Connecticut's New Data Privacy Law and the Proposed Federal Law that Could Preempt It

BY DENA M. CASTRICONE

PROTECTING PERSONAL INFORMATION is important to all Americans. In the absence of a comprehensive federal privacy law (the US is one of the few remaining countries without one), states are stepping up. Five states have adopted comprehensive privacy legislation: California, Colorado, Connecticut, Virginia, and Utah. And more than half of the country's state legislatures have considered such measures over the past year.

States serving as incubators of privacy legislation certainly encourages innovation and creativity, but it also produces differing rules among the states. The resultant patchwork of laws make compliance difficult and cause confusion about applicable rights and standards. While there are similarities in the state laws, many of the rules in California are different than those in Connecticut, Virginia, or Colorado (each of which have their own nuances) and Utah is distinctly different.

The prospect of a comprehensive federal privacy law that establishes a national standard seemed a remote possibility until recently. A privacy bill with bipartisan support awaits consideration on the House floor in Congress. While the bill faces an uphill battle this year, the proposal brings the prospect of a federal privacy law much closer to reality. It also could mean the end of the newly enacted Connecticut law before it even takes effect.

I. Connecticut's Data Privacy Act (CTDPA)

After failed attempts in years past, on April 28, 2022, Connecticut became the fifth state to pass a consumer data privacy bill. The governor signed *An Act Concerning Personal Data Privacy and Online Monitoring*[1] (CTDPA)[2] on May 10, 2022. The CTDPA enjoyed bipartisan support, passing unanimously in the Senate and by a vote of 144-5 in the House.

Learning from the failed attempts, the bill's primary sponsor, Senator James Maroney, built a coalition and reworked the bill's language with input from all stakeholders. The result: a consumer protection law that balances the rights and obligations of consumers and businesses. While not perfect, the CTDPA is a good starting point for a data privacy law.

Modeled primarily after the Colorado and Virginia laws, the CTDPA also adopted some concepts from the more protective California law and from Europe's General Data Protection Regulation (GDPR). Additionally, the CTDPA contains some unique characteristics not yet seen in any of the other state laws.

A. Effective Date and Scope

The CTDPA takes effect on July 1, 2023. Similarly, the data privacy laws in Colorado, Virginia, and Utah take effect in 2023, as does the California Privacy Rights Act, which replaces California's current privacy law. In other words, all five states have effective dates for new or revised privacy laws in 2023.

Who must comply with the CTDPA? It applies to individuals or legal entities doing business in Connecticut or producing products or services targeted to Connecticut residents if they meet either of the thresholds below. In the previous calendar year, they controlled or processed the personal data of at least:

- 100,000 Connecticut residents, excluding data used solely for completing a payment transaction ***OR***
- 25,000 Connecticut residents and derived more than 25 percent of gross revenue from the sale of personal data.[3]

"Personal data," under the CTDPA means "any information that is linked or reasonably linkable to an identified or identifiable individual." It is a broad definition; however, it does not include de-identified data or publicly available information.[4]

Significantly, Connecticut is the only state to exempt data used solely for completing a payment transaction. Small retailers and

Image credit: DrAfter123/Digital Vision Vector


01$
11001
10$11$100
0
1011101
10111101
$0101111
110$11

restaurants lobbied for the addition as many of their businesses collect no other personal data.

B. Exemptions

The CTDPA has extensive exemptions at both an entity level and a data level. The following entities do not need to comply with the CTDPA: the state or its agencies, non-profits, institutions of higher education, national securities associations registered under 15 U.S.C. 78o-3 of the Securities Exchange Act, financial institutions subject to the Gramm-Leach Bliley Act, and covered entities or business associates under the Health Insurance Portability and Accountability Act (HIPAA).[5]

There are also 16 data-level exemptions, including categories of data including financial, health, and educational information protected under other laws, research information, and employment information as well as others.[6]

The laws in California, Colorado, Virginia, and Utah also offer numerous exemptions.

