D R A F T

FOR DISCUSSION ONLY

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

April 24, 2020 Drafting Committee Meeting

Redline 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.

April 21, 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 TIPPPER	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" or "controller" means a person who, alone or jointly with others, determines the purposes and means~~, and~~ of processing ~~of~~ personal data.

~~(2) "Data custodian" or "custodian" refers to both data controllers and data processors who have possession or control of personal data or deidentified data.~~

(3) "Data processor" or "processor" means a person who processes personal data on behalf of a data controller and under that data controller's direction.

(4) "Data subject" means the individual~~, device, or household~~ to whom personal data refers.

(5) "Deidentified" means that the capacity of information to identify, describe, or be associated with any particular data subject ~~individual, device, or household~~ has been eliminated, provided the custodian of the information makes no attempt to restore the capacity ~~fo~~of the information to identify, describe, or be associated with any particular data subject ~~reidentify the information~~ and implements the following measures to prevent others from doing so:

(A) Technical safeguards that reasonably prevent reidentification of the ~~individual, device, or household~~data subject to whom the information may pertain;~~.~~

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

(C) Business processes that reasonably prevent inadvertent release of deidentified data.

(6) “Device” means any physical object that connects to the internet or to another device. Data related to a device, including unique identification numbers and IP addresses, is personal data if it can be associated with a particular data subject by using a reasonable amount of effort.

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

(8) “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.

(9) “Personal data” means information that identifies or describes a particular ~~individual~~ data subject and information that can be associated with a particular ~~individual~~ data subject by using a reasonable amount of effort. Personal data need not have been collected directly from a data subject. Probabilistic inferences about an individual, including inferences derived from profiling, are included in the definition of personal data. –Information that identifies a household or a device is personal ~~date~~ data if it can be associated with a particular ~~individual~~ data subject by using a reasonable amount of effort. Deidentified data is not personal data.

(10) “Processing ” means any operation performed on personal data , whether or not by automated means, including use, storage, disclosure, analysis, ~~and~~ or modification.

(11) “Profiling ” means any 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. Profiling 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 the completion of the

activity. Probabilistic inferences derived from profiling are personal data.

(12) "Public available data " means information that has been made available from federal, state, or local government records in accordance with law, provided the information is being used in a manner consistent with any conditions on its use imposed by law.

(13) "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; and

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

(14) "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.

(15) "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.]

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

(17) "Transfer" means to convey personal data into the possession or control of another custodian.

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 who conducts business [in the State of X] or produces products or provides services targeted to [the State of X], provided that the person:

(1) is the custodian of personal data concerning more than [50,000] ~~individuals, devices, or households~~data subjects in one year,

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

(3) is a data processor acting on behalf of a data controller whose activities the data processor knows or has reason to know satisfy the requirements of this section.

(b) This Act does not apply to

(1) personal health information as defined under the Health Information Portability and Accountability Act [CITE] [and regulations] when the custodian of that data is regulated by that statute.

(2) an activity involving personal information governed by the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code, or otherwise used to generate a consumer report, by a consumer reporting agency, as defined by 15 U.S.C. Sec. 1681a(f), by a furnisher of information, or by a person procuring or using a consumer report.

(3) publicly available information. ~~For purposes of this section, publicly available~~

~~information means information that is lawfully made available from federal, State, or local government records, or generally accessible or widely-distributed media.~~

(4) personal information collected, processed, sold, or disclosed by a financial institution as defined by 15 U.S.C. § 6809(3) pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102).

(5) personal information regulated by the Federal Family Educational Rights and Privacy Act, 20 U.S.C. 1232 and its implementing regulations.

(~~5~~6) This [act] does not apply to state or local government entities.

(~~6~~7) Personal data collected or retained by an employer with regard to its employees that is directly related to the employment relationship.

(~~7~~8) The [Attorney General] may by regulation exempt other information or transactions from this Act or a portion of this act, provided the collection, processing, transfer, or retention of the information is regulated by other law.

