Wisconsin Legislative Council

STUDY COMMITTEE MEMO

Memo No. 1

TO: MEMBERS OF THE STUDY COMMITTEE ON THE REGULATION OF ARTIFICIAL INTELLIGENCE IN WISCONSIN

FROM: Patrick Ward and Tom Koss, Staff Attorneys, and Brian Larson, Principal Attorney

RE: Consumer Data Privacy Legislation in Select States

DATE: August 22, 2024

At its July 24, 2024, meeting, the study committee members requested information regarding consumer data privacy legislation in Colorado, Connecticut, and Utah, along with a summary of Wisconsin law and legislation related to this topic. This Memo provides information in response to this request.

Colorado, Connecticut, and Utah have similar consumer data privacy laws ("sample state laws") that went into effect in 2023.[1] These sample state laws create rights for consumers and obligations for businesses relating to consumer data privacy when a business that controls or processes consumer data meets certain thresholds related to consumer volume and sales revenue, with certain exemptions. This Memo provides an overview of the sample state laws and describes relevant differences. It compares the sample state laws by the following themes: (1) applicability; (2) consumer rights; (3) business obligations; and (4) enforcement.

Wisconsin has not enacted a data privacy law. In the most recent legislative session, the Legislature considered 2023 Assembly Bill 466 ("AB 466"), relating to consumer data protection and providing a penalty, which passed the Assembly but did not pass the Senate.[2] It is similar to the sample state laws, as noted throughout this Memo.

APPLICABILITY

Generally, the sample state laws apply to any controller or processor that operates in the state and meets certain thresholds related to the number of consumers for whom they process or control data. However, the laws exempt certain entities and information from the requirements, such as entities subject to certain federal privacy laws.

Key Definitions

As was mentioned, the sample state laws create certain obligations for controllers and processors. A controller is an entity that determines the purposes and means of processing personal data, and a

[1] Those state laws are: Colorado S.B. 21-190; Connecticut Public Act No. 22-15; and Utah Code § 13-61.

[2] This Memo discusses AB 466, as amended and passed by the Assembly. For more information, see the bill history page.

processor is an entity that processes personal data on behalf of a controller. Processing is generally the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.[3]

The sample state laws define personal data as any information that is linked, or can reasonably be linked, to an identified or identifiable individual, and does not include de-identified data or publicly available information.[4] Each state defines de-identified data and publicly available information similarly. De-identified data is data that cannot be reasonably linked to a certain individual and that is possessed by a controller who takes certain actions relating to maintaining the de-identified nature of the data.[5] Each state includes in its definition of publicly available information any information that is lawfully made available from government records, and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public.[6]

AB 466 uses similar definitions, but does not include aggregated data in its definition of personal data. AB 466 also does not include synthetic data in its definition of de-identified data and does not require controllers to maintain the de-identified nature of the data.

Consumer Volume and Sales Revenue Thresholds

The sample state laws apply to any controller or processor that either operates in the relevant state or targets products or services to residents of the relevant state, and that meets certain thresholds related to the number of consumers[7] for whom they process or control data. Those thresholds are as follows:

- In Colorado, those that: (1) control or process the personal data of at least 100,000 consumers during a calendar year; or (2) derive revenue or receive a discount on the price of goods or services from the sale of personal data and processes, or control the personal data of at least 25,000 consumers.
- In Connecticut, those that: (1) control or process the personal data of at least 100,000 consumers during a calendar year; or (2) control or process the personal data of at least 25,000 consumers, and derive more than 25 percent of gross revenue from the sale of personal data.
- In Utah, those that have an annual revenue of $25 million or more and: (1) control or process the personal data of at least 100,000 consumers during a calendar year; or (2) derive 50 percent of the entity's gross revenue from the sale of personal data, and control or process personal data of at least 25,000 consumers.

[3] To this list, Colorado also includes the sale of personal data and a controller's direction of a processor to process personal data.

[4] Utah also exempts from its definition of personal data the term "aggregated data," which it defines as information that relates to a group or category of consumers from which individual consumer identities have been removed, and that is not linked or cannot be reasonably linked to any consumer.

[5] Utah additionally specifies that "synthetic data" is included in its definition, which Utah defines as data that has been generated by computer algorithms or statistical models and does not contain personal data.