C. Consumer Rights

The CTDPA provides five consumer rights that are largely in line with most data privacy laws.[7] Those rights are:

1. Right to Know and Access. This allows a consumer to confirm whether or not a business is processing the consumer's personal data and to access that data;
2. Right to Correct. A consumer has the right to correct inaccuracies in the consumer's personal data;
3. Right to Delete. A consumer has a right to have personal data provided by or obtained about the consumer deleted;
4. Right to Portability. This allows a consumer to obtain a copy of their personal data and transmit it elsewhere; and
5. Right to Opt-Out. A consumer has the right to opt-out of the processing of the personal data for purposes of (A) targeted advertising, (B) selling the data, or (C) profiling that can adversely affect the consumer.

D. Business Obligations

Businesses subject to the CTDPA must take the following steps to ensure protection of consumers' personal data:[8]

- Provide consumers with "a reasonably accessible, clear and meaningful privacy notice" outlining the data that is collected, used, and shared and how consumers can exercise rights.
- Limit the collection of personal data to what is necessary and use it only for the purposes disclosed in the Privacy Notice unless the consumer consents.
- Implement reasonable data security safeguards to protect the confidentiality, integrity, and accessibility of personal data.
- Do not process sensitive data[9] without the required consent.
- Provide an effective mechanism for consumers to exercise rights.
- Do not sell or use for targeted advertising the personal data of minors ages 13 to 15 without consent. This requirement extends the existing rules under the federal law that protects children under the age of 13.
- Conspicuously disclose the sale of personal data or processing for targeted advertising and provide an opportunity to opt-out (including the acceptance of a global opt-out signal by January 1, 2025).
- Do not discriminate against consumers for exercising rights.
- Engage in contracts with contractors that will process personal data on behalf of the business.
- Perform a data protection assessment for processing activities that present a heightened risk of harm to the consumer.

E. Enforcement

The Connecticut Attorney General's office will enforce the CTDPA.[10] Unlike other states, there is no minimum or maximum penalty, but any violation will constitute a violation of the Connecticut Unfair Trade Practices Act.

For the first 18 months, if a violation of the CTDPA can be cured, the attorney general's office must provide the business 60 days to remedy the violation. After January 1, 2025, the attorney general's office may grant an opportunity to cure in its discretion and it may also engage in multijurisdictional enforcement with California and/or Colorado.

Finally, like the other state laws,[11] there is no private right of action for a violation of the CTDPA.

II. A Proposed Federal Law that Could End the CTDPA before it Starts

Less than a month after the governor signed the CTDPA, a discussion draft of the proposed federal American Data Privacy and Protection Act (ADPPA) surfaced on June 3, 2022. It took many (including me) by surprise. Lawmakers formally introduced the bill in the House of Representatives on June 21, 2022.[12]

I had not expected any push for federal privacy legislation this year and I certainly did not expect a bipartisan proposal. Not only does the ADPPA have bipartisan support, but it is vastly different than the other state laws and would preempt most of them, including the recently enacted CTDPA.

A. A Bipartisan/Bicameral Attempt

The ADPPA is the first proposed federal data privacy bill with bipartisan and bicameral support (Representatives Frank Pallone Jr. (D-NJ), Cathy McMorris Rodgers (R-WA), and Senator Roger Wicker (R-MS)). Notably absent from support is Senator Maria Cantwell (D-WA), a leader in the Senate who has previously proposed data privacy legislation and has expressed concern that the ADPPA does not provide enough protection.

Despite the lack of support from Senator Cantwell, after a markup session, the House Committee on Energy & Commerce voted 53-2 to send the bill to the House floor. All sides made concessions to create legislation that could succeed and resolved to not let perfect be the enemy of good.

Federal lawmakers found common ground on the most contentious issues: preemption and private right of action. Generally, Republican law makers want preemption and not a private right of action and the reverse is true for their Democratic counterparts. The ADPPA splits the baby. It preempts most state laws and allows for a private right of action. More on both below.

