D R A F T

FOR DISCUSSION ONLY

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

TENTATIVE FIRST READING DRAFT

The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the drafting committee. They do not necessarily reflect the views of the Conference and its commissioners and the drafting committee and its members and reporter. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

May 20, 2020

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

The committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this act consists of the following individuals:

HARVEY S. PERLMAN	Nebraska, *Chair*
JAMES BOPP JR.	Indiana
STEPHEN Y. CHOW	Massachusetts
PARRELL D. GROSSMAN	North Dakota
JAMES C. McKAY JR.	District of Columbia
LARRY METZ	Florida
JAMES E. O'CONNOR	Nebraska
ROBERT J. TENNESSEN	Minnesota
KERRY TIPPER	Colorado
ANTHONY C. WISNIEWSKI	Maryland
CANDACE M. ZIERDT	Florida
DAVID V. ZVENYACH	Wisconsin
CARL H. LISMAN	Vermont, *President*
WILLIAM H. HENNING	Alabama, *Division Chair*

OTHER PARTICIPANTS

WILLIAM McGEVERAN	Minnesota, *Reporter*
MICHAEL AISENBERG	Virginia, *American Bar Association Advisor*
STEVEN L. WILLBORN	Nebraska, *Style Liaison*
TIM SCHNABEL	Illinois, *Executive Director*

Copies of this act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
111 N. Wabash Ave., Suite 1010
Chicago, Illinois 60602
312/450-6600
www.uniformlaws.org

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

TABLE OF CONTENTS

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

SECTION 1. SHORT TITLE. This [act] may be cited as the Collection and Use of Personally Identifiable Data Act.

SECTION 2. DEFINITIONS. In this [act]:

(1) "Data controller" means a person that, alone or jointly with others, determines the purposes and means of processing personal data.

(2) "Data processor" means a person that processes personal data on behalf of a data controller under the controller's direction.

(3) "Data subject" means an individual to whom personal data refers.

(4) "Deidentified", with respect to information, means lacking capacity to identify, describe, or be associated with a particular data subject, provided the data processor or data controller of the information makes no attempt to restore the capacity of the information to identify, describe, or be associated with the data subject and implements the following measures to prevent others from doing so:

(A) technical safeguards that reasonably prevent reidentification of the data subject;

(B) business processes that specifically prohibit reidentification of the information; and

(C) business processes that reasonably prevent inadvertent release of the data.

(5) "Device" means a physical object that connects to the Internet or to another device. Data related to a device, including a unique identification number and an Internet protocol address, is personal data if it can be associated with a particular data subject by using a reasonable amount of effort.

(6) “Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(7) “Person” means an individual, estate, business or nonprofit entity, or other legal entity. The term does not include a public corporation, government or governmental subdivision, agency, or instrumentality.

(8) “Personal data” means information that identifies or describes a particular data subject or that can be associated with a particular data subject by a reasonable amount of effort, whether or not the data has been collected directly from a data subject. The term includes probabilistic inferences about the data subject, including inferences derived from profiling and information that identifies a household or device if it can be associated with a particular data subject by a reasonable amount of effort. The term does not include deidentified data.

(9) “Processing” means an operation performed on personal data, whether or not by automated means, including use, storage, disclosure, analysis, and modification. “Process” has a corresponding meaning.

(10) “Profiling ” means a form of automated processing of personal data to evaluate, analyze, or predict a data subject’s economic status, health, demographic characteristics including race, gender, or sexual orientation, personal preferences, interests, character, reliability, behavior, social or political views, physical location, or movements. The term includes probabilistic inferences derived from personal data. The term does not include evaluation, analysis, or prediction based solely on a data subject’s current activity, including search queries, if no personal data is retained for future use after completion of the activity.

(11) “Publicly available data” means information that has been lawfully made available from federal, state, or local government records, or generally accessible and widely-distributed

media.

(12) "Sensitive data" means:

(A) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, activities or preferences related to gender or sexuality, or citizenship or immigration status;

(B) biometric and genetic data; or

(C) personal data about a data subject who is known to be under [13] years of age.

(13) "Sign" means, with present intent to authenticate or adopt a record:

(A) to execute or adopt a tangible symbol; or

(B) to attach to or logically associate with the record an electronic symbol, sound, or process.

(14) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. [The term includes a federally recognized Indian tribe.]