[6] Connecticut and Utah add to that definition information that is lawfully made available through widely distributed media. Utah also includes information that a consumer has not restricted to a specific audience, and that the controller obtains from a person to whom the consumer disclosed the information.

[7] The sample state laws generally define a consumer as an individual who is a resident of the state, except for individuals acting in certain commercial or employment contexts. Colorado, Utah, and AB 466 further define a consumer as an individual acting only in an individual or household context.

For AB 466, those thresholds are: (1) controlling or processing the personal data of at least 100,000 consumers during a calendar year; or (2) controlling or processing the personal data of at least 25,000 consumers while deriving over 50 percent of gross revenue from the sale of personal data.

Exemptions

The sample state laws exempt certain entities and types of information from the laws' requirements. Generally, entities and information exempted include the following: entities subject to certain federal laws related to privacy, such as the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, and Driver's Privacy Protection Act; certain entities regulated under federal law, such as air carriers and financial institutions; data used for determining a consumer's creditworthiness; data maintained for employment record purposes; certain health care information; institutions of higher education; public utilities; and governmental entities.[8]

The exemptions in AB 466 are very similar to those in the sample state laws. Those exemptions include the following: entities subject to certain federal laws, such as the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, and Driver's Privacy Protection Act; certain health care information; institutions of higher education; nonprofit organizations; and state and local governmental bodies.

CONSUMER RIGHTS

The sample state laws provide a consumer with certain rights with respect to the consumer's data. Those rights include the right to access, right to delete, right to portability, and right to opt out of certain processing activities; Colorado, Connecticut, and AB 466 also provide a right to correct.

Right to Access

Under the sample state laws, a consumer has the right to confirm whether a controller is processing the consumer's personal data and to access that personal data.[9]

Right to Delete

Under the sample state laws, a consumer generally has the right to delete personal data that concerns the consumer. Utah's right to delete, however, only allows a consumer to delete the personal data that the consumer provided to the controller, while the right to delete in Colorado and Connecticut applies to any personal data obtained by the controller, regardless of how it was obtained. AB 466 follows the approach taken by Colorado and Connecticut.

Right to Portability

Under the sample state laws, a consumer generally has the right to obtain a copy of his or her personal data in a portable and readily-usable format that allows the consumer to transmit the data to another controller without hindrance, unless doing so would require the disclosure of a trade secret.[10]

[8] One substantive difference between the sample state laws is that Connecticut and Utah exempt nonprofit organizations, while Colorado does not.

[9] Connecticut and Utah created an exception to this right if the confirmation or access would require a controller to reveal a trade secret, with Connecticut's exception applying narrowly to the right to access and Utah's exception applying broadly to any requirement in its law. AB 466 uses Connecticut's approach.

[10] Connecticut and Utah only provide that this right includes transmitting data to another controller if the processing is carried out by automated means.

Generally, the controller must provide the data in a format that is portable and readily usable.[11] Of the sample state laws, two states limit the right to portability; Utah's right to portability applies only to data that the consumer previously provided to the controller, while Colorado allows a consumer to exercise the right to portability no more than twice per calendar year.

AB 466 follows the approach taken by Utah.

Right to Opt-Out

Under the sample state laws, a consumer generally has the right to opt out of the processing of the consumer's personal data for the purposes of targeted advertising and the sale of personal data.

However, this right to opt out differs in several ways among the sample state laws. First, Colorado and Connecticut also allow a consumer to opt out for the purpose of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.[12] Second, Colorado and Connecticut allow a consumer to designate a third-party agent to exercise this opt-out right, and require a controller to comply with the request if it can identify the consumer and verify the third-party's authority to act on behalf of the consumer; the consumer may designate the third-party through actions like using an internet link or browser setting. Finally, Colorado allows consumers to use a user-selected universal opt-out mechanism to opt out of the processing of personal data for targeted advertising and the sale of personal data.

AB 466 creates a right to opt out that is most similar to the right to opt out in Colorado, except that AB 466 does not allow the Attorney General to establish a universal opt-out mechanism.

Right to Correct

Under Colorado and Connecticut law, a consumer has the right to correct inaccuracies in his or her personal data, taking into account the nature of the personal data and the purpose of the processing of the consumer's personal data. AB 466 creates a similar right. Utah does not create this right.

