D R A F T

FOR DISCUSSION ONLY

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

OCTOBER 16–17, 2020 DRAFTING COMMITTEE MEETING

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.

October 12, 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

JANE BAMBAUER	Arizona, *Reporter*
MICHAEL AISENBERG	Virginia, *American Bar Association Advisor*
DANIEL R. McGLYNN	New Mexico, *American Bar Association Section 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) "Compatible data practice" is data processing that is consistent with the ordinary expectations of reasonable individuals based on the context of data collection, or that is likely to substantially benefit such individuals.

(2) "Data controller" means a person that, alone or jointly with others, ~~initially collects~~ personal data from or about an individual.

(3) "Data processor" means a person that has received authorized access to personal data, pseudonymous data, or deidentified data from the controller.

(4) "Deidentified data" means personal data that has been modified to remove direct identifiers and to use technical safeguards to ensure the data cannot reasonably be linked to a specific individual with reasonable certainty by a person who does not have personal knowledge of the relevant circumstances.

(5) "Incompatible data practice" is a data practice that is not a compatible data practice or a prohibited data practice, and for which consent must be obtained from the individual.

(6) "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.

(7) "Personal data" means information that identifies or describes a particular individual by name or by other direct identifiers such as addresses, recognizable photographs, telephone numbers, and social security numbers. The term does not include pseudonymized data or

Commented [JH1]: Should be an objective standard, but be flexible enough to be the equivalent of "legitimate interests of the data controller" exception under GDPR.

Commented [HJ2]: Needs to follow the definition of this term under GDPR and other privacy laws. This formulation makes processors into controllers in some circumstances

Commented [HJ3]: Same issue. This is needlessly confusing

Commented [JH4]: The distinction between de-identified and pseudonomyzed data is murky.

Commented [HJ5]: Confusing construction

Commented [HJ6]: Again, a novel and confusing definition. The title of the bill uses Personally Identifiable data and this definition should focus on that, not on descriptors that are not identifiable.

Commented [HJ7]: These may or may not be personally identifiable data.

deidentified data.

(8) “Pseudonymized data” means information that was derived from personal data by removing direct identifiers. A controller or processor can create pseudonymized data by replacing direct identifiers with a unique ID or other code that allows the pseudonymized data to be converted back to personal data with the use of a decryption key. The term includes information containing Internet protocol addresses or other data related to a particular devices as long as direct identifiers are not included. The term does not include deidentified data.

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

(10) “Profiling ” means processing to evaluate, ~~analyze,~~ or predict an individual’s economic status, health, personal preferences, interests, character, reliability, behavior, social or political views, physical location, movements or demographic characteristics, including race, gender, and sexual orientation. The term does not include evaluation, analysis, or prediction based on an individual’s contemporaneous activity, such as search queries or access to a particular website, if no personal data is retained for use after completion of the processing.

(11) “Publicly available information” means information that is (A) made available to the general public from federal, state, or local government records; (B) available in widely distributed media; (C) observable from a publicly accessible vantagepoint; or (D) that a person has a reasonable basis to believe is lawfully made available to the general public. For purposes of this definition:

(A) a person has a reasonable basis to belief that information is lawfully made available to the general public if the person has taken steps to determine that the information is

Commented [JH8]: This is true if a specific individual’s personal data was attached to but is removed from the IP addresss.

Commented [HJ9]: Should be tied to compilation of a profile over time to evaluate an individual, not the attributes themselves. Also first party profiling should not be subject to the same restrictions as 3rd party profiling, as it is appropriate for and expected by consumers that businesses will try to figure out how best to serve their customers.

of the type that is available to the general public and that the data subject who can direct that the information not be made available to the general public has not done so, and

(B) "Widely distributed media" means information that is available to the general public, including information from a publicly accessible website; a telephone book or online directory; a television, Internet, or radio program; or news media. This term includes information that is available from a website or other forum that has restricted access as long as the information is nevertheless available to a broad audience.

