GIBSON DUNN

April 13, 2023

U.S. PRIVACY LAW UPDATE: IOWA BECOMES SIXTH STATE TO ENACT COMPREHENSIVE PRIVACY LAW, OTHER STATES' LAWS CONTINUE TO DEVELOP

To Our Clients and Friends:

On March 29, 2023, Iowa's Governor, Kim Reynolds, signed Senate File 262 into law, making Iowa—somewhat unexpectedly—the sixth state, following California, Virginia, Colorado, Utah and Connecticut, to enact comprehensive data privacy legislation. Meanwhile, the Colorado Office of the Attorney General filed a final draft of the Colorado Privacy Act Rules ("CPA Rules") with the Colorado Secretary of State's Office on March 15, 2023. Additionally, on February 3, 2023, the California Privacy Protection Agency ("CPPA") Board voted to (1) adopt and approve the CPPA's California Privacy Rights Act ("CPRA") regulations and (2) invite pre-rulemaking comments from the public on the topics of cybersecurity audits, risk assessments, and automated decision making. Finally, Utah's Governor, Spencer Cox, signed two bills that regulate social media companies with respect to children's use of social media platforms into law on March 23, 2023.

Iowa's Comprehensive Privacy Law

Iowa's law will become effective on January 1, 2025, and applies to any person conducting business in the state of Iowa, or producing products or services that are targeted to consumers who are residents of the state, *and* that processes a certain number of Iowa consumers' personal data during a calendar year, namely:

1. 100,000 Iowa consumers;[1] or

2. 25,000 Iowa consumers, if the person derives over fifty percent of gross revenue from the sale of personal data.[2]

This definition tracks the non-California laws, though does not additionally have the $25 million incremental requirement like Utah. As a result, small businesses that process a large number of Iowa consumers' data might be covered. Further, like Virginia's, Colorado's, Utah's and Connecticut's laws, Iowa's law defines "consumer" as a natural person *acting only in an individual or household context*, thereby excluding employee and business-to-business (B2B) data from the law's applicability.[3]

Iowa's law draws heavily from its predecessors elsewhere as well, and is most similar to, and even more business-friendly in many ways than, Utah's privacy law. Like Utah's law, Iowa's does not grant consumers the right to correct their personal data or opt out of the processing of their personal data for purposes of profiling, and grants consumers the right to opt *out* of (as opposed to opt in to) the processing of their sensitive personal data.[4] Additionally, Iowa's law does not explicitly grant consumers the right

to opt out of the processing of their personal data for purposes of targeted advertising or cross-context behavioral advertising, making it the only comprehensive state privacy law that does not do so.[5] However, Iowa's law does specify that a controller that engages in targeted advertising "shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity", suggesting that not including the right to opt out of the processing of personal data for purposes of targeted advertising under consumer data rights may have been a drafting error.[6] Iowa's law allows controllers 90 days to respond to consumer requests, which period may be extended by an additional 45 days upon notice to the consumer, along with a reason for the extension;[7] by contrast, all of the other state laws require controllers to respond within 45 days and allow them to extend such period by an additional 45 days upon notice and explanation to the consumer. Unlike Utah's law, and like Virginia's, Colorado's, and Connecticut's laws, Iowa's affords consumers the right to appeal a controller's denial of a consumer request.[8] Like Utah's law, and unlike the others, Iowa's law does not require controllers respond to opt-out preference signals or conduct data protection assessments. Additionally, Iowa's law does not require controllers to practice purpose limitation or data minimization.

Iowa's law grants the state attorney general exclusive enforcement authority, subject to a (longer-than-others) 90-day cure period.[9] The attorney general may seek injunctive relief and civil penalties of up to $7,500 per violation.[10]

Colorado Privacy Act Rules

On March 15, 2023, the Colorado Office of the Attorney General filed a final draft of the CPA Rules, which will be published in the Colorado Register later this month and will go into effect July 1, 2023. The draft regulations – finalized after a review of 137 written comments, five virtual and in-person public input sessions, and a rulemaking hearing – clarify language around consumers' rights, consent, universal opt-out mechanisms, duties of controllers, and data protection assessments. Below, we've highlighted what we believe to be some of the most interesting and potentially impactful rules.