Exercising Consumer Rights

Under the sample state laws, a consumer may exercise any right by submitting a request to a controller that specifies the right being exercised, using a method established by the controller that is stated in the controller's privacy notice. Colorado requires that the method consider how consumers normally interact with the controller, the need for secure and reliable communication, and the ability of the controller to verify the identity of the consumer. Connecticut requires the method to be secure and reliable. Utah does not specify a similar requirement.

The sample state laws generally require a controller to respond to a consumer request within 45 days, subject to specified exceptions and possible time extensions. In Colorado and Connecticut, if the controller chooses not to act on a consumer's request, the controller must inform the consumer of the reasons for not acting and provide instructions for how to appeal the decision through a process

[11] Connecticut requires that the data be provided in a format that is portable and, to the extent technically feasible, readily usable. Utah requires that the data be provided in a format that is portable to the extent technically feasible and readily usable to the extent practicable. Colorado requires that the data be provided in a format that is portable and, to the extent technically feasible, readily usable.

[12] Profiling is defined as any form of automated processing of personal data to evaluate, analyze, or predict personal aspects related to an identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. Connecticut's right to opt out of data used for profiling applies only to decisions that are solely automated.

established by the controller. Utah requires that the controller inform the consumer of the reasons for not acting, but does not require controllers to implement an appeal process.

AB 466 is most similar to Colorado.

BUSINESS OBLIGATIONS

The sample state laws create similar business obligations. Generally, the sample state laws establish obligations for controllers, including the obligation to provide a privacy notice and disclosure of a consumer's right to opt out; obligations for processors, including the obligation to adhere to a controller's instructions and to assist in meeting the controller's obligations; and requirements for contracts between controllers and processors.

Controller Obligations

Privacy Notice

Under the sample state laws and AB 466, a controller must provide consumers with a reasonably accessible and clear privacy notice that includes all of the following:[13]

- The categories of personal data processed by the controller.
- The purpose for which the categories of personal data are processed.
- How consumers may exercise a right.
- The categories of personal data that the controller shares with third parties, if any.
- The categories of third parties, if any, with which the controller shares personal data.

Disclosure of Right to Opt-Out

Under the sample state laws and AB 466, any controller that sells a consumer's personal data or engages in targeted advertising must clearly and conspicuously disclose how a consumer may exercise the right to opt out of those activities. Colorado and Connecticut further specify that a controller must also disclose that the controller is engaging in these activities.

Duties Relating to Discrimination

Under the sample state laws and AB 466, a controller may not discriminate against a consumer for exercising a right. Prohibited discrimination includes: denying a good or service; charging a consumer a different price or rate; or providing a different level of quality of good or service. The sample state laws generally do not require a controller to provide a product or service when that product or service requires consumer data that the controller does not collect or maintain. Similarly, the same state laws do not prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering a good or service for no fee, if the consumer voluntarily participates in certain reward programs, or, in Utah and under AB 466, if the consumer has opted out of targeted advertising.

Colorado, Connecticut, and AB 466 also prohibit a controller from processing a consumer's personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers.

[13] Colorado and Connecticut also require that the privacy notice include the controller's contact information; Colorado also requires that the privacy notice include the method for opting out of certain consumer data processing.

Duty Regarding Sensitive Data

Under the sample state laws and AB 466, a controller generally must obtain a consumer's consent in order to process the consumer's sensitive data. Sensitive data is generally defined to mean personal data that reveals a person's racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or immigration status; personal data that concern's a person's medical history or medical condition; the processing of genetic personal data or biometric data for the purpose of identifying a specific individual; and specific geolocation data.[14] If the personal data concerns a known child, then the controller may only process the data in compliance with the federal Children's Online Privacy Protection Act.

Duty to Specify Purpose and Minimize Data Collection

Colorado and Connecticut require a controller to disclose the purpose for which the controller collects and processes personal data, and to limit the collection of personal data to what is adequate, relevant, and reasonably necessary with respect to the disclosed purpose. A controller may process data for another purpose only if the controller obtains the consumer's consent. AB 466 also includes this limitation.