(12) "Sensitive data" means personal data that reveals:

(A) racial or ethnic origin, religious belief, mental or physical health condition or diagnosis, an activity or preference related to gender, sexual orientation, transgender status, citizenship, or immigration status;

(B) passwords and other authenticating information, including biometric identifiers used for authentication purposes;

(C) credit card numbers;

(D) tax identification numbers;

(E) real time geolocation information

(F) financial information

(G) information related to a disease or health condition;

(H) genetic sequencing information; or

(I) information about an individual known to be under [13] years of age.

(13) "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.]

Commented [HJ10]: This is unnecessarily wordy and can be moved up to paragraph (1)(B) more clearly and succinctly.

Commented [JH11]: Overbroad. An individual posting that they have a cold is not sensitive data.

Commented [JH12]: Very unclear and not tied to individuals

Commented [HJ13]: How does a business know it holds this information unless it uses the information for authentication purposes?

Commented [HJ14]: A business tax ID is not personal data

Commented [HJ15]: This is vague. Financial account numbers are sensitive but not the mere fact that someone has a mortgage, for example.

Commented [HJ16]: This is overbroad and includes a simple email that someone is staying home from work because they have a cold or that they have a sore finger. Should be diagnosis or treatment by a medical professional.

(14) "Targeted content and advertising" means purely expressive content or advertising displayed to an individual on the basis of profiling.

(15) "Targeted decisional treatment" means differential treatment of, or offers made to, an individual on the basis of profiling.

Comment

The definition of "profiling" in subsection (10) is meant to avoid capturing "contextual" inferences based on the contemporaneous transaction.

SECTION 3. SCOPE.

(a) This [act] applies to the activities of a data controller or data processor that conducts business in this state or produces products or provides services targeted to this state six months after the person:

(1) becomes the controller or processor of personal data concerning more than [50,000] individuals in any one calendar year;

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

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

(b) This [act] does not apply with respect to personal data that is:

(1) publicly available information

(2) subject to the Health Insurance Portability and Accountability Act, Pub. L. 104-191 if the data controller is regulated by that act;

(3) subject to 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 in 15 U.S.C. Section 1681a(f) [,as amended], by a furnisher of the information or a

Commented [HJ17]: Why use this undefined and confusing term? Is commercial content excluded that is not advertising?

Commented [HJ18]: Some notion of compiling information should be part of profiling and may help in this regard

Commented [HJ19]: Individuals anywhere in the world should not count for these purposes.

Commented [HJ20]: Should be similar to CCPA in also exempting information treated in accordance with HIPAA requirements or de-identified in accordance with HIPAA standards

person procuring or using a consumer report;

(4) collected, used, processed or disclosed by a financial institution that processes information to the extent such personal information is subject to the Gramm-Leach-Bliley Act of 1999, or is treated in substantial compliance with that Act's data privacy and security requirements. This exemption also applies to personal data collected, used, processed, or disclosed by other entities to the extent such personal information is subject to the Gramm-Leach-Bliley Act;

(5) subject to the Drivers Privacy Protection Act of 1994, 18 U.S.C. Section 2721 et seq.;

(6) subject to the Family Education Rights & Privacy Act of 1974, 20 U.S.C. Section 1232;

(7) subject to the Children's Online Privacy Protection Act of 1998, 15 U.S.C. Sections 6501 et seq.;

(8) disclosed to a government unit if the disclosure is required or permitted by a warrant, subpoena, an order or rule of a court, or otherwise as specifically required by law; or

(9) subject to public disclosure requirements under [the public records laws].

Legislative Note: *Add a reference to the relevant public records statute in (b)(9).*

SECTION 4. CONTROLLER RESPONSIBILITIES AND INDIVIDUAL RIGHTS; GENERAL PROVISIONS.