(15) "Targeted advertising" means advertising displayed to a data subject on the basis of profiling.

(16) "Transfer" means to convey personal data to the possession or control of another person.

Comment

The definition of "personal data" includes any information that incorporates specific personal identifiers, including name; a unique identification number such as a social security number; an individual number for financial or similar accounts; payment card information; a postal address; a telephone number; or an email address. The definition is not limited to such directly identifying informaton, however. A profile about a unique data subject may be personal data even if it lacks any of these traditional identifiers. When information can be used to make an association with a data subject through one or more intervening inferences using a reasonable amount of effort, that information qualifies as personal data. Similarly, information associated

with a device or a household is personal data if it can be associated with a particular data subject, even if the name of that data subject is not known to the relevant data controller or processor.

SECTION 3. SCOPE.

(a) This [act] applies to the commercial activities of a person that conducts business in this state or produces products or provides services targeted to this state, provided that the person:

(1) is the custodian of personal data concerning more than [50,000] data subjects in one year;

(2) earns more than [50] percent of its gross annual revenue directly from its activities as a data controller or data processor; or

(3) is a data processor acting on behalf of a data controller whose activities the processor knows or has reason to know satisfy paragraph (1) or (2).

(b) Subject to subsection (c), this [act] does not apply to:

(1) personal health information as defined under the Health Information Portability and Accountability Act, codified in scattered sections of 42 U.S.C., [as amended] when the custodian of the information is regulated by the Act;

(2) an activity involving personal information governed by the Fair Credit Reporting Act, 15 U.S.C. Section 1681 et seq. [as amended], or otherwise used to generate a consumer report, by a consumer reporting agency, as defined by 15 U.S.C. Section 1681a(f), by a furnisher of the information, or by a person procuring or using a consumer report;

(3) publicly available information;

(4) personal information collected, processed, sold, or disclosed by a financial institution as defined by the Gramm-Leach Bliley Act, 15 U.S.C. Section 6809(3) [as amended];

(5) personal information regulated by the Federal Family Educational Rights and

Privacy Act, 20 U.S.C. Section 1232 [as amended];

(6) state or local government; or

(7) personal data collected or retained by an employer with regard to its employees that is directly related to the employment relationship.

(c) The [Attorney General] may by regulation exempt other information or activities from this [act] or a portion of this [act], provided the collection, processing, transfer, or retention of the information or activity is regulated by law other than this [act].

(d) Nothing in this [act] may be construed to prevent the collection, authentication, maintenance, retention, disclosure, sale, processing, communication, or use of personal information necessary to:

(1) initiate or complete a transaction in goods or services that the data subject requested;

(2) protect against, prevent, detect, investigate, report on, prosecute, or remediate actual or potential:

(A) fraud;

(B) unauthorized transactions or claims;

(C) security incidents;

(D) malicious, deceptive, or illegal activity; or

(E) other legal liability;

(3) assist a person or government agency to conduct an activity under paragraph (2); or

(4) comply with or defend legal claims:

(A) setting requirements, standards, or expectations to limit or prevent

corruption, money laundering, or violation of export controls; or

(B) related to any of the activities under paragraph (2).

Comment

The scope section is one of the more contentious provisions of the Act. The issues memorandum outlines some of the issues yet to be resolved. The section has three functions. It first limits the applicability of the Act to larger enterprises or at least enterprises that do significant data collection and processing. Second, it specifically exempts certain data processes where privacy concerns have already been addressed. And, third, it exempts general uses of data collected from data subjects where the use or processing and retention of data should be reasonably be expected by data subjects when they submit data to others or is necessary to protect the interests of the data collector or processor from legal liability.

The issue of personal data privacy associated with a public health emergency like the current pandemic has not been addressed by the committee in this draft.

SECTION 4. DATA SUBJECT'S RIGHTS GENERALLY. With respect to a data subject's personal data, the data subject may exercise the following rights:

(1) to have a data controller confirm whether or not the controller has retained or is processing the data subject's personal data;

(2) to have a data controller provide a copy of the data subject's personal data under Section 5;

(3) to have a data controller correct inaccuracies in the data subject's personal data retained or processed by the data controller; or

(4) subject to Section 3, to have the data controller delete the data subject's personal data.

Comment

This section states the primary rights of data subjects in their personal data.

SECTION 5. DATA SUBJECT'S RIGHT TO COPY OF PERSONAL DATA.