Data Protection Assessment

Colorado and Connecticut generally require a controller to perform a data protection assessment for any of the controller's processing activities that present a heightened risk of harm to a consumer, including processing personal data for targeted advertising and certain consumer profiling, selling personal data, and processing sensitive data. The data protection assessment must include a risk-benefit analysis that considers the benefits the processing creates for the controller, the consumer, other stakeholders, and the public along with the risks to the consumer.[15] AB 466 also requires a controller to perform a data protection assessment.

Processor Obligations

Under the sample state laws, a processor must adhere to a controller's instructions and assist the controller in meeting the controller's obligations, including consumer rights requests, security, notification of a breach of security, and data protection assessments. AB 466 includes a similar provision.

Contract Between the Controller and Processor

Under the sample state laws and AB 466, controllers and processors of consumer data must enter into a contract regarding the data. The contract must include the instructions for processing data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the rights and obligations of each party. The contract also must require the processor to ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data. Generally, the contract must also require a processor, when engaging with a subcontractor, to use a

[14] Colorado, Connecticut, and AB 466 also include in this definition personal data from a known child; Colorado does not include specific geolocation data.

[15] The state Attorney General may request a controller's data protection assessment. The assessment is confidential, excluded from open records law, and remains protected by any applicable attorney-client privilege or work product protection.

written contract that requires the subcontractor to meet the same obligations as the processor with respect to personal data.[16]

Colorado, Connecticut, and AB 466 also require that the contract include the following terms:

- The controller may instruct the processor to delete or return all personal data to the controller at the end of the provision of services, unless retention is required by law.
- The processor must provide the controller with all information necessary to demonstrate compliance with the controller's obligations.
- The processor must allow and contribute to reasonable reviews of the processor's policies and technical and organizational measures in support of the law's obligations. The processor must provide a report of the review to the controller upon request. Colorado requires that this review take place at least annually.

Limitations on Business Obligations

The sample state laws and AB 466 establish certain limits on the obligations created for controllers and processors. The laws specify that the obligations do not restrict a controller's or processor's ability to perform certain activities, including the following:

- Complying with federal, state, or local laws, or with legal requests by governmental authorities.
- Cooperating with law enforcement in certain cases.
- Performing activities related to a legal claim.
- Providing a product requested by a consumer.
- Performing under a contract with a consumer.
- Conducting internal research to develop, improve, or repair products, services, or technology, or make certain repairs.
- Protecting a vital interest of the consumer or another individual.
- Engaging in certain research that is in the public interest.
- Performing protective activities related to security, identity theft, fraud, harassment, or malicious or deceptive activities.
- Assisting another person with any of the exempted activities.[17]

The sample state laws and AB 466 also specify certain limits relating to de-identified data, pseudonymous data, certain consumer requests, evidentiary privileges, privileged communication, and protected speech.

ENFORCEMENT

Unlike another prominent state data privacy law, California's Consumer Privacy Act, the sample state laws do not create a private right of action for violations of the law; instead, in Connecticut and Utah, the state Attorney General is responsible for enforcement, while in Colorado, the state Attorney General

[16] In Colorado and Connecticut, the controller may object to the subcontracting of processing.

[17] Connecticut and Utah also include effectuating a product recall in the list of exempt activities.

and district attorneys are responsible for enforcement. Colorado and Connecticut further specify that a violation of their law is a deceptive or unfair trade practice.

Under the sample state laws, the Attorney General (or, in Colorado, district attorney) generally must issue a notice of a violation prior to initiating an enforcement action and the state must provide an opportunity to cure the violation before initiating the enforcement action. Colorado and Connecticut provide discretion to the enforcer to determine that whether a cure is possible and specify a 60-day cure period, and Utah provides a 30-day cure period. Colorado's cure period sunsets on January 1, 2025.

Under AB 466, the Department of Justice (DOJ) and Department of Agriculture, Trade, and Consumer Protection (DATCP) may enforce violations in the name of the state. As under the sample state laws, DOJ or DATCP must issue a notice of violation prior to initiating an enforcement action, and the state must provide 30 days to cure the violation before initiating the enforcement action.[18] A violation is punishable by a civil forfeiture of up to $10,000. In addition to a forfeiture, the state may seek a permanent or temporary injunction to restrain any violation of the bill's provisions.

PW:TK:BL:kp;ksm

[18] The right to cure prior to the state initiating an enforcement action sunsets on July 1, 2029.