(a) A data controller shall:

(1) provide a copy of an individual's personal data in accordance with Section 5;

(2) correct an inaccuracy in an individual's personal data upon reasonable request in accordance with Section 5;

Commented [HJ21]: Is the intention to regulate employee and B2B data the same as consumer data? Employee data is not regulated by the CCPA or Nevada OPPA and raises different issues. We recommend using the term "consumer".

Commented [JH22]: This structure is confusing because 4(b) applies to the (a)(2) right, but nothing else in the section applies to the (a)(1) copying right.

Commented [JH23]: Materiality standard should apply

(3) provide notice and transparency about their data processing practices in accordance with Section 6;

(4) obtain consent for any processing that would constitute an incompatible data practice under Section 8;

(5) abstain from processing personal data using prohibited data practices as defined in Section 9; and

(6) conduct routine data privacy assessments in accordance with Section 10.

(b) With respect to an individual's personal data, an individual may require a data controller to:

(1) confirm whether the controller has retained and to provide a copy of the data in accordance with Section 5;

(2) correct a~~n~~ material inaccuracy in the data retained or processed by the controller in accordance with Section 5; and

(3) provide redress for any incompatible or prohibited data practices that has occurred or will occur in the course of processing the individual's personal data.

SECTION 5. INDIVIDUAL RIGHTS TO COPY AND CORRECT PERSONAL DATA.

(a) A data controller shall establish a reasonable procedure for an individual to request a copy of any currently-maintained data and to request an amendment or correction of personal data. This procedure should make use of any authentication procedures that are already in use to authenticate the requester and ensure the security of the personal data.

(b) Subject to subsection (c), upon request, a data controller shall:

(1) provide one copy of any currently-maintained personal data relating to the

Commented [HJ24]: Under GDPR these are required for sensitive data and in limited other circumstances. The same approach makes sense here to avoid unnecessary cost.

Commented [JH25]: This should not include data that are inherently risky – eg breach notice information.

individual free of charge once every twelve months;

(2) provide additional copies either free of charge or upon payment of a fee reasonably based on administrative costs;

(3) make a requested correction of incorrect personal data if:

(A) the controller has no reason to believe the request for correction is fraudulent; and

(B) the correction is reasonably likely to affect decisions that will materially affect a legitimate interest of the individual; and

(4) make reasonable effort to ensure that any correction performed by the data controller is also performed on personal data held by a data processor acting on the controller's behalf.

(c) If a request by an individual under subsection (a) is manifestly unreasonable or excessive, a data controller may refuse to act on the request after notifying the individual about the basis for the refusal.

(d) A data controller shall comply with a request under this section without undue delay. If the controller does not comply with the request [not later than 45 days] [within a reasonable time] after receiving it, the controller shall provide the individual who made the request an explanation of the action being taken to comply with the request.

(e) A data controller may not discriminate against an individual for exercising a right under Section 4 to access and copy the individual's personal data or correct an inaccuracy in personal data by denying a good or service, charging a different rate, or providing a different level of quality.

(f) An agreement that waives or limits a right or duty under this section is contrary to

Commented [HJ26]: Fraud is a very high standard. The consumer could want to delete accurate info about non-payment, for example, for non-fraudulent reasons but in almost all cases should not be able to require this

Commented [HJ27]: Maybe better to ld say notify processors, as this is clearer.

public policy and is unenforceable except as provided under subsection (c).

SECTION 6. PRIVACY POLICY.

(a) A data controller shall provide an individual with a reasonably accessible, clear, and meaningful privacy policy that discloses:

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

(2) categories of personal data the controller provides to a data processor or another person, and the purpose of the disclosures;

(3) compatible data practices that will routinely be applied to the personal data by the controller or by authorized processors;

(4) incompatible data practices that the controller knows at the time of collection will be applied to the personal data by the controller or by authorized processors with consent;

(5) the procedures by which an individual may exercise a right under Section 5;

(6) the identification of any state, federal, or international privacy laws or frameworks with which the controller complies; and

(7) the identity of any voluntary consensus standards that the controller has chosen to adopt.

