

Privacy Bill Essentials: Oklahoma

Privacy, Cyber & AI Decoded Alert | 3 min read

February 23, 2021 | Updated May 13, 2021

**Update - The Oklahoma Data Privacy Act has died in committee. The Senate Judiciary Committee did not meet the April 8, 2021 deadline to pass bills out of committee for the Data Privacy Act. The Act was last referred to the committee in March and has not progressed further. As a result, the bill will not be passed at this time.*

The recently introduced [Oklahoma Computer Data Privacy Act](#) (OCDPA) is one of the nation's first "opt-in" proposed data privacy laws. The law would require businesses to obtain consent before collecting and selling consumer personal information and create a private right of action with potentially steep statutory damages.

To whom would it apply?

The OCDPA would apply to businesses that:

- Do business in Oklahoma;
- Collect consumers' personal information or have that information collected on their behalf;
- Alone or in conjunction with others, determine the purpose for and means of processing consumers' personal information; and
- Satisfy specified financial and business thresholds.

What types of information would it cover?

The OCDPA covers a wide range of personal information collected by businesses. This includes information that could be used to identify a person; personal characteristics; commercial information; biometric information—which includes DNA, sleep and health information, and images of an iris, retina, face, or fingerprint; internet network information; geolocation data; employment-related information; financial information; medical information; and health insurance information.

What rights would it create?

Businesses would be permitted to offer a financial incentive for the collection and sale of personal information. If a consumer enrolls in a financial incentive program, the business must provide a clear description of the material terms of the program, obtain opt-in consent, and permit the consumer to revoke consent at any time. Any attempt to waive or limit these rights through contract provisions would be unenforceable as against public policy.

Along with the right to opt-in to the sale of personal information, consumers could request deletion of their personal information, and request a report containing (1) the categories of personal information collected, sold, or disclosed about them for business purposes; and (2) the categories of third parties to whom that information that was sold or disclosed. Businesses would have 45 days to provide the report or to notify the consumer that additional time is needed, providing the reason for the delay.

What obligations would it impose?

Covered businesses would be required to provide notice on their website that: (1) the information may be sold; (2) identifies the persons to whom the information will or could be sold to; (3) the *pro rata* value of the information; and (4) the consumer's right to opt-in to the sale of personal information.

OCDPA aims to make the opt-in process as seamless as possible by requiring businesses to provide a clear and conspicuous opt-in link and by not requiring consumers to create an account in order to opt-in. Businesses would also be required to implement and maintain "reasonable security procedures and practices" to protect personal information.

How would it be enforced?

The Oklahoma Corporation Commission would be required to adopt rules necessary to implement, administer, and enforce the OCDPA, and would be authorized to seek injunctive relief and fines up to \$2,500.00 for negligent violations. If the violation is intentional, a fine of \$7,500.00 per violation is authorized. The commission would also be entitled to recover reasonable expenses, including attorney fees and court and investigatory costs.

Notably, the OCDPA also creates a private right of action for any violation, allowing recovery of statutory damages of \$2,500.00 for each negligent violation or \$7,500.00 for each intentional violation.

Where does it stand?

This bipartisan legislation unanimously passed the House Technology Committee and is now eligible to be heard on the House floor.

Related Capabilities

Data Privacy, AI & Cybersecurity