(c) Nothing in this act shall prevent the collection, authentication, maintenance, retention, disclosure, sale, processing, communication, or use of personal information necessary to:

(1) Initiate or ~~C~~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:

(i) Fraud;

(ii) Unauthorized transactions or claims;

(iii) Security incidents;

(iv) Malicious, deceptive, or illegal activity; or

(v) Other legal liability;

(3) Assist another person, entity, or government agency in conducting any of the activities specified in subsection (~~1~~2); or

(4) Comply with or defend claims under federal, state, or local laws, regulations, rules, guidance, or recommendations:

(i) Setting requirements, standards, or expectations to limit or prevent corruption, money laundering, export controls; or

(ii) Related to any of the activities specified in subsection (~~1~~2) of this subsection.

SECTION 4. DATA SUBJECT'S RIGHTS. Data subjects may exercise, as provided in this Act, the following rights with respect to their personal data:

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

(2) The right to be provided by a data controller of a copy of the data subject's personal data in accordance with section 5 of this act.

(3) The right to have a data controller correct inaccuracies in the data subjects personal data retained or processed by the data controller.

(4) Subject to section 3 of this Act, t~~T~~he right~~, subject to section 3,~~ to have the data controller delete the data subject's personal data.

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

(a) In implementing the data subject's right to a copy of personal data held by the data controller, the following rules apply:

(1) Upon request, a data controller must provide a data subject with a copy of the

data subject's personal data once per year free of charge.

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

(3) If requests by a data subject are manifestly unreasonable or excessive, the data controller may refuse to act on the requests for one year.

(4) If the data controller collected the data subject's personal data directly from the data subject, the copy should, to the extent technically feasible, be provided in a way that would enable the data subject to transmit the data to another data controller by automated means.

SECTION 6. RIGHTS RELATED TO TARGETED ADVERTISING AND PROFILING.

(a) A data subject has the right to restrict a data controller from processing or transfer ring personal data pertaining to the data subject (an "opt out") for purposes of

(1) targeted advertising;

(2) profiling in furtherance of decisions that result in a provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities~~, such as food and water~~.

(b) If a controller processes or transfer s sensitive data for the purposes listed in subsection (a), the controller must receive affirmative consent (an "opt in") from the data subject before undertaking such processing or transfer.

SECTION 7. DATA SUBJECT RIGHTS GENERALLY.

(a) A data subject may exercise rights under section 4 of this act by notifying the controller by any reasonable means of the data subject's intent to exercise one or more of these

rights. Parents of a [minor child] may exercise these rights on behalf of the [minor child].

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

(c) A data controller shall make reasonable efforts to ensure that its responses to requests by data subjects to exercise rights under this [act] include personal data in the possession or control of data processors acting on the controller's behalf. The data controller shall make reasonable efforts to notify processors acting on its behalf when a data subject has exercised these rights, 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 pursuant to section 8 of this act which will describe the procedures to be used in exercising the rights under this act. The data privacy officer for a data controller shall approve such commitment. An explanation of the procedures in clear language shall be reasonably accessible to all data subjects. The procedures shall include an opportunity to appeal an initial determination by the data controller. Appeals of an initial determination shall be reviewed under the supervision of the data privacy officer. If a data subject is dissatisfied with the final disposition of an appeal, the data 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 who collects, uses, processes or retains personal data of a data subject, shall file with the [Attorney General] a data privacy commitment. Such commitment shall set forth the following consistent with the requirements of this Act:

(1) The precise method by which a data subject may communicate with the data controller in order to exercise the rights stated in Section 4.

(2) The manner and extent to which the person intends to use or transfer to others the personal data of data subjects, the purposes of such use or transfer, and a simplified method by which the data subject can withdraw consent for such use or transfer as authorized by this act.

(3) The manner in which the person intends to respond to a data subjects request for correction of personal data including any policy to authenticate the request and to notify any data processor to make the correction.

(4) The manner by which the person intends to respond to a data subjects request to delete personal data.

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

(b) A person who files a data privacy commitment shall also publish the commitment on its website and other points where it will be reasonably accessible to data subjects. ~~transactions between the data subject and the data controller take place.~~

(c) The [Attorney General] may at any time review the privacy commitment of any person and may institute a regulatory action ~~to determine whether the commitment represents an unfair or deceptive practice in that it does not provide reasonable protection for a data subject's privacy or the subject's rights with regard to its personal data as provided in this Act.~~pursuant to Section 19 to determine whether the commitment satisfies the provisions of this Act.