(b) The privacy policy required in part (a) must be reasonably available at the time personal data is collected from an individual. If the controller maintains a public website, the controller must provide notice under this section using the website. This is so even if the controller provides a different reasonable form of notice at the time personal data is collected from the individual.

(c) The [Attorney General] at any time may review the privacy policy of a data controller

Commented [JH28]: The nature of this definition is that it restricts subsequent uses that may not be anticipated at the time of collection. That subset cannot be included in the definitinon,

Commented [HJ29]: This could be a long list and will not be meaningful to residents of individual states. It also opens the door to class action lawsuits challenging these statements for laws other than this one.

Commented [HJ30]: How does this work if a 3rd party actually collects the personal data on behalf of a controller?

Commented [JH31]: Move to the enforcement section.

and may institute an action under Section 15 if the privacy policy or the data practices described in the policy fail to comply with this [act].

Comment

Data controllers and processors do not have to explicitly state compatible data practices that are not routinely used. For example, a data controller may disclose personal data that provides evidence of criminal activity to a law enforcement agency without listing this practice in its privacy policy as long as this type of disclosure is unusual.

SECTION 7. COMPATIBLE DATA PRACTICE.

(a) GENERAL STATEMENT OF COMPATIBLE DATA PRACTICE– A compatible data practice is processing of personal data that is consistent with typical expectations or, if inconsistent, processing that is likely to substantially benefit the individuals whose data is being processed. Compatible data practices are mutually exclusive from incompatible and prohibited data practices described in Sections 8 and 9.

(b) The following factors apply to determine whether processing of personal data constitutes a compatible data practice:

(1) the consumer's relationship with the data controller;

(2) the type of transaction in which the personal data was collected;

(3) the type and nature of the personal data that was collected;

(4) the risk of any negative consequences on the consumer of the proposed use or disclosure of the personal data;

(5) the effectiveness of any safeguards against unauthorized use or disclosure of the personal data; and

(6) the benefits of any proposed use or disclosure of personal data to the individual.

(c) Compatible data practices include processing that:

Commented [HJ32]: Could insert as to which the consumer received notice at the time of collection.

Commented [HJ33]: This is a balancing test that is different than most "secondary use" tests in that notice of the use in the mandatory privacy notice is not included. This creates significant subjectivity and is not a good fir with private right of action enforcement. The result would be obtaining consent unless a compatible practice was specified in (c). Is that a desired outcome?

Commented [HJ34]: There is a serious structural implication of tucking these exceptions in the compatible data practices section. In the CCPA, several (eg fraud prevention and compliance) are overarching exceptions – including to access and data deletion rights.

Commented [HJ35]: They should also include practices that are in the initial privacy notice. That is not clear with the current structure.

(1) initiates or effectuates a transaction with a consumer with the consumer's knowledge or participation;

(2) is reasonably necessary for compliance with legal obligations or regulatory oversight of the data controller;

(3) meets a managerial, personnel, administrative or ~~and~~ operational need of the data controller;

(4) permits appropriate internal oversight of the data controller, or external oversight by a government unit or by the controller's agents, auditors or other third parties;

(5) is reasonably necessary to create pseudonmymized or deidentified data;

(6) permits analysis for the purpose of generalized research or for the research and development of new products and services;

(7) is reasonably necessary to prevent, detect, investigate, report on, prosecute, or remediate an actual or potential:

(A) fraud;

(B) unauthorized transaction or claim;

(C) security incident;

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

(E) other legal liability of the controller;

(8) assists a person or government entity acting under paragraph (7); or

(9) is reasonably necessary to comply with or defend a legal claim.

(d) A data controller may use personal data for the purpose of delivering targeted content and advertising to the individual. It may also disclose pseudonymized data to data processors for these purposes. This provision applies only to targeted delivery of expressive content, and does

Commented [JH36]: This does not address gifts to consumers that require collection of information. Should include enforcing the transaction.