(a) Upon request, a data controller shall provide a data subject with a copy of the data subject's personal data once during any 12-month period free of charge.

(b) A data controller may charge a reasonable fee based on actual administrative costs to comply with additional requests.

(c) If requests by a data subject are manifestly unreasonable or excessive, a data controller may refuse to act on the requests for a 12-month period.

(d) If a data controller collected a data subject's personal data directly from the data subject, the controller shall, to the extent technically feasible, provide the data in a way that would enable the data subject to transmit the data to another data controller by automated means.

SECTION 6. DATA SUBJECT'S RIGHTS RELATED TO TARGETED ADVERTISING AND PROFILING.

(a) A data subject has the right to restrict a data controller from processing or transferring personal data pertaining to the data subject for the purpose of:

(1) targeted advertising; or

(2) profiling that might result in providing or denying financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities.

(b) Before a data controller processes or transfers sensitive data for a purpose listed in subsection (a), the controller must receive affirmative consent from the data subject.

Comment

This section is based on several other proposals that distinguish between general personal data and that which is particularly sensitive. The data subject has the right to "opt out" if their general personal data is being used for targeted advertising or profiling that may impact important decisions made about them. The data subject must "opt in" to the use of their sensitive personal data for purposes of targeted advertising or profiling. Thus for example a data subject may have to take affirmative action to prevent the use of their name, address, or buying habits from being used to direct advertising in their direction. However, a data subject would have to give prior permission for the use of their genetic composition or health records.

SECTION 7. DATA SUBJECT'S RIGHTS, MEANS OF EXERCISING.

(a) A data subject may exercise a right under this [act] by notifying the data controller by any reasonable means of the data subject's intent to exercise the right. A parent of a child under age [18] may exercise a right on behalf of the child.

(b) A data controller shall comply with requests under this section without undue delay. If the controller has not complied with the request within [45 days] [a reasonable time] of receiving it, the controller shall notify the data subject who made the request and provide an explanation of the action being taken to comply with the request.

(c) A data controller shall make reasonable efforts to ensure that its response to a request by a data subjects to exercise a right under this [act] includes personal data in the possession or control of a data processor acting on the controller's behalf. The controller shall make a reasonable effort to notify the processor acting on its behalf when a data subject has exercised a right, and shall instruct the processor to adjust the data subject's personal data to be consistent with the controller's response to the data subject's request.

(d) A data controller shall adopt a privacy commitment under Section 8 that describes the procedures to be used in exercising a right under this [act]. The data privacy officer for the controller shall approve this commitment. An explanation of the procedures in clear language must be reasonably accessible to all data subjects. The procedures must include an opportunity to appeal an initial determination by the controller. An appeal of an initial determination must be reviewed under supervision of the data privacy officer. If a data subject is dissatisfied with the final disposition of an appeal, the processor shall inform the data subject of the procedure to [file a complaint] with the [Attorney General].

SECTION 8. DATA PRIVACY COMMITMENT.

(a) A data controller that collects, uses, processes or retains personal data of a data subject shall file a data privacy commitment with the [Attorney General]. The commitment must contain the following:

(1) the precise method by which a data subject may communicate with the controller in order to exercise a right under Section 4;

(2) the manner and extent to which the controller intends to use or transfer to others the personal data of data subjects, the purposes of the use or transfer, and a simple method by which a data subject can withdraw consent for the use or transfer;

(3) the manner in which the controller intends to respond to a data subject's request for correction of personal data including a policy to authenticate the request and to notify the processor to make the correction;

(4) the manner in which the controller intends to respond to a data subject's request to delete personal data; and

(5) any conditions on the exercise of a right made necessary by the nature of the controller's business or industry, provided that the substance of the rights are not adversely affected.

(b) A data controller that files a data privacy commitment shall publish the commitment on its website and other places where it will be reasonably accessible to data subjects.

(c) The [Attorney General] may review the privacy commitment of a data controller at any time and may institute an action under Section 19 to determine whether the commitment complies with this [act].

Comment

The privacy commitment required by this section is envisioned as permitting the incorporation and use of voluntary consensus standards or best practices in compliance with this Act. Statutory provisions directing the means of compliance with the Act are difficult to apply to the variety of different industries and purposes for which data is collected and used. Thus this section requires a data controller to publish how they intend to comply with the Act. The incentive to do so is that following their own commitments provides a safe harbor for any private right of action authorized in section 20. The terms of the commitment remain subject to regulatory enforcement by the state Attorney General if it fails to meet the substantive standards of privacy protection provided in this Act.

