.
- It's likely that big cases in the courts will do more to decide what standards will be enforced than guidance, public commentary or lobbying.

1 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 to 1798.199 (West 2018), http://bit.ly/2sAsI2P.
2 Sascha Matuszak, "California legislature passes key privacy law amendments," *Report on Supply Chain Compliance* 2, no. 18 (September 26, 2019), http://bit.ly/2QAt8xY.

3 "Background on the CCPA & the Rulemaking Process," California Consumer Privacy Act (CCPA), State of California Department of Justice, accessed December 31, 2019, http://bit.ly/2QzqbxM.
4 Natasha Singer, "What Does California's New Data Privacy Law Mean? Nobody Agrees," *The New York Times*, December 29, 2019, https://nyti.ms/2teT4az.
5 Assemb. B. 375, (Cal. 2018), http://bit.ly/2rEIcSS.
6 Maria Korolov, "California Consumer Privacy Act (CCPA): What you need to know to be compliant," *CSO*, October 4, 2019, http://bit.ly/2Qc5Iju.
7 Sascha Matuszak, "Supply chain mapping and the transparency wave of the future," *Report on Supply Chain Compliance* 2, no. 19 (October 10, 2019), http://bit.ly/2BkUWiW.
8 Sascha Matuszak, "AI solutions for supply chains," *Report on Supply Chain Compliance* 2, no. 23 (December 12, 2019), http://bit.ly/2F40xMk.
9 Rachael Myrow, "California Rings In The New Year With A New Data Privacy Law," *NPR*, December 30, 2019, https://n.pr/2MLnjwC.
10 Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. L119.