SECTION 9. ~~CUSTODIAN'S~~ CONTROLLER'S ~~AND~~OR PROCESSOR'S DUTY OF LOYALTY.

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

(b) The [Attorney General] may adopt regulations declaring particular processing practices to be unfair, deceptive, or abusive.

(c) A violation of subsection (a) shall be subject to regulatory enforcement under section 19.

(d) A data ~~custodian~~ controller or processor who engages in a practice after the final decision in the regulatory enforcement action that the practice is unfair, deceptive, or abusive under subsection (b) shall be subject to a private cause of action by a data subject under section 20.

SECTION 10. ~~CUSTODIAN'S~~ CONTROLLER'S ~~AND~~OR PROCESSOR'S DUTY OF DATA SECURITY. A data ~~custodian~~ controller or processor shall adopt, implement, and maintain reasonable data security measures to protect the confidentiality and integrity of personal data in the ~~custodian's~~ controller's or processor's possession or control. Reasonable data security measures shall include administrative, technical, and physical safeguards as appropriate. Data security measures shall be evaluated as part of the data privacy assessment required under this [act]. An evaluation of the reasonableness of data security measures shall take into consideration the magnitude and likelihood of security risks and potential resulting harms, the resources available to the ~~custodian~~controller or processor, and industry practices among other ~~custodians~~ controllers or processors who are similarly situated. Reasonable security practices may be

derived from best practices promulgated by professional organizations, government entities, or other specialized sources.

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

SECTION 12. CONTROLLER'S DUTY OF TRANSPARENCY.

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

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

(2) purposes for processing of personal data, either by the controller or on the controller's behalf;

(3) categories of personal data that the controller provides to processors or to any other persons;

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

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

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

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

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

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

SECTION 13. CONTROLLER'S DUTY OF PURPOSE LIMITATION. A controller shall not process personal data, or permit processors or other persons to process personal data, for purposes that are not specified in the notice to data subjects required by this [act].

SECTION 14. DATA PROCESSING BY WRITTEN AGREEMENT.

(a) Processing of personal data by a data processor who is not the data controller shall be governed by a written agreement between the processor and the data 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 the processing (including the identification of any sensitive data), the duration of the processing, and the obligations and rights of both parties. The written agreement shall also

provide:

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

(2) the purposes of the data processing as provided in the notice to data subjects and that the data processor shall not process personal data for any purpose other than that stated in the agreement.

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

(4) the data processor may not transfer the personal data to another processor or to any other person without the permission of the controller. Any such transfer must be governed by a written contract that imposes all the same obligations on the recipient of the personal data that are imposed on the processor in the contract between the controller and the processor, regardless of whether the recipient is otherwise subject to this [act].

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

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

SECTION 15. DESIGNATION OF DATA PRIVACY OFFICER. A data

~~custodian~~controller ~~and~~or processor shall designate an individual employee or contractor to serve as the ~~custodian~~controller ~~and~~or processor's data privacy officer.

(a) A data privacy officer shall have qualifications appropriate for the supervision of the ~~custodian~~controller ~~and~~or processor's responsibilities under this [act]. Minimum qualifications shall depend on the scale, complexity, and risks of the data processing activities undertaken by the ~~custodian~~controller ~~and~~or processor.

(b) A data privacy officer shall be responsible for the data privacy assessments required by this [act] and shall sign each data privacy assessment personally.

(c) A data privacy officer may perform other duties for the ~~custodian~~controller ~~and~~or processor or for other persons, provided the data privacy officer spends a reasonably sufficient amount of time directing a ~~custodian~~controller ~~and~~or processor's duties under [this law]. If a data privacy officer is not an employee of the ~~custodian~~controller ~~and~~or processor, the ~~custodian~~controller ~~and~~or processor and the data privacy officer must execute a written agreement that clearly specifies the data privacy officer's duties. An individual may serve as a data privacy officer for more than one data ~~custodian~~controller ~~and~~or processor.