SECTION 9. DATA CONTROLLER'S OR DATA PROCESSOR'S DUTY OF LOYALTY.

(a) A data controller or data processor shall not engage in processing practices that are unfair, deceptive, or abusive. Unfair processing includes processing or use of data that exposes the data subject to an unreasonable and material risk of harm.

(b) The [Attorney General] may adopt regulations that identify particular processing practices as unfair, deceptive, or abusive.

(c) A violation of subsection (a) is subject to enforcement under Section 19.

(d) A data controller or data processor that engages in a processing practice after a final decision in an enforcement action that the practice is unfair, deceptive, or abusive is subject to a private cause of action by a data subject under Section 20.

SECTION 10. DATA CONTROLLER'S OR DATA PROCESSOR'S DUTY OF DATA SECURITY. A data controller or data processor shall adopt, implement, and maintain reasonable data security measures to protect the confidentiality and integrity of personal data in the controller's or processor's possession or control. Reasonable data security measures include appropriate administrative, technical, and physical safeguards. Data security measures must be evaluated as part of the data privacy assessment under Section 16. An evaluation of the

reasonableness of data security measures must take into consideration the magnitude and likelihood of security risks and potential resulting harms, the resources available to the controller or processor, and industry practices among other controllers or processors that are similarly situated. Reasonable security practices may be derived from best practices promulgated by professional organizations, government entities, or other specialized sources.

SECTION 11. DATA CONTROLLER'S OR DATA PROCESSOR'S DUTY OF DATA MINIMIZATION. A data controller or data processor shall not collect, process, or retain more personal data than necessary to achieve the purposes of processing. When a controller transfers personal data to a processor, the controller may transfer only as much personal data as necessary to complete the processor's processing. A processor shall delete, deidentify, or return personal data to the relevant controller at end of the provision of services or as otherwise specified by agreement.

SECTION 12. DATA CONTROLLER'S DUTY OF TRANSPARENCY.

(a) A data controller shall provide data subjects with a reasonably accessible, clear, and meaningful privacy notice that discloses:

(1) categories of personal data collected or processed by or on behalf of the controller;

(2) the purpose for processing personal data by the controller or on the controller's behalf;

(3) categories of any personal data that the controller provides to a data processor or any other person;

(4) categories of processors or other persons that receive personal data from the controller;

(5) the nature and purpose of any profiling of data subjects using personal data; and

(6) means by which a data subject may exercise a right under this [act].

(b) The notice under this section must clearly and conspicuously designate at least two methods for a data subject to contact the data controller to exercise a right under this [act]. At least one of these methods must be a toll-free telephone number. If the controller maintains an Internet website, at least one of these methods must be contact through the website.

(c) If a data controller processes personal data for targeted advertising, or provides personal data to a data processor or other person to process for targeted advertising, the notice under this section must clearly and conspicuously disclose the processing and must provide an automated Internet-based mechanism for the data subject to exercise the right to opt out of targeted advertising.

(d) The notice under this section must be reasonably available at the time personal data is collected from a data subject.

SECTION 13. DATA CONTROLLER'S DUTY OF PURPOSE LIMITATION. A data controller shall not process personal data, or permit a data processor or other person to process personal data, for a purpose that is not specified in the notice to data subjects under Section 12.

SECTION 14. DATA PROCESSING BY WRITTEN AGREEMENT.

(a) Processing of personal data by a data processor that is not the data controller must be governed by an agreement in a record between the processor and controller that is binding on both parties and that sets out the nature and purpose of the processing, the type of personal data subject to processing including identification of any sensitive data, the duration of the

processing, and the obligations and rights of both parties. The agreement must also contain the following terms:

(1) The processor shall adhere to the instructions of the controller regarding the processing of the data and shall assist the controller by adopting appropriate technological or organizational measures to fulfill its duties under this [act].

(2) The processor shall not process personal data for a purpose other than the purposes of the processing provided in the notice to data subjects under Section 16 and purposes stated in the agreement.

(3) The controller has a reasonable right to audit the conduct of the processor, and the processor shall make available to the controller all information necessary to demonstrate the processor's compliance with the requirements of this [act] and with the requirements of the agreement between the controller and processor.