Right to Delete. While the Colorado Privacy Act (the "CPA") affords Colorado consumers the right to delete personal data *concerning* them,[11] the CPA Rules clarify that if the controller has obtained personal data concerning the consumer from a source other than the consumer, the controller may comply with a consumer's deletion request with respect to such personal data by opting the consumer out of the processing of such personal data.[12] This brings Colorado's rules in line with Virginia's law, leaving Connecticut as the only state that truly affords consumers the right to delete personal data obtained about them.

Universal Opt-Out Mechanisms. The CPA allows consumers to exercise their right to opt out of certain processing through a universal opt-out mechanism.[13] The CPA Rules specify the required technical specifications for such mechanisms and create standards governing the way that opt-out mechanism requirements must be implemented. Specifically, the CPA Rules indicate that the mechanism must (1) allow consumers to automatically communicate their opt-out choice with multiple controllers; (2) allow consumers to clearly communicate one or more opt-out rights; (3) store, process, and transmit consumers' personal data using reasonable data security measures; (4) not prevent controllers from determining (a) whether a consumer is a Colorado resident or (b) that the mechanism represents a

legitimate request to opt out of the processing of personal data; and (5) not unfairly disadvantage any controller.[14] The CPA Rules also specify that universal opt-out mechanisms may not be the default setting for a tool that comes pre-installed.[15] Additionally, the CPA Rules require the Colorado Department of Law to maintain a public list of universal opt-out mechanisms that have been recognized to meet the foregoing standards, with an initial list to be released no later than January 1, 2024.[16] The Global Privacy Control (GPC), which is recognized by the California Attorney General, is likely to be included on such list. By July 1, 2024, controllers must respond to opt-out requests received through universal opt-out mechanisms included on such list, provided that the controller has had at least six months' notice of the addition of new mechanisms; the controller may (but is not required to) recognize universal opt-out mechanisms that are not included in such list.[17] Finally, a controller may not interpret the absence of a universal opt-out mechanism after the consumer previously used one as a consent to opt back in.

Loyalty Programs. The CPA Rules contain extensive disclosure requirements for controllers maintaining a "bona fide loyalty program", which it defines as "a loyalty, rewards, premium feature, discount, or club card program established for the genuine purpose of providing [an offer of superior price, rate, level, quality, or selection of goods or services] to [c]onsumers that voluntarily participate in that program, such that the primary purpose of [p]rocessing [p]ersonal [d]ata through the program is solely to provide [such benefits] to participating [c]onsumers."[18] Specifically, the CPA Rules require controllers disclose: (1) the categories of personal data collected through the bona fide loyalty program that will be sold or processed for targeted advertising; (2) the categories of third parties that will receive the consumer's personal data; (3) a list of any bona fide loyalty program partners, and the benefits provided by each such partner; (4) an explanation of why the deletion of personal data makes it impossible to provide a bona fide loyalty program benefit (if the controller claims that is the case); and (5) an explanation of why sensitive data is required for the bona fide loyalty program benefit (if the controller claims that is the case).[19]

Changes to a Privacy Notice. The CPA Rules require controllers to *notify* consumers of material changes to their privacy notices, and specify that material changes may include changes to: (1) categories of personal data processed; (2) processing purposes; (3) a controller's identity; (4) the act of sharing personal data with third parties; (5) categories of third parties personal data is shared with; or (6) methods by which consumers can exercise their data rights request.[20]

Purpose Specification, Data Minimization, and Secondary Use. The CPA Rules clarify the CPA's purpose specification, data minimization, and secondary use provisions.[21] Notably, the CPA Rules require controllers set specific time limits for erasure or conduct a periodic review to ensure compliance with data minimization principles, and specify that biometric identifiers, photographs, audio or voice recordings and any personal data generated from photographs or audio or video recordings should be reviewed at least annually.[22] The CPA Rules require controllers obtain consent before processing personal data for purposes that are not "reasonably necessary to or compatible with specified [p]rocessing purpose(s)", and enumerate factors that controllers may consider to determine whether the new purpose is "reasonably necessary to or compatible with" the original specified purpose.[23]