Commented [JH37]: Necessary is too restrictive. Used for or is collected for the purpose of compliance is closer.

Commented [JH38]: Align with compliance use formulation above. Necessity standard is too restrictive to be workable.

Commented [JH39]: This has the unintended consequence of restricting use of processors for other purposes by negative implication, when the data controller should be able to use processors for any purpose.

Commented [HJ40]: This term is undefined. Is advertising intended to be expressive content? It is very important for small businesses that need to attract customers during the pandemic.

not cover disclosures or uses of personal data or pseudonymous for the purpose of targeted decisional treatment unless the processing is compatible for a different, independent reason.

(e) A data controller may process personal data in accordance with the rules of any Voluntary Consent standard that recognized in accordance with Sections 11 through 14 to which the data controller has committed in the privacy policy unless the processing has been found to be incompatible or prohibited by a court of law.

(f) A data controller may use or disclose personal data in any other compatible manner consistent with subparts (a) and (b) of this section.

Comment

Subsection (d) makes clear that the act will not require pop-up windows or other forms of consent before using data for tailored advertising. This leaves many common web practices in place, allowing websites and other content-producers to command higher prices from advertisers. But websites and other controllers cannot use data even in pseudonymized form for tailored treatment unless tailoring treatment is compatible for____.

SECTION 8. INCOMPATIBLE DATA PRACTICES.

(a) Data processing is an incompatible data practice if it is not consistent with typical reasonable expectations, and is not likely to substantially benefit the individuals. Incompatible data practices may proceed with the individual's consent as long as the processing is not a prohibited data practice.

(b) Data processing is an incompatible data practice if it contradicts the policies that the data controller has described in their privacy policy as required by Section 6. This is so even if the processing would otherwise qualify as a compatible use.

(c) Data processing is an incompatible data practice if it fails to provide reasonable data security measures, including appropriate administrative, technical, and physical safeguards to prevent unauthorized access. Security practices that conform to best practices promulgated by a professional organization, government entity, or other specialized source are presumptively

Commented [JH41]: What is the intent of this exception?

Commented [JH42]: What happens before the voluntary standard is approved – as this may never happen – or if there is a rulemaking?

Commented [HJ43]: Is this a proxy for reasonableness, or does it require polling or surveys to establish what is typical? Recall private right of action enforcement with lack of clarity wastes resources and chills legitimate commercial activity.

Commented [HJ44]: Is the intent that consistency with the notice be required, but not sufficient, to establish compatible use? Note that right now "incompatible uses" cover both practices that are "unfair" under traditional consumer protection law and practices that are contrary to a privacy policy. They could be treated differently.

Commented [HJ45]: Do you intend that reasonable security measures be tied to the sensitivity of the data and the context of use – eg whether the data is held by the controller?

reasonable absent a finding by a court of law that the practice is unreasonable.

(d) If a data processor engages in an incompatible data practice, a data controller that willfully disclosed the relevant personal data to the data processor is deemed to have engaged in the same incompatible data practice.

(e) A data controller shall not engage in a noncompatible data practice unless, at the time the personal data was collected from the consumer:

(1) sufficient notice and information was provided to the consumer by the data controller, or by another controller that originally collected the personal data, to convey to a reasonable consumer that the consumer's personal data can be processed for incompatible purposes; and

(2) the consumer had a reasonable opportunity to withhold consent to that incompatible use.

(f) A data controller shall not process a consumer's sensitive personal data for an incompatible data practice without obtaining the consumer's express, voluntary, and signed or e-signed consent in a record for each such incompatible use.

(g) Unless the processing is prohibited by federal law or constitutes a prohibited data practice subject to Section 9, a data controller may require that an individual consent to an incompatible data practice as a condition for access to its goods or services. The data controller may also offer a reward or discount in exchange for the individual's consent to process the consumer's personal data.