(4) The processor may not transfer the personal data to another data processor or any other person without the permission of the controller. A transfer to another processor must be governed by an agreement in a record that imposes all the same obligations on the recipient of the personal data that are imposed on the processor in the agreement between the controller and the processor, even if the recipient is not subject to this [act].

(5) The data controller may indemnify a data processor for liability of the processor under this [act].

(b) Processing personal data without a written agreement that complies with this section is an [unfair act and practice] subject to enforcement under Section 19. A data controller that authorizes the processing of information by another without an agreement reasonably consistent with this section is subject to a private cause of action under Section 20.

Comment

The entity that collects data (data controller) is often different from the entity that processes that data (data processor). It is the data controller who normally has the direct relationship with the data subject and makes commitments to the data subject regarding the future use and processing the data. The concern remains however whether data processors will comply with the commitments made by the data controller. Similarly a data subject is most likely to assert their rights of access, correction, or deletion against the controller and in most instances will not know the identity of any data processor using the data.

The primary mechanism for enforcement of data subject's rights must accordingly be focused on the data controller. However, in order to insure processor compliance, this section requires that all processing be accomplished pursuant to a written agreement that binds the processor to the obligations and commitments of the controller and requires the processor cooperate with the controller in satisfying legitimate consumer requests.

It has been argued by some in the industry that this simple view may be unworkable given the current methods and mechanisms of data use and processing. It may be difficult for processors to "find" a particular data subject's data given the technological way data is stored. The committee will need to explore this issue further.

SECTION 15. DESIGNATION OF DATA PRIVACY OFFICER.

(a) A data controller or data processor shall designate an individual employee or contractor to serve as the controller's or processor's data privacy officer.

(b) A data privacy officer must have qualifications appropriate for supervision of the data controller's or data processor's responsibilities under this [act]. Minimum qualifications depend on the scale, complexity, and risk of the processing of the controller or processor.

(c) A data privacy officer is responsible for the data privacy assessment required by Section 16 and shall sign the data privacy assessment personally.

(d) If a data privacy officer designated under subsection (a) spends a reasonable amount of time directing a data controller's or data processor's duties under this [act], the officer may perform other duties for the controller, processor, or other persons. If the officer is not an employee of the controller or processor, the controller or processor and the officer must execute an agreement in a record that clearly specifies the officer's duties. An individual may serve as an

officer for more than one controller or processor.

(e) A data privacy officer may assign or delegate other persons to complete tasks under supervision, but the officer must retain authority over the completion of the tasks.

Comment

This section requires the designation of someone in entities that collect and use data to designate an individual as the data privacy officer. The function of the officer is to conduct the data privacy assessment required by section 16. The section is drafted to assure that for many entities this may be an assignment added to the responsibilities of another official or it may be a function that can be contracted out to a firm who specializes in privacy assessment.

SECTION 16. DATA PRIVACY ASSESSMENT. A data controller or data processor shall prepare in a record, to the extent not previously prepared, a data privacy assessment of each processing undertaken by the controller or processor to evaluate all material risks, harms, and benefits of processing.

(a) A data privacy assessment must be completed about each processing every two years. The assessment must be updated any time a change in processing activities may materially affect the risks, harms, and benefits of processing.

(b) A data privacy assessment shall evaluate the:

(1) type of personal data being processed;

(2) presence of any sensitive data among the personal data being processed;

(3) scale of the processing activities;

(4) context in which personal data is collected and processed;

(5) seriousness of privacy risks imposed on data subjects as a result of the processing;

(6) likelihood of privacy risks causing harm to data subjects as a result of the processing;

(7) benefits that may flow directly or indirectly to the data controller or data processor, data subjects, the public, or others as a result of the processing;

(8) resources reasonably available to the controller or processor for addressing privacy risks, taking account of the revenue generated by the processing; and

(9) measures the controller or processor has undertaken to mitigate any privacy risks.

(c) Privacy risks evaluated in a data privacy assessment must encompass risks of all potential harms to data subjects, including:

(1) accidental disclosure, theft, or other breaches of security causing personal data to be revealed to persons without authorization;

(2) identity theft;

(3) harassment;

(4) unwanted profiling;

(5) stigmatization or reputational harm;

(6) emotional harm including anxiety, embarrassment, fear, and other demonstrable mental harms; and

(7) other foreseeable outcomes that would be highly offensive to a reasonable person.