The House is not in session again until September, and given the proximity of the mid-term elections, many question whether the ADPPA will receive consideration this year. Even if it does not, we likely will see this bill again in one form or another.

B. The ADPPA Is Different and More Protective than State Privacy Laws

While the ADPPA provides consumer rights and imposes business obligations similar to those in the five states, it offers greater overall privacy protections than any of the state laws. The ADPPA is also structured differently. Transparency and consent are the focus in the state laws. On the other hand, the ADPPA recognizes that bombarding consumers with notices that most will never read does not protect information. Rather, the ADPPA does not permit the collection or processing of data except as necessary to provide a product or service or as otherwise permitted under the ADPPA.[13]

This approach is more like Europe's GDPR. It is more protective of consumers because it provides clearly defined boundaries.

Critically important is the fact that the ADPPA is broader in scope than the state laws, which all offer significant exemptions. The ADPPA recognizes only a few entity-level exemptions, including governmental entities and entities Congress designates to protect victims, families, and children.[14] The ADPPA would apply broadly to businesses, nonprofits and common carriers regardless of size or complexity of operations.[15]

While size will not exempt an entity, it certainly will impact compliance requirements. The ADPPA would hold massive data holders and social media giants to a higher standard than smaller companies.[16] It also requires data brokers to register with the Federal Trade Commission (FTC) and provide special notices to consumers.[17]

Further, the ADPPA would more aggressively protect minors.[18] The bill prohibits targeted advertising to a minor under 17 years of age. It also prohibits data transfers relating to a minor under 17 years old without affirmative express consent. While the bill requires that the covered entity have knowledge that the minor is under 17, it defines knowledge differently for large data holders and social media giants than for others.

C. The ADPPA Would Preempt Most State Privacy Laws

Generally, the ADPPA would preempt any state law that addresses issues covered by the ADPPA or its regulations.[19] The bill carves out 16 categories of exceptions to the preemption rule, including data breach notification laws, Illinois' Biometric Information Privacy Act, and California's private right of action for data breach victims. Further, the bill specifically recognizes the California Privacy Protection Agency, established under California's privacy law, and empowers it to enforce the ADPPA in the same manner it would have enforced the California law.

Preemption is a divisive issue. Those in favor of preemption generally want a single federal standard to govern privacy instead of a patchwork of state laws, which can make compliance difficult. For that reason, the business community strongly supports preemption.

Those opposed to preemption are concerned that a federal law cannot remain nimble enough to keep up with changes in technology and believe that a federal law should serve merely as a floor for protection, not a ceiling. They believe that states are in the best position to quickly pass legislation needed to address unanticipated changes and new developments in technology. Recently, 10 state attorneys general, including Connecticut's Attorney General Tong, wrote to Congressional leaders emphasizing this point.[20]

D. Enforcement of the ADPPA Would be a Team Effort

The ADPPA envisions a three-pronged enforcement strategy: (1) the Federal Trade Commission through a newly created Bureau of Privacy; (2) State Attorneys General; and (3) individuals through a private right of action, which will not be available until two years after the ADPPA's effective date.[21] Violations of the ADPPA would be deemed an unfair or deceptive act or practice under the Federal Trade Commission Act (FTCA).

A commonly cited ADPPA concern relates to resources for enforcement. Given the breadth of the bill and the lack of current structure and sufficient resources within the FTC to handle enforcement, weak enforcement could take the bite out of the ADPPA.

Additionally, many point to the ramp-up time for the FTC, the time-consuming rule making process and the two-year delay of the private right of action as creating a problematic gap in enforcement. Notably, state privacy laws would be preempted six months after the ADPPA is signed into law leaving a sizable gap in any effective privacy law enforcement efforts on the state or federal level.

E. Small Business Protections

Entities with annual gross revenues of less than $41 million in the last three years may be eligible for some exemptions to certain ADPPA requirements if they meet two additional requirements.[22] First, the entity must not collect or process the data of more than 200,000 individuals for a purpose beyond processing payment. Second, the entity cannot receive more than 50 percent of its revenue from transferring covered data.

