GIBSON DUNN

May 13, 2022

U.S. PRIVACY LAW UPDATE: CONNECTICUT ENACTS COMPREHENSIVE PRIVACY LAW AS OTHER STATES' LAWS CONTINUE TO DEVELOP

To Our Clients and Friends:

Connecticut has joined California, Virginia, Colorado, and Utah in enacting comprehensive data privacy legislation, with a signature from Governor Lamont this week on the Connecticut Data Privacy Act ("CTDPA"). Meanwhile, the text of Virginia's privacy law was amended and finalized, and the California Privacy Protection Agency ("CPPA") held pre-rulemaking stakeholder sessions about topics related to automated decision-making, consumers' rights, business' concerns, and cybersecurity, among others. Companies should account for these changes as they develop and refine their privacy compliance programs.

Connecticut Data Privacy Act

The CTDPA draws heavily upon its predecessor statutes in Virginia and Colorado, with very few departures of significance.[1] Indeed, while the specific combination of features in the CTDPA may be unique, the combination is largely made of elements seen in at least one of its preceding laws. The CTDPA will become effective by its terms in a little over a year, on July 1, 2023[2] – six months after the California Privacy Rights Act ("CPRA") and Virginia Consumer Data Protection Act ("VCDPA"), simultaneously with the Colorado Privacy Act ("CPA"), and six months before the Utah Consumer Privacy Act ("UCPA").

Potentially one of the most significant differences between the CTDPA and other states' laws may be within the threshold requirements. The CTDPA applies to persons that conduct business in Connecticut or produce products or services that are targeted to residents of the state, and that control or process the personal data of a particular number of residents, namely either:

1. 100,000 or more Connecticut residents, excluding residents whose personal data is controlled or processed solely for the purpose of completing a payment transaction; or

2. 25,000 or more Connecticut residents, where the business derives more than 25% of its gross revenue from the sale of personal data.[3]

Connecticut is the first state law to explicitly carve out payment transaction data from its applicability threshold; this provision was added to alleviate concerns of restaurants, small convenience stores, and similar businesses that process the personal information of many customers for the sole purpose of completing a transaction.

Like existing state data privacy laws, the CTDPA grants consumers—defined as Connecticut residents who are not acting in a commercial or employment context—various rights, including: (1) to confirm whether an entity acting as a data controller is processing their personal data, and to access such data; (2) to obtain a copy of their personal data in a portable and readily usable format; (3) to correct inaccuracies therein; and (4) to delete personal data provided by, or obtained about, them. It also requires data controllers to practice data minimization and purpose limitation, implement technical safeguards, and conduct data protection assessments.[4] The CTDPA adopts language similar to that of Virginia's recent amendment, described more fully below, relating to compliance with a consumer's request to delete by opting the consumer out of the processing of such personal data, where such information was obtained from a source other than the consumer.

Like the Virginia and Colorado laws, the CTDPA allows consumers to opt out of the processing of their personal data for purposes of (a) targeted advertising, (b) the sale of personal data, and (c) profiling in furtherance of solely automated decisions that produce similarly significant effects.[5] Like the California and Colorado laws, the CTDPA permits consumers to designate an authorized agent to act on their behalf and opt out of the processing of their data.[6] By January 1, 2025, data controllers must allow consumers to exercise their opt-out right through an opt-out preference signal.[7] Unlike California, which expects its CPPA to opine on what an opt-out signal might be, and how it might work, this provision is largely undefined, encouraging the market to create signals, bringing with it the potential for confusion as to what signals must be followed. The CTDPA, like other state laws, also prohibits processing a consumer's sensitive data without consent, and requires data controllers to provide a mechanism for revoking consent that is "at least as easy as" the mechanism by which the consumer provided consent.[8]

Like Virginia, Colorado, and Utah, and unlike California, Connecticut does not include a private right of action in its law – the CTDPA limits enforcement to the states' attorney general.[9] Until December 31, 2024, enforcement actions will be subject to 60-day cure period; thereafter, the attorney general may, but is not required to, provide an opportunity to correct an alleged violation.[10] A violation of the CTDPA will constitute an unfair trade practice,[11] which carries civil penalties of up to $5,000 per violation for willful offenses.[12]

Finally, the CTDPA, similar to Virginia, requires the joint standing committee of the General Assembly convene a task force to study various topics concerning data privacy. The task force must submit a report of its findings and recommendations to the joint standing committee by January 1, 2023.