(d) To satisfy its obligation under this section, a data processor may adopt a data privacy assessment completed by a data controller concerning the same personal data.

(e) A data controller or data processor shall retain a record of each data privacy assessment for 10 years after completion. Upon request of the [Attorney General] in connection with [an investigation], a controller or processor shall provide a record of each current and

former data privacy assessment.

(f) Whether or not a data controller or data processor has provided a data privacy assessment to the [Attorney General], an assessment is confidential business information [and is not subject to public records requests or subject to compulsory civil discovery in any court].

Legislative Note: *The state should include appropriate language in subsection 6(f) exempting data privacy assessments from open records requests and compulsory civil discovery requests to the maximum extent possible under state law.*

Comment

The primary obligation to consider and protect personal data is placed on the data controller who is the person who collects the data and directs the processing. The controller is also normally the person who deals directly with the data subject. This section requires the data controller to assess the privacy risks associated with each effort to process personal data. To encourage an open assessment of the benefits and risks, the assessment should be protected from disclosure. Otherwise the assessment will be done in a way to protect against the potential for legal liability.

While the section appears to impose the obligation of assessment on both data controllers and data processors, subjection (d) allows the processor to satisfy its obligation by obtaining the assessment of the controller. This would encourage processors to assure that their clients comply with this section and provide the processor the controller's assessment and means of mitigation of risks.

SECTION 17. NONDISCRIMINATION.

(a) A data controller shall not discriminate against a data subject for exercising a right to access and copy the data subject's personal data or requesting correction of inaccuracies in personal data pursuant to Section 4 by denying a good or service, charging a different rate, or providing a different level of quality.

(b) Subject to subsection (a), a data controller may adopt and enforce as a condition for access to its goods or services that consumers permit the processing of their personal data.

Comment

Nondiscrimination provisions have been subject to considerable concern. To the extent a data subject's interest in privacy is considered a "right", it would follow that the exercise of that

right should not result in discrimination. However, there are businesses whose business plan is built on providing goods and services in exchange for access to personal data. As long as this is made clear to data subjects, they should not be entitled to the goods or services without being willing to make the exchange. However, this should not implicate their right to access the data held about them or to correct inaccurate data. The section acknowledges here that the right to delete or withhold data cannot be subject to the nondiscrimination mandate.

SECTION 18. WAIVER PROHIBITED. A provision of a contract or agreement that purports to waive or limit rights or duties imposed by this [act] is contrary to public policy and is void and unenforceable, except that a controller may indemnify a processor for liability under Section 14(a)(5).

SECTION 19. ENFORCEMENT BY [ATTORNEY GENERAL].

(a) An act or practice by a person covered by this [act] is an [unfair practice] under the [cite consumer protection law] of this state if the [act or practice]:

(1) substantially fails to comply with a provision of this [act]; or

(2) deprives data subjects of a right accorded by this [act].

(b) The authority of the [Attorney General] to bring an action to enforce the provisions of the [cite consumer protection law] includes enforcement of this [act].

(c) The [Attorney General] may adopt rules and regulations to implement this [act] in accordance with the [cite administrative procedure act].

(d) In adopting rules and regulations and in bringing enforcement actions under this [act], the [Attorney General] shall consider the need to promote uniformity within a particular industry and among the states by:

(1) examining and, where appropriate, adopting rules and regulations consistent with the rules and regulations adopted in other states; and

(2) giving due deference to any voluntary consensus standards adopted by an industry in accordance with a process that is open, allows balanced participation by interested

parties including representatives of data subjects, is conducted through a fair process, and provides an independent appeals process.

Legislative Note: *In subsection (a), the state should use the term for unfair practice that is used in the state's consumer protection law.*

In subsection (a), the state should cite to the state's consumer protection law.

Comment

The states vary in the powers and authority granted to the Attorney General, although most states authorize the Attorney General to enforce their Consumer Protection Act. Under the Consumer Protection Act, the Attorney General can often bring a civil action to enforce the act and can seek civil penalties and injunctive relief. Such authority should be extended to enforce the provisions of this Act.

States also vary on the extent to which the Attorney General adopts rules and regulations to interpret and enforce statutory provisions. Unless prohibited by other law, the Attorney General should be specifically directed to adopt rules and regulations pursuant to this act and in accordance with the state Administrative Procedure Act.