Sensitive Data. The CPA prohibits controllers from processing a consumer's sensitive data without first obtaining consent.[24] Among other clarifications (including that biometric data must be used or intended for identification), the CPA Rules create a new category of sensitive data called sensitive data inferences, which are defined as "inferences made by a [c]ontroller based on [p]ersonal [d]ata, alone or in combination with other data, which indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status", and specify that controllers must obtain consent in order to process sensitive data inferences unless such inferences are (1) from consumers over the age of thirteen, (2) the processing purposes are obvious, (3) such inferences are permanently deleted within 24 hours, (4) such inferences are not transferred, sold, or shared with any processor, affiliates, or third parties, and (5) the personal data and sensitive data inferences are not processed for any purpose other than the express purpose disclosed to the consumer.[25]

Consent. The CPA Rules contain detailed requirements for what constitutes and how to obtain valid consent, as well as a significant discussion of user interface design, choice architecture, and dark patterns.[26] Specifically, consent must be informed, specific, freely given, obtained through clear and affirmative action, and reflect the consumer's unambiguous agreement, and the CPA Rules provide additional guidance on each of these elements.[27] The CPA Rules require that controllers refresh consent to continue processing sensitive data or personal data for a secondary use that involves profiling in furtherance of decisions that produce legal or similarly significant effects when a consumer has not interacted with the controller in the prior 24 months; however, controllers are not required to refresh consent when the consumer has access and ability to update their opt-out preferences at any time through a user-controlled interface.[28] The CPA Rules indicate that controllers need to obtain consent before January 1, 2024 in order to continue processing sensitive data collected prior to July 1, 2023.[29] The CPA Rules also specify that if a controller has collected personal data prior to July 1, 2023 and the processing purposes change after July 1, 2023 such that it is considered a secondary use, the controller must obtain consent at the time the processing purpose changes.[30]

Data Protection Assessments. The CPA requires controllers to conduct and document a data protection assessment before conducting a processing activity that presents a heightened risk of harm to a consumer.[31] The CPA Rules clarify the scope and requirements of such data protection assessments, making Colorado the first state to provide regulations governing data protection assessments conducted under a comprehensive state privacy law. The CPA Rules specify thirteen topics that must be included in a data protection assessment, including a short summary of the processing activity, the categories of personal data processed, the sources and nature of risks to consumers associated with the processing activity, measures and safeguards the controller will employ to reduce such risks, and a description of how the benefits of the processing outweigh such risks. The CPA Rules indicate that if a controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, such assessment shall satisfy the requirements set forth in the CPA Rules if such assessment is "reasonably similar in scope and effect" to the assessment that would otherwise be conducted pursuant to the CPA Rules.[32] If the assessment is not reasonably similar, a controller may still submit that assessment, along with a supplement that contains any additional information required by Colorado.[33] The CPA Rules also clarify that data protection assessments are required for activities created or generated after July 1, 2023; the requirement is not retroactive.[34]

Profiling. Colorado is also the first state to enact regulations governing profiling in the context of a comprehensive state privacy law. With respect to the right of access, the CPA Rules clarify that "specific pieces of personal data" include profiling decisions, inferences, derivative data, marketing profiles, and other personal data created by the controller that is linked or reasonably linkable to an identified or identifiable individual.[35] With respect to the right to opt out of the processing of personal data for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects, the CPA Rules clarify that a controller may decide not to take action on such a request if the profiling is based on "human involved automated processing" (i.e., "the automated processing of [p]ersonal [d]ata where a human (1) engages in a meaningful consideration of available data used in the [p]rocessing or any output of the [p]rocessing and (2) has the authority to change or influence the outcome of the [p]rocessing"), provided that certain information is provided to the consumer.[36]

California Privacy Rights Act Regulations

On February 3, 2023, the CPPA Board voted to adopt and approve the CPPA's CPRA regulations promulgated and revised to date, and to direct staff to take all steps necessary to complete the rulemaking process, including the filing of the final rulemaking package with the Office of Administrative Law ("OAL").[37] On February 14, 2023, the CPPA submitted the rulemaking package to the OAL for final review.[38] The OAL has 30 days from the date of submission to review the proposed regulations; while the 30 days have passed, an update has not explicitly been released. The details of the regulations have been detailed in prior Gibson Dunn alerts.[40]

The Board also voted to invite pre-rulemaking comments from the public on cybersecurity audits, risk assessments, and automated decision making, for which there have not been any regulations drafted.[41] Following the vote, on February 10, 2023, the CPPA issued an Invitation for Preliminary Comments on Proposed Rulemaking on these topics.[42] Interested parties were required to submit comments by 5:00 p.m. PT on Monday, March 27, 2023. A copy of the invitation that was issued is available here.