If those criteria are met, then the qualifying entity would have more flexibility with respect to certain consumer rights and less onerous data security, privacy impact assessment, and other obligations.

Importantly, smaller entities with annual gross revenues under $25 million that collect the data of fewer than 50,000 individuals and derive less than 50 percent of revenue from transferring data would be exempt from the private right of action altogether.[23]

F. Unique or Notable Aspects of the ADPPA

Civil Rights

Unlike any state law, the ADPPA would prohibit the use of consumers' data in a way that discriminates based on race, color, religion, national origin, sex, or disability.[24] Large data holders using computerized decision making that could pose "a consequential risk of harm" would be required to perform an algorithm impact assessment annually to evaluate disparate impact. Other entities that engage in similar computerized decision-making processes would have to perform a less prescriptive algorithm design evaluation prior to deploying the algorithm.

Corporate Accountability

Similar in concept to the Sarbanes-Oxley Act and unlike the state laws, the ADPPA requires corporate accountability for compliance.[25] Large data holders would be required to submit annually a certificate of compliance, signed by an executive. Entities with more than 15 employees would have to appoint a privacy and data security officer. Further, there would be a privacy impact assessment requirement, the breadth of which depends on the size of the entity.

Transparency: China, Russia, Iran and North Korea

Privacy notice or privacy policy requirements are commonplace in privacy laws. The ADPPA is no exception. Unlike other laws, however, the ADPPA also mandates that the privacy policy to disclose whether data is transferred to, processed in, stored in, or otherwise accessible to China, Russia, Iran, or North Korea.[26]

Conclusion

The enactment of a comprehensive federal privacy law would be a game-changer in every state and, based on the current version of the federal bill, across every industry. In light of the federal bipartisan effort, we may see fewer states considering privacy measures in upcoming legislative sessions out of concern that their work may be in vain. As for the five states with laws that have not yet become effective, they are left in limbo wondering if their laws will ever take effect. ■

NOTES

1. Public Act 22-15; https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF.
2. Privacy professionals agreed that "CTPDPOMA" was simply not an acceptable acronym, so we use the shorter acronym of "CTDPA," which stands for the Connecticut Data Privacy Act, as we have lovingly renamed it.
3. P.A. 22-15, § 2.
4. *Id*. at § 1(25).
5. *Id*. at § 3(a).
6. *Id*. at § 3(b).
7. *Id*. at § 4.
8. *Id*. at § 6.

9. "Sensitive data" means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual; (C) personal data collected from a known child; or (D) precise geolocation data." *Id.* at § 1(27)

10. *Id.* at § 11.

11. California permits a limited private right of action for harm caused by a data breach.

12. H.R. 8152; https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf.

13. *Id.* at §§ 101 and 102.

14. *Id.* at § 2(9).

15. *Id.*

16. *Id.* at Titles II and III.

17. *Id.* at § 206.

18. *Id.* at § 205.

19. *Id.* at § 404.

20. https://oag.ca.gov/system/files/attachments/press-docs/Letter to Congress re Federal Privacy.pdf

21. Id. §§ 401-403.

22. *Id.* at § 209.

23. *Id.* at § 403(e).

24. *Id.* at § 207.

25. *Id.* at § 301 et. al.

26. *Id.* at § 201(b).

27. California's Consumer Privacy Act took effect in 2020. Substantial changes to that law, known as the California Privacy Rights Act, are scheduled to take effect on January 1, 2023.

Dena M. Castricone *CIPP/US, CIPM, managing member of DMC Law, LLC, is a privacy and healthcare attorney with substantial experience helping businesses and healthcare providers navigate privacy challenges and counseling clients on compliance with privacy laws. Attorney Castricone also advises healthcare providers on a broad range of regulatory compliance, risk management, and day-to-day operational issues.*