CCPA: How to Prepare for California's New Privacy Law Before Enforcement Starts July 1
TechRepublic
Veronica Combs
June 19, 2020
[Link]

Companies need to look for PII across all corporate data silos and consider building an automated system to respond to requests from consumers, experts say.

For businesses preparing to comply with California's new data privacy law, the first challenge is figuring out how much data is covered by the law. The next is collecting all of that information in one place.

California's attorney general, Xavier Becerra, will start enforcing the California Consumer Protection Act law on July 1. Companies have to provide residents of the state with a copy of any personal data they have and show that they are taking reasonable security measures to protect that data.

Christine Lyon, a partner at Morrison & Foerster and a member of the firm's global privacy and data security group, said that the CCPA establishes a new right that US consumers have never had.

She also said that the data protected by the CCPA includes much more than just email address and name.

"That makes it challenging for companies because they have a CRM database with PII in it but they may well have other data sets about preferences or buying history and they have to pull all of the relevant information," she said. "It's often in different databases and no one anticipated having to pull a copy when these systems were built."

Jon Mendoza, the field CTO for Technologent, used the example of a sales person's digital Rolodex as data that could be governed by the CCPA.

"You would think that information that people use for relationship building—birthdates or a spouse's name—would be innocuous, but if you don't secure it and the account gets compromised, the employer could be liable for the breach," he said.

The CCPA requires companies to acknowledge receipt of requests from consumers and be ready to honor requests to not share data and even delete it. The CCPA applies to companies with $25 million in annual revenue and corporations that make money from buying or selling personal information.

The law creates two penalties for mismanagement of consumer data. Individuals can file a class-action lawsuit or the state attorney general can bring an action against a company with fines ranging from $2,500 to $7,500 per violation. Consumers don't need to show actual damages to receive compensation ranging from $100 to $750 per violation.

To comply with the law, Mendoza said that companies should be identifying what data is sensitive and then locating it.

"You can't secure something if you don't know where it is," he said.

Lyon said that companies also have to figure out how to verify the identity of the person making the request for the data.

"Companies might be thinking about something that only this person will know, the date of your last transaction, or other information that isn't easily guessable by someone else," she said.

Lyon said that some larger companies have been building portals and other automated systems to automate consumer requests for personal data.

"Companies that anticipate receiving large volumes of requests know the process should be self-service," she said.

California residents are entitled to a printed or electronic copy of the data report and the electronic copy must be portable and machine readable.

Lyon also said that there is some ambiguity about the exact definition of "doing business in California," which determines whether a company is subject to the law.

"Just selling products might not be enough to qualify, it might be more about having a presence there or targeting customers in California," she said.

Lyon said that complying with the CCPA will be the most challenging for companies in non-regulated industries that have never had to consider securing and providing access to consumer data.

"The more data you have, the more challenging it is to comply, so there will be a lot of operational changes for companies that have never had to deal with this," she said.

How to prepare for the CCPA

The law does not specify what kind of security measures companies should take to protect data, so Mendoza recommends that clients follow the top 20 CIS security controls. Technologent is a value-added reseller and solution provider, specializing in infrastructure, data center, cloud and cybersecurity work.

"Following the top 20 controls sounds simple but you have to make investments and prioritize," he said.

While working with companies preparing to comply with the CCPA, Mendoza said he has identified three approaches to the new requirements. Some companies are already ahead of the game because of the financial impact of a class-action lawsuit.

"Also, if you're transacting business online, you have to preserve trust with your customers and optics plays a big role in that," he said.

Another set of companies is doing what they can without spending too much money.

"These companies have the security basics down and they are rationalizing their sensitive data," he said.

The last group of organizations are taking a wait and see approach and hoping that the law may not apply to their business.

Mendoza recommends that companies take these three steps to prepare for data requests from consumers:

- Rationalize company data
- Improve security and data management tools
- Educate users about new requirements

"Security is not necessarily tool-centric, the tools are only as good as the people using them," he said.

Mendoza said that companies also need to include all elements of the supply chain in this data review.

"If you have company information that traverses through partners, it could be sensitive, so the whole supply chain that needs to be accounted for," he said.

Lyon expects the privacy law and the new rights it establishes to expand over the next several years.

"This should encourage companies to be even more thoughtful about collecting data and to consider how long they keep it," she said.

Data privacy rights are limited in the US

Only three states have laws that protect consumer data: California, Nevada, and Maine. Fifteen states have pending legislation.

Security.org has a report on privacy rights by state and lists these 15 principles as the most common digital privacy provisions:

1. Right of access & information: Consumers should be informed of what information businesses or data collectors are gathering about them, and they should be able to access the information or categories of information as well as accessing names or categories of third parties who received the shared information.

2. Right of rectification: Consumers should be able to request corrections to outdated or incorrect personal information.

3. Right of deletion: Consumers should be able to request that personal information be deleted in certain conditions.

4. Right to restriction of processing: Consumers should be able to restrict a company's ability to access their personal information.

5. Right to data portability: Consumers should be able to request their information be disclosed in a common file format.

6. Right to opt-out of sale of personal data: Consumers should be able to choose not to have their personal information sold by the collector to a third party.

7. Right against automated decision-making: Businesses should not make decisions about consumers based on an entirely automated process that has no human input.

8. Right of action: Consumers should be able to seek civil damages from a business that violates privacy statutes.

9. Age-based opt-in: Business must default to strict opt-in for sale of personal information for consumers under a certain age.

10. Transparency requirements: Businesses must provide notice to consumers about their data practices and privacy programs.

11. Data breach notification: Businesses must notify consumers or enforcement authorities in the event of privacy or security breach.

12. Risk assessment: Businesses must conduct formal risk assessments of their established security and privacy practices.

13. Non-discrimination: Businesses are prohibited from treating a consumer differently if they exercise data privacy rights.

14. Purpose & processing limitation: Businesses must collect and process consumer data only for a specific purpose.

15. Fiduciary duty: Businesses must act in the best interest of the consumer.

The Security.org report found that as of April 2020 no state has a law on the books that covers all 15 areas. A bill pending in the New York legislature covers 12 of the 15 areas.

CCPA covers only eight of the 15 and does not address the right of rectification, a restriction of processing, a ban on automated decision-making, data breach notification, risk assessment, purpose and processing limitations, and fiduciary duty.

Lyon said that data privacy advocates in California have already decided that the CCPA is not sufficient and are collecting signatures on a new ballot initiative to strengthen data privacy rights.