Utah Social Media Regulation Act

On March 23, 2023, Utah's Governor, Spencer Cox, signed two bills into law that regulate social media companies with respect to children's use of social media platforms. Both will take effect on March 1, 2024.

S.B. 152 requires "social media companies", which it defines as "a person or entity that: (a) provides a social media platform that has at least 5,000,000 account holders worldwide; and (b) is an interactive computer service", to verify the age of Utah residents seeking to maintain or open an account, obtain parental consent before allowing a Utah resident under the age of 18 to open or maintain an account, and implement specific restrictions for Utah residents under 18.[43] Specifically, S.B. 152 prohibits social media companies from (1) showing minors' accounts in search results, (2) displaying advertising to minors' accounts, (3) targeting or suggesting groups, services, products, posts, accounts or users to minors' accounts or (4) collecting, sharing, or using personal information from minors' accounts (with certain exceptions).[44] Additionally, S.B. 152 requires social media companies to (1) prohibit minors' accounts from direct messaging "any other user that is not linked to the [minor's] account through

friending", (2) limit hours of access (subject to parental or guardian direction), and (3) provide parents with a password or other means of accessing the minor's account.[45]

H.B. 311 prohibits social media companies from using a practice, design or feature that it knows (or should know through the exercise of reasonable care) causes a Utah resident under the age of 18 to "have an addiction to" the social media platform.[46] H.B. 311 defines "addiction" as "use of a social media platform that: (a) indicates the user's substantial preoccupation or obsession with, or the user's substantial difficulty to cease or reduce use of, the social media platform; and (b) causes physical, mental, emotional, developmental, or material harms to the user."[47]

The laws grant authority to administer and enforce their requirements to the Division of Consumer Protection.[48] S.B. 152 also delegates certain rulemaking authority to the Division of Consumer Protection.[49] Violations of S.B. 152 are punishable by an administrative fine of up to $2,500 for each violation, subject to a 30-day cure period.[50] Violations of H.B. 311 are punishable by (1) a civil penalty of $250,000 for each practice, design, or feature shown to have caused addiction and (2) a civil penalty of up to $2,500 for each Utah minor account holder who is shown to have been exposed to such practice, design or feature.[51] Additionally, the laws provide for private rights of action and specify that the person who brings action is entitled to (a) an award of reasonable attorney fees and court costs and (b) an amount equal to the greater of (i) $2,500 per violation or (ii) actual damages for financial, physical, and emotional harm incurred by the person bringing the action.[52]

In a previous client alert, we discuss the California Age-Appropriate Design Code Act, which is also aimed at protecting the wellbeing, data, and privacy of children under the age of 18 using online platforms. However, Utah's laws go much further. Together, these laws evidence the increased attention children's privacy is receiving from lawmakers and regulators, as they are more targeted in scope—and incremental—as compared to each state's previous, comprehensive privacy law.

Other States

State legislative activity regarding data privacy appears to be at an all-time high. Proposed data privacy legislation has passed a legislative chamber in Hawaii, Indiana, Kentucky, Montana, New Hampshire, and Oklahoma. Numerous other states are also actively considering data privacy legislation, 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] This is a fairly significant threshold to meet, as it is about 3% of the state's population.

[2] S.F. 262, 90th Gen. Assemb., Reg. Sess. §§ 2(1), 10 (Iowa 2023).

[3] *Id.* § 1(7).

[4] *See id*. § 3.

[5] *See id.*

[6] *See id.* § 4(6).

[7] *Id.* § 3(2)(a).

[8] *Id.* § 3(3).

[9] *Id.* §§ 8(1)-(2).

[10] *Id.* § 8(3).

[11] Colorado Privacy Act ("CPA"), S.B. 21-190, 73rd Gen. Assemb., Reg. Sess., § 6-1-1306(1)(d) (Colo. 2021) (to be codified in Colo. Rev. Stat. Title 6).