Developments in Other States

Virginia

In April, Virginia Governor Youngkin signed into law three amendments to the VCDPA, which finalizes the VCDPA's text ahead of its January 1, 2023 effective date. The first amendment concerns consumers' right to delete their personal information. The VCDPA grants consumers the right to delete "personal data provided by *or obtained about*" them. The amendment provides that data controllers that have obtained personal data from a source other than the consumer will be deemed to be in compliance with

a consumer's request to delete if they opt the consumer out of the processing of such personal data, allowing businesses to avoid potentially technically infeasible requirements to delete data, so long as they no longer use it for any purpose.[13] The second amendment changes the definition of "nonprofit organization" to include political organizations, thus exempting them from the VCDPA.[14] The third and final amendment provides that all civil penalties, expenses, and attorney fees will be paid into the state treasury and credited toward the Regulatory, Consumer Advocacy, Litigation, and Enforcement Revolving Trust Fund, rather than a separate Consumer Privacy Fund.[15] Unlike California's and Colorado's laws, the VCDPA does not include rulemaking authority. Therefore, businesses subject to the VCDPA can develop their compliance programs ahead of January 1, 2023 without concern of significant changes resulting from the adoption of regulations.

California

As explained in more detail in a prior update, the CPPA is responsible for implementing and enforcing the CPRA and California Consumer Privacy Act ("CCPA"), a role which includes updating existing regulations and adopting new regulations. The CPPA is currently engaging in preliminary information-gathering activities to help inform its rulemaking. The CPPA accepted written comments in Fall 2021, provided informational sessions in March 2022, and, recently, held stakeholder sessions on May 4, 5, and 6, 2022, to provide an opportunity for stakeholders to speak on topics relevant to the upcoming rulemaking.

The topics discussed during the stakeholder sessions included automated decision-making, data minimization and purpose limitations, dark patterns, consumers' rights, business' concerns, and cybersecurity, among others. Between two and ten stakeholders spoke on each topic, and the speakers ranged from individuals to representatives of private organizations, non-profits, government, and industry groups.

Below are highlights from some of the sessions:

- Automated Decision-Making. Stakeholders articulated divergent views on the definition of Automated Decision-Making ("ADM"). Industry stakeholders proposed a narrower definition to exclude processes related to safety, such as automobile lane-keeping features. Consumers and NGOs conversely asked for a broad definition that would sweep in processes that are not fully automated but that would have a substantial impact on individuals.

- Business Concerns. Businesses expressed a number of concerns over their responsibilities related to disclosure and consumers' rights, including the difficulty of harmonizing compliance across numerous regimes, including other states' laws and GDPR; the vagueness of certain definitions, including "contractor," "service provider," and "sale," among others; the cost of implementation; and harm to data-driven businesses through strict interpretation of the "purpose limitation."

- Consumer Concerns. Consumers were concerned with the difficulty of navigating click-through options to exercise their rights, noting that in some cases, they had to hand over PII in connection with the verification process before they could ask for correction or deletion of their information. Single-click and global, browser-level opt-outs were the most commonly cited suggestion for

making the consumer experience of exercising rights more effective and easier, and discussion about how those should be implemented based on the language of the statute were also brought up.

- Dark Patterns. Stakeholders requested more clarity on the definition of "dark patterns," and suggested that unfair and deceptive practice laws and regulations could already be used to address dark patterns that harm consumers.

- Cybersecurity and Risk Assessments. Speakers suggested looking to the GDPR for guidance around risk assessment requirements and implementation, and emphasized the benefits of harmonizing the requirements across jurisdictions.

The CPPA did not comment on any suggestions, and noted that they were in "listening mode." The CPPA has not commenced formal rulemaking activities, and continues to gather information. Updates on the CPPA's activities related to rulemaking are available here.

Separately, there has been no further movement on the proposals floated by the California legislature to extend the business-to-business and employment-related exemptions in the CCPA, leaving businesses to continue to consider how to comply with the CPRA with respect to those individuals' information.

Other States

Proposed data privacy legislation currently remains in committee in Alaska, Louisiana, Massachusetts, Michigan, North Carolina, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, and Vermont. Numerous other states also are actively considering such laws, with drafting and negotiations at various phases.

We will continue to monitor developments in this area, and are available to discuss these issues as applied to your particular business.

---

[1] Connecticut Data Privacy Act ("CTDPA"), S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Conn. 2022).

[2] CTDPA, § 1.

[3] CTDPA, § 2.

[4] CTDPA, §§ 6(1)–(3); 8

[5] CTDPA, § 4(a).

[6] CTDPA, § 5.

[7] CTDPA, § 6(e)(1)(A)(ii).

[8] CTDPA, § 6.

[9] CTDPA, § 11(a).

[10] CTDPA, § 11(b).

[11] CTDPA, § 11(e).

[12] Conn. Gen. Stat. § 42-110o.

[13] H 381, 2022 Gen. Assemb., Reg. Sess. (Va. 2022).

[14] S 534, 2022 Gen. Assemb., Reg. Sess. (Va. 2022).

[15] S 534, 2022 Gen. Assemb., Reg. Sess. (Va. 2022).

This alert was prepared by Cassandra Gaedt-Sheckter, Ryan Bergsieker, Alexander Southwell, Sarah Scharf, Abbey Barrera, Tony Bedel, Courtney Wang, Raquel Sghiatti, and Samantha Abrams-Widdicombe.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity and Data Innovation practice group:

United States

Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)
Svetlana S. Gans – Washington, D.C. (+1 202-955-8657, sgans@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)

Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Europe
Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0) 1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)