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

SECTION 16. DATA PRIVACY ASSESSMENT. A ~~custodian~~controller ~~and~~or processor must conduct, to the extent not previously conducted, a written data privacy assessment of each data processing activity undertaken by the ~~custodian~~controller ~~and~~or processor, in order to evaluate all material risks, harms, and benefits of processing.

(a) A data privacy assessment shall be completed about each data processing activity every two years. It shall be updated any time a change in processing activities may materially

increase privacy risks to data subjects.

(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 ~~custodian~~controller ~~and~~or processor, data subjects, the public, or others as a result of the processing;

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

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

(c) Privacy risks evaluated in a data privacy assessment shall 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 the reasonable person.

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

(e) A data ~~custodian~~controller ~~and~~or processor must retain a written copy of all data privacy assessments for ten years after their completion. Upon request of the [Attorney General] in connection with [an investigation], a data ~~custodian~~controller ~~and~~or processor must provide copies of all current and former data privacy assessments.

(f) Whether or not a data ~~custodian~~controller ~~and~~or processor has provided data privacy assessments to the Attorney General, a data privacy 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 data subjects for exercising their rights to access and copy their personal data or to request correction of inaccuracies in their personal data pursuant to section 4 by denying goods and services, charging different rates, or providing a different level of quality.

(b) Subject to subsection (a) of this section, 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.

SECTION 18. WAIVERS PROHIBITED. Any 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 shall be void and unenforceable, except that a controller may indemnify a processor for liability under this [act].

SECTION 19. REGULATORY ENFORCEMENT.

~~(a) The [Attorney General] may adopt rules and regulations as authorized by this act. The adoption and enforcement of such rules and regulations shall be in accordance with [The Administrative Procedure Act.].~~

~~(b) The authority of the [Attorney General] to bring an action to enforce the provisions of [The Consumer Protection Act] is extended to enforce the provisions of this act.~~

(a) An act or practice by an entity covered by this Act shall be construed as an [unfair, deceptive, abusive] act or practice under the [consumer protection law] of this State if such act or practice:

(1) substantially fails to comply with the provisions of this Act, ~~and~~or

(2) deprives data subjects of the rights accorded by this A~~c~~ct.

(b) The authority of the Attorney General to bring an action to enforce the provisions of the [consumer protection law] is extended to enforce the provisions of this Act.

(c) The Attorney General may adopt rules and regulations to implement the provisions of this Act. Such rules and regulations shall be adopted in accordance with the [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: *The state should include appropriate language cross-referencing the particular powers of the Attorney General that will be applied to enforcement of this statute and the applicable penalties.*

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 who negligently or intentionally: ~~alleging the following violations of the act:~~

(1) ~~Processing~~ Processes the data subject's personal data without filing and publishing a privacy commitment pursuant to ~~s~~Section 8 of this Act;

(2) ~~Processing~~ Processes the data subject's personal data in a way that materially violates the privacy commitment governing the data as required by Section 8 of this Act;

(3) ~~Processing~~ Processes the data subject's data after a final determination in a regulatory action pursuant to Section 19 of this Act that the privacy commitment governing the data is an [unfair, deceptive, or abusive practice];

(4) ~~A data controller or data processor engages~~Engages in a practice with respect to the data subject's data after a final decision in a regulatory enforcement action finding that the practice is [unfair, deceptive, or abusive].

(5) ~~A violation of section 14 of this Act~~Processes a data subject's data without an

agreement pursuant to Section 14 of this Act.

(b) Damages available to a person in a suit under this section shall be actual damages or damages of [$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 shall be treated by the court in the same manner as a confidential offer of settlement, unless a data ~~custodian~~controller ~~and~~or processor voluntarily introduces evidence related to a data privacy assessment. If a data ~~custodian~~controller ~~and~~or processor voluntarily introduces evidence related to a data privacy assessment, admissibility and discoverability of evidence related to that data privacy assessment shall 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 ~~custodian~~controller ~~and~~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 ~~custodian~~controller ~~and~~or processor~~s~~ is either clear or can be tailored by the ~~custodian~~controller ~~and~~ 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 ~~codes of conduct~~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.