[12] Colo. Dep't of Law, Colorado Privacy Act Rules ("CPA Rules"), to be codified at 4 Colo. Code Regs. § 904-3, r. 4.06(D), *available at* https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.

[13] CPA, § 6-1-1306(1)(a)(IV).

[14] CPA Rules, r. 5.06.

[15] *Id.*, r. 5.04(A).

[16] *Id.*, r. 5.07(A).

[17] *Id.*, r. 5.08(A)-(B).

[18] *Id.*, r. 2.02.

[19] *Id.*, r. 6.05(F).

[20] *Id.*, r. 6.04(A).

[21] *Id.*, r. 6.06-.08

[22] *Id.*, r. 6.07(B).

[23] *Id.*, r. 6.08(B)-(C).

[24] CPA, § 6-1-1308(7).

[25] CPA Rules, r. 2.01(A), 6.10(A)-(B).

[26] *Id.*, pt. 7

[27] *Id.*, r. 7.03

[28] *Id.*, r. 7.08(A)-(B).

[29] *Id.*, r. 7.02(B)(1).

[30] *Id.*, r. 7.02(B)(2).

[31] CPA, § 6-1-1309(1).

[32] CPA Rules, r. 8.02(B).

[33] *Id.*

[34] *Id.*, r. 8.05(F).

[35] *Id.*, r. 4.04(A)(1).

[36] *Id.*, r. 2.02, 9.04(C)

[37] Cal. Priv. Prot. Agency, News & Announcements, *CPPA Board Unanimously Votes to Advance Regulations* (Feb. 3, 2023), available at https://cppa.ca.gov/announcements/.

[38] Cal. Priv. Prot. Agency, News & Announcements, *CPPA Files Proposed Regulations with the Office of Administrative Law (OAL)* (Feb. 14, 2023), available at https://cppa.ca.gov/announcements/.

[39] *Id.*

[40] *See*, *e.g.*, U.S. Cybersecurity and Data Privacy Outlook and Review – 2023 (January 30, 2023), available at https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/#_ednref2; Insights on New California Privacy Law Draft Regulations, Gibson Dunn (June 15, 2022), available at https://www.gibsondunn.com/insights-on-new-california-privacy-law-draft-regulations/.

[41] Cal. Priv. Prot. Agency, News & Announcements, *CPPA Board Unanimously Votes to Advance Regulations* (Feb. 3, 2023), available at https://cppa.ca.gov/announcements/.

[42] Cal. Priv. Prot. Agency, News & Announcements, *CPPA Issues Invitation for Preliminary Comments on Cybersecurity Audits, Risk Assessments, and Automated Decision Making* (Feb. 10, 2023), available at https://cppa.ca.gov/announcements/.

[43] S.B. 152, 2023 Gen. Sess., §§ 13-63-101(8), 13-63-102(1),(3) (Utah 2023).

[44] *Id.*, § 13-63-103.

[45] *Id.*, §§ 13-63-103(1), 13-63-104, 13-63-105.

[46] H.B. 311, 2023 Gen. Sess., § 13-63-201(2) (Utah 2023).

[47] *Id.*, § 13-63-101(2).

[48] S.B. 152, § 13-63-202(1); H.B. 311, § 13-63-201(1)(a).

[49] S.B. 152, § 13-63-102(4).

[50] S.B. 152, §§ 13-63-202(3)(a)(i), (4).

[51] H.B. 311, § 13-63-201(3)(a).

[52] S.B. 152, § 13-63-301; H.B. 311, § 13-63-301.

The following Gibson Dunn lawyers assisted in preparing this alert: Cassandra Gaedt-Sheckter, Ryan T. Bergsieker, and Sarah Scharf.

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 & Data Innovation practice group:

United States

S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Jane C. Horvath – Co-Chair, PCDI Practice, Washington, D.C. (+1 202-955-8505, jhorvath@gibsondunn.com)
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@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)
Gustav W. Eyler – Washington, D.C. (+1 202-955-8610, geyler@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)
Lauren R. Goldman – New York (+1 212-351-2375, lgoldman@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202-955-8510, shandler@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)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)

Rosemarie T. Ring – San Francisco (+1 415-393-8247, rring@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@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)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

Europe
Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Joel Harrison – London (+44(0) 20 7071 4289, jharrison@gibsondunn.com)
Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)

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