Subsection (d) attempts to encourage uniformity among the states by requiring the Attorney General to consider actions in other states. Adoption of this Act with this provision would lead naturally to the development, by state attorney general's or other groups of a set of model rules and regulations for implementing the Act.

The act also seeks to encourage the adoption and implementation of voluntary consensus standards by industries as long as they are adopted in an open, fair, and balanced process. The criteria are modeled on the Office of Management and Budget Circular a-119 which governs federal administrative agencies.

SECTION 20. PRIVATE RIGHT OF ACTION.

(a) Unless authorized by this section, a data subject may not bring a private action in federal or state court alleging a violation of this [act].

(b) A data subject may bring a private action for damages against a person that negligently or intentionally:

(1) processes the data subject's personal data without filing and publishing a privacy commitment under Section 8;

(2) processes the data subject's personal data in a way that materially violates the privacy commitment governing the data under Section 8;

(3) processes the data subject's data after a final determination in an action under Section 19 that the privacy commitment governing the data is an [unfair practice];

(4) engages in a practice with respect to the data subject's data after a final decision in an enforcement action finding that the practice is [unfair, deceptive, or abusive]; or

(5) processes a data subject's data without an agreement under Section 14.

(b) Damages available to a person in a suit under this section are limited to actual damages or $[100], whichever is greater.

(c) Evidence about the development or results of a data privacy assessment is not subject to compulsory discovery in a civil suit brought under this [act] and must be treated by the court in the same manner as a confidential offer of settlement, unless a data controller or data processor voluntarily introduces evidence related to the assessment. If a controller or processor voluntarily introduces evidence related to the assessment, admissibility and discoverability of evidence related to the assessment must be handled in accordance with the court's ordinary rules of evidence.

Comment

This section provides a limited private cause of action to persons injured by specified violations of the Act. Whether or not to authorize a private cause of action has been a matter of considerable controversy. The substantive provisions of any data privacy act must be broad in order to encompass the wide variety of data uses and industries to which it applies. Such provisions make it difficult for data controller or processors to assure in advance that it has met all technical requirements and provides plaintiffs and their lawyers considerable leverage to force settlements and large judgments. On the other hand, leaving enforcement solely to a public agency, particularly a State Attorney General's office, is subject to the resource allocation and priorities of each office.

Section 20 attempts to respond to both concerns. Private causes of action are limited to circumstances in which the obligation on a data controller or processor is either clear or can be

tailored by the controller or processor to create a safe harbor. Conduct is only actionable on proof of negligence or intentional conduct. Of particular importance is section 8 which requires a data controller to publish and file with the Attorney General a "privacy commitment"—a document that would specify the manner in which data subjects may exercise their rights under the act and the method in which the controller will respond to the assertion of those rights. This would allow an entity to adopt best practices or voluntary consensus standards particular to its industry and the nature of its data processing.

The privacy commitment would be subject to review by the Attorney General and through regulatory enforcement could be rejected. However, as long as the commitment was enforce, compliance would serve as a safe harbor from private actions. Violations of the commitment or failure to publish a commitment would be subject to a private cause of action.

The section also authorizes a private cause of action where a data controller fails to establish a written agreement for the processing of personal data. Most of the obligations under the Act are imposed on the controller as the entity that is in a direct relationship with the data subject. However, it is essential the controller, through contract, impose the same obligations on a data processor.

SECTION 21. UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

SECTION 22. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT. This [act] modifies, limits, and supersedes the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001, et seq., but does not modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

SECTION 23. SEVERABILITY. If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act] which can be given effect without the invalid provision or application, and to this end the provisions of this [act] are severable.

Legislative Note: *Include this section only if this state lacks a general severability statute or a decision by the highest court of this state stating a general rule of severability.*

SECTION 24. EFFECTIVE DATE. This [act] takes effect [180 days] after the date of enactment.

Comment

The effective date depends on the realistic time it would take for entities to bring themselves into compliance with the Act. To the extent the Act ultimately requires adjustments in technology and publications, a longer effective date is appropriate. Entities in California after enactment of the CCPA had almost two years to achieve compliance before the Act became effective. It may also be true that some sections of the Act might lend themselves to earlier effectiveness. The committee thus is reserving proposing an effective date or dates until it decides on the substantive provisions.