GIBSON DUNN

U.S. Privacy Law Update: Utah Joins Growing List of States with Comprehensive Privacy Laws as Other States See Potential Changes

Client Alert | March 11, 2022

Click for PDF

Utah is poised to join California, Virginia, and Colorado in enacting comprehensive data privacy legislation. Although Utah's law largely follows the Virginia and Colorado models—with a few provisions that may ease the burden on businesses—it adds to an increasingly active state legislative landscape. Meanwhile, California is proposing changes to its landmark privacy law as other states plow ahead with debating or updating their own data privacy laws. Companies should account for these changes as they develop programs to comply with the laws.

Utah Consumer Privacy Act

In Utah, the legislature unanimously passed the Utah Consumer Privacy Act.[1] After the bill reaches the governor's desk, he will have 20 days to sign or veto it or it will become law automatically signature if the governor vetoes the bill, the legislature has sufficient votes to override the veto, given that it was passed unanimously. Once enacted, the new law will become effective by its terms on December 31, 2023,[2]—approximately one year after the similar laws in Colorado and Virginia go into force. Comparable to the other laws, the new law applies to companies that (1) conduct business in Utah or target consumers in the state, (2) have $25 million or more in annual revenue, and (3) either (a) process or control personal data of 100,000 or more Utah consumers or (b) process or control personal data of 25,000 or more Utah consumers and derive 50 percent or more of their gross revenue from selling personal data.[3]

While Utah's law is similar to Virginia's and Colorado's laws, it has a few differences that may make the law easier for businesses to follow. For example, like Virginia and Colorado, Utah does not include a private right of action in its law, although the attorney general can seek statutory damages, as described more fully below. However, unlike the laws in Virginia and Colorado, Utah's law does not require businesses to conduct and document data protection assessments about their data-processing practices.[4] Utah also does not require businesses to set up a mechanism for consumers to appeal a business's decision regarding the consumer's request to exercise any of their personal data rights.[5] And finally, Utah's law makes it easier to charge a fee when responding to consumer requests. Specifically, businesses may charge a fee when responding to consumer requests to exercise their personal data rights in Virginia only if those requests are "manifestly unfounded, excessive, or repetitive,"[6] or in Colorado only if a second request is made in a 12-month period.[7] But Utah allows businesses to charge a fee in both those situations as well as when the business "reasonably believes the primary purpose in submitting the request was something other than exercising a right" or is harassing, disruptive, or poses an undue burden on the controller.[8]

Related People

Ryan T. Bergsieker

Cassandra L. Gaedt-Sheckter

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Relating to enforcement, while Utah's Division of Consumer Protection can investigate potential violations, Utah's law, like Colorado's and Virginia's, limits enforcement to the state attorney general.[9] The attorney general must give companies at least 30 days to cure before initiating an action.[10] If the attorney general does bring such an action, they may collect statutory damages of up to $7,500 per violation or actual damages.[11]

Developments in Other States

As Utah moves ahead with its new privacy law, California legislators have floated proposals to extend the business-to-business and employment-related exemptions in the California Consumer Privacy Act ("CCPA"). Under those exemptions, the CCPA does not generally apply to employment-related data or data involved in transactions between businesses for due diligence or to provide a good or service. The California Privacy Rights Act ("CPRA") is presently set to sunset those exemptions on January 1, 2023. But the bills introduced in California would extend those exemptions either through January 1, 2026, or pursuant to the alternative bill, indefinitely.[12]

California is not the only state with updates to its comprehensive data privacy law in the works. Colorado's attorney general announced recently that a formal notice of proposed rulemaking under the Colorado Privacy Act will be issued by this fall to prepare regulations that will be implemented by January 2023. In the meantime, town halls and meetings are planned to gather comments on that rulemaking.

Other states are moving rapidly to join California, Colorado, Virginia, and Utah. Data privacy laws have passed committee or chamber votes this year in Indiana, Iowa, Florida, Massachusetts, Ohio, Washington, and Wisconsin, and numerous other states also are considering legislation. Although the precise contours of these laws—and how many, if any more this year, will be enacted, and when—remain in flux, the enactment of state privacy laws already has ushered in notable regulatory changes affecting how companies collect and manage data while imposing a host of new obligations and potential liability, across the country. Companies would be well-served to focus their compliance programs accordingly.

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

---

[1] Utah Consumer Privacy Act ("UCPA"), S.B. 227, 2022 Leg. Sess. (Utah 2022).

[2] UCPA, § 17.

[3] UCPA, § 3, 13-61-102(1).

[4] *See* Colorado Privacy Act ("CPA"), S.B. 21-190, § 6-1-1309, 73d Leg., 2021 Regular Sess. (Colo. 2021); Virginia Consumer Data Protection Act ("VCDPA"), S.B. 1392, § 59.1-576, 2021 Spec. Sess. (Va. 2021).

[5] *See* CPA, 6-1-1306(3)(a); VCDPA, § 59.1-573(C).

[6] VCDPA, § 59.1-573(B)(3).

[7] CPA, § 6-1-1306(2)(c).

[8] UCPA, § 7, 13-61-203(4)(b)(i)(B)-(C).

[9] UCPA, § 13, 13-61-305; § 13, 13-61-401; § 14, 13-61-402(1)-(2).

[10] UCPA, § 14, 13-61-402(3)(b)-(c).

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

[11] UCPA, § 14, 13-61-402(3)(d).

[12] *See* A.B. 2871, 2021–2022 Reg. Sess. (Calif. 2022); A.B. 2891, 2021–2022 Reg. Sess. (Calif. 2022).

This alert was prepared by Ryan T. Bergsieker, Cassandra Gaedt-Sheckter, Eric M. Hornbeck and Alexander H. Southwell.

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) 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)

© 2022 Gibson, Dunn & Crutcher LLP

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.

Related Capabilities

Privacy, Cybersecurity, and Data Innovation

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**