NCSL

LegisBrief

A QUICK LOOK INTO IMPORTANT ISSUES OF THE DAY

FEB 2019 | VOL. 27, NO. 7

Did You Know?

- Data privacy and data security are two sides of the same coin. Generally, privacy is about controlling who has access to personal information, and security is about protecting that information from unauthorized access.
- There are several voluntary frameworks for protecting consumer data privacy, including the Information Technology Industry Council Framework to Advance Consumer Privacy, the Network Advertising Initiative and one in development from the National Telecommunications and Information Administration.
- The Federal Trade Commission (FTC) and state attorneys general can bring legal actions against entities that tell consumers they will safeguard their privacy and then fail to do so.

A Higher Profile for Data Privacy

BY PAM GREENBERG

Protecting consumers has long been a priority in state legislatures, and protecting individual privacy is part of that tradition. Even so, neither state legislatures nor the federal government has in place a single, comprehensive privacy law. Recent developments in Europe and California, however, have focused new attention on the privacy and security of personal information in the U.S.

Privacy regulation in the U.S. is based on a sectoral approach: Current privacy laws apply to financial and health information, children's privacy and many other areas. Also, states historically have offered more privacy protections than the federal government, particularly states with privacy clauses in their constitutions, which provide an additional overlay of protection for citizens in those states.

This piecemeal approach to data privacy would likely have continued for some time in the U.S., except that in May 2018, Europe's General Data Protection Regulation (GDPR) took effect, extending European Union jurisdiction beyond those countries. Any global business that sells to or has European Union customers is subject to the GDPR, regardless of where that business is based. The GDPR sets forth rules about how companies treat the personal data of EU citizens, even those purchasing U.S. products or services or living in the U.S. The rules are most conspicuously evident in the notifications about the use of "cookies" that recently began appearing on websites.

State Action

■ **California's Consumer Privacy Act.** Just as the GDPR began taking effect, privacy advocates in California had gathered enough signatures for a stringent privacy act to qualify for the November 2018 ballot. The backers of the initiative, however, agreed to keep it off the ballot after the Legislature introduced a similar proposal: the California Consumer Privacy Act of 2018. It passed quickly in June, was amended in September, and will become effective Jan. 1, 2020 (with possible additional amendments in 2019).

The new California law would constitute one of the broadest online privacy regulations in the U.S., affecting businesses across the country. The law, which applies to California residents:

- Allows consumers the right to request a business to disclose the categories and specific pieces of personal information that have been collected about them, as well as the source of that information and the purpose for collecting it.
- Gives consumers the right to request a business' sale of their personal information without being discriminated against for opting out.
- Allows consumers to ask businesses to delete personal information that has been collected from them.
- Provides for enforcement by the state attorney general and for a private right of action in certain cases of unauthorized access, theft or disclosure of a consumer's personal information.

■ **Other State Digital Privacy Laws.** California was the first state to enact several digital privacy laws. The Online Privacy Protection Act (CalOPPA), for example, requires websites and other online services that collect personally identifiable information from California residents to post and comply with an online privacy policy. Although specific provisions differ, Connecticut, Delaware, Nevada and Oregon also have laws expressly requiring websites or online services that collect personal information to have or abide by online privacy policies.

The Privacy Rights for California Minors in the Digital World Act, also known as the Online Eraser Law, allows Californians under 18 to request removal of their own social media or other online postings that they later regret having shared. It also prohibits websites or online services catering to children from advertising products or services that minors are legally prohibited from buying or are based on personal information collected about a minor. Delaware passed a similar law in 2015.

A 2018 Vermont law requires data brokers (businesses that collect and sell or license personal information to third parties) to disclose to individuals which data is being collected and to permit them to opt out of the collection. Other states are exploring legislative action on the issue during current sessions as well.

Other types of state data privacy laws include those regulating wiretapping/eavesdropping; restricting location tracking and using data collected by automated license plate readers and event data recorders in cars; and protecting social security numbers, biometric or health information, employee and student social media passwords, and other student data.

NCSL also tracks laws and legislation related to cybersecurity and data security, data breach notification, computer crime and other security-related issues.

Federal Action

California's Consumer Privacy Act has prompted new calls for a comprehensive federal data privacy and security law. Some of these proposals would give the FTC greater jurisdiction over data privacy standards, and state pre-emption at some level is a possibility. Bills to be considered in Congress include the Data Care Act, the Consumer Data Protection Act, the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act and the Information Transparency and Personal Data Control Act. Other data privacy and security bills are likely to be introduced this year as well.

Additional Resources

- NCSL Data Privacy and Security Resources
- NCSL State Laws Related to Internet Privacy
- Managing Your Privacy, Stay Safe Online

NCSL Contact

Pam Greenberg
303-856-1413

Abbie Gruwell
303-856-1413