



Data Privacy Detective Podcast – Episode 23 – California’s New Data Privacy Law

Jul 09, 2018

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

With the support of large tech firms and privacy advocates, statute AB 375 moves California in the direction of the European Union, granting rights to California consumers concerning the personal information they share online. The Data Privacy Detective turns his glass on this new statute. It will have an impact. If California were a country, it would boast the world’s fifth largest economy.

California has citizen initiative rights that let people propose laws enacted by a popular vote, bypassing the legislature. A wealthy Californian, enraged by the Cambridge Analytica scandal over data shared by Facebook and eventually sold without consumers’ direct knowledge for political campaign purposes, tired of waiting for the legislature to act. He promoted an initiative aimed at creating tough consumer data privacy protections. Alarmed by the proposal, California’s large tech community backed a quick legislative response that is a compromise compared to the initiative’s language. The statute was drafted, enacted, approved and signed into law in about a week, and the initiative leader withdrew his effort and supported the outcome. See www.caprivacy.org.

The California Consumer Privacy Act of 2018 will not become effective until January 1, 2020. Before then the California Attorney General must issue regulations, and there will probably be legislative fixes to some rushed language. But the new law upgrades protection for online consumers’ data and is more similar to than different from principles of the EU’s General Data Protection Regulation (GDPR), which became effective in late May of 2018.

The statute gives California consumers – defined as residents of California on a broadly detailed basis – access to, and controls over, their personal data shared online, including:

- Right to know what personal information is being collected and used.
- Right to know whether their information is being sold or shared with others.
- Right to refuse the sale or transfer of personal information.
- Right to access, correct or have deleted personal information.
- Right to equal service and price if they refuse the sale of personal information – more on that later!

To comply, businesses subject to the law must take the following steps by January 1, 2020:

- Provide particular notices to consumers before collecting personal information about what data will be collected and how data will be used.
- Establish a process to respond to “verifiable consumer requests” to access personal information a business collects about a consumer.
- Respond to consumer requests for correction or deletion of personal information, with stated exceptions.
- Permit consumers to refuse (opt out of approving) sale of their personal information, with certain exceptions related to data sharing and other details.
- Refrain from selling to third parties personal information of consumers who have refused it.
- Update websites to have a link to a page called “Do Not Sell My Personal Information” and with specific privacy policy disclosures.
- Include a disclosure of consumer privacy rights updated annually.
- Include certain specific terms in contracts with business subcontractors.

What businesses are subject to the new law? There are three defined **alternative** thresholds – generally businesses that have any of the following:

- \$25 million of California-connected gross revenue.

- Possession of personal information of more than 50,000 California consumers.
- 50% of gross revenues derived from the sale of personal information.

Attention to the statutory details of these thresholds is essential for businesses outside of California to assess their need to comply with California's rules.

The provision that prevents a business from charging more for its goods or services to a consumer that refuses to let the business sell the consumer's personal information is balanced by a right not found in GDPR – that is, the right for businesses to offer incentives to consumers who permit the sale of their personal information. This provision will lead to creative thinking about how businesses present such "incentives" or extend "discounts" encouraging people to approve the sale of their personal information, yet without infringing the principle of equal pricing and access to goods and services for consumers who refuse such permission.

When effective in 2020, enforcement of the statute will be the responsibility of the California Attorney General or result from direct claims by affected consumers, with \$7,500 in statutory damages provided for violations. One such violation involves the failure of a business to use reasonable security measures to safeguard personal information of consumers, resulting in unauthorized access or infiltration, theft or disclosure of non-encrypted or unredacted consumer personal information.

California's statute is not an overarching general data protection statute like the GDPR, and it builds on a two-decade history of privacy innovation in California. Still, many of the provisions express basic principles found in the GDPR and a growing number of other countries' data privacy laws, including:

- Right to be informed about collection and use of personal data.
- Right of access, correction and deletion of personal information.
- Right to refuse the use and sale of personal information.

- Right not to be subjected to unwarranted automated decision-making and profiling.

Absent an overarching U.S. federal statute on data privacy – protecting all persons, not only online consumers – California’s new statute demonstrates the strength of the U.S. federal system in allowing states to experiment and develop laws that fit their populations. And given the size and importance of California’s economy, as well as the leadership of its tech community, other U.S. states are certain to consider the new statute carefully, with an eye toward adopting some or most of its provisions.

For more information, please contact [Joe Dehner](#) or any attorney in Frost Brown Todd’s [Privacy and Information Security Law Industry Group](#).

To share your thoughts or questions about this or other Data Privacy Detective podcasts, send a message to info@thedataprivacydetective.com. And remember – protecting your personal information begins with you.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.