Comment

Statements in a privacy policy do not meet the standards of notice required here.

Commented [HJ46]: Standard should likely be knowing and willful disclosure, as awareness of the data processor's incompatible practice needs to be a basis for liability of controllers. This is different from the CCPA and WPA standards.

Commented [HJ47]: Seems to contradict the reference to notice above, which does not reference section 8.

Commented [HJ48]: No state privacy law requires E-Sign consent and to do so would add a pretty long boiler plate notice ot the consent form. The privacy trend is toward shorter, more intuitive affirmative consent mechanisms that users will read.

SECTION 9. PROHIBITED DATA PRACTICE.

(a) A prohibited data practice is processing that causes undue risk of harm to the individual or to others that cannot effectively be cured by consent.

(b) A data controller or processor may not process personal data in a manner that would reasonably and foreseeably:

(1) inflicts specific and significant financial, physical, or reputational harm to a person, or undue embarrassment or ridicule, intimidation or harassment;

(2) causes the misappropriation of the personal data for the purposes of assuming another's identity;

(3) causes physical or other intrusions upon the solitude or seclusion of a person or a person's private affairs or concerns, if the intrusion would be inappropriate and highly offensive to a reasonable person;

(4) constitutes a clear violation of federal law;

(5) recklessly or knowingly fails to provide reasonable data security measures, including appropriate administrative, technical, and physical safeguards to prevent unauthorized access;

(6) processes personal data in a manner that a court has deemed "incompatible" without the consent described in Section 8; or

(7) recklessly or knowingly causes an increased risk of subjecting a person to discrimination if the discrimination would violate a state or federal anti-discrimination law.

(c) If a data processor engages in a prohibited data practice, a data controller that willfully disclosed the relevant personal data to the data processor is deemed to have engaged in the same prohibited data practice.

Commented [JH49]: Consent is acceptance of risk. Compensating controls mitigate risk

Commented [HJ50]: Again, appropriate in relation to what data and what context and is this a workable PRA standard?

Commented [HJ51]: Shouldn't this be invidious

Commented [HJ52]: Again, recommend knowingly and willfully or the CCPA standard.

(d) No person shall collect or create personal data by reidentifying or causing the reidentification of designated pseudonymized or deidentified data unless:

(1) the reidentification is performed by a data controller or data processor that can process personal data consistent with this act; or

(2) the purpose of the reidentification is to assess the privacy risk of deidentified data, and the person does not use or re-disclose reidentified personal data except to the data controller or producer that had created the deidentified data for the purpose of demonstrating the privacy vulnerability.

SECTION 10. DATA PRIVACY AND SECURITY ASSESSMENT.

(a) A data controller or data processor shall prepare in a record a data privacy and security assessment of its data practices. The assessment shall evaluate the material privacy and security risks associated with its data practices, the types of personal data being processed, the efforts taken compared to means available to mitigate the risks, the extent to which its data practices comply with the provisions of this [act], and the likely tradeoffs between remaining risks and the benefits of data processing for individuals.

(b) A data privacy and security assessment shall be updated if there is a change in data practice that may materially affect the risks or benefits of the practice or two years have passed since the last assessment.

(c) A written record of a data privacy and security assessment is confidential business information [and is not subject to the public records request or compulsory civil discovery in a court]. The fact that a data controller or data processor conducted an assessment and the dates thereof are not confidential information.

Legislative Note: *The state should include appropriate language in subsection (f) exempting data privacy assessments from open records requests and compulsory civil discovery requests to*

Commented [HJ53]: What about public safety or cybersecurity uses?

Commented [HJ54]: This is somewhat unclear. Does it mean a compatible use? An activity not prohibited by the Act?

Commented [HJ55]: All data practices or data practices involving personal data?

Commented [HJ56]: How is this intended to relate to DPIA under GDPR? Those apply to specific high risk processing activities, not all processing, and are fairly prescriptive.

This seems to be a general assessment of data practices. How would a general assessment be regularly updated for changes as required in (b) below? This would take place all the time. And under what circumstances would the assessment be required to be disclosed? Would it be privileged? Or made available to plaintiffs in PRA? If they have to be disclosed this would make the assessment far less useful and more of an exercise in building a defensive record.

Commented [HJ57]: This is critical. Otherwise, these assessments will become self-justifying liability avoidance exercises by any entity nervous about litigation risk,

the maximum extent possible under state law.

Comment

The goal here is to ensure that all controllers and processors go through a reflective process of evaluation that is appropriate for their size and the intensity of data use. Other than being a record, the act does not require any particular format for the evaluation. There are many existing forms that companies can use to help them through a privacy impact assessment, and the Attorney General may recommend or provide some of these on their website.

SECTION 11. ADHERENCE TO A RECOGNIZED VOLUNTARY CONSENSUS STANDARD. A data controller or data processor may comply~~ies~~ with Sections 5 through 9 of this [Act], and any regulations under these sections, by complying with a voluntary consensus standard that has been recognized by the [Attorney General].

SECTION 12. PROCESS FOR VOLUNTARY CONSENSUS STANDARDS BODIES.

(a) The [Attorney General] may recognize a voluntary consensus standard only if the standard is developed by a voluntary consensus standards body through a process that:

(1) achieves general agreement, but not necessarily unanimity, through a consensus process which:

(A) consists of stakeholders representing a diverse range of industry, consumer, and public interests;

(B) gives fair consideration to all comments by stakeholders;

(C) responds to each good faith objection made by stakeholders;

(D) attempts to resolve all good faith objections by all stakeholders;

(E) provides each stakeholder an opportunity to change the stakeholder's vote after reviewing comments received; and

(F) informs all stakeholders of the disposition of each objection and the

Commented [HJ58]: This is interesting but would be very slow in practice, it seems. This section seems to require a multi-stakeholder process and rules out industry developed standards that are reviewed and approved by the AG, which means development could be very slow and expensive. Should all stakeholders have equal voice? How will things like "fair consideration be determined? Would the process be more efficient if the AG took into account the views of different parties in evaluating an industry developed standard? Parties are allowed to file dissenting views already under this construct.

reasons therefor.

(2) provides stakeholders a reasonable opportunity to contribute their knowledge, talents, and efforts to the development of voluntary consensus standard;

(3) is responsive to the concerns of all stakeholders;

(4) consistently adheres to documented and publicly available policies and procedures that provide adequate notice of meetings and standards development;

(5) includes a right for any stakeholder to file a statement of dissent with the Attorney General; and

(6) includes a right to appeal by any stakeholder that asserts that a voluntary consensus standard was not developed in substantial compliance with this section.

(b) In developing a voluntary consensus standard, the voluntary consensus standards body shall reasonably reconcile the requirements of this [Act] with the requirements of other federal and state laws.

SECTION 13. RECOGNITION OF VOLUNTARY CONSENSUS STANDARDS.

(a) The [Attorney General] may recognize a voluntary consensus standard only if the [Attorney General] finds that the standard:

(1) substantially complies with the requirements of Sections 5 through 9;

(2) is developed by a voluntary consensus standards body through a process that substantially complies with Section 12; and

(3) reasonably reconciles the requirements of this [Act] with the requirements of other applicable federal and state laws;

(b) Not later than 180 days after the filing of the request in a record to recognize a voluntary consensus standard, the [Attorney General] shall in a public record decide whether to grant the

Commented [HJ59]: Some or all of these concerns (they may not be reasonable)

Commented [HJ60]: Is the AG bound by this restriction as well in reviewing the standard,

Commented [HJ61]: Is the AG obligated to recognize it if it meets the requirements? May the AG hold out and reject it for some other reason?

request and state the reasons for the decision.

(c) A final decision by the [Attorney General] on a request under subsection (b), or a failure to decide within 180 days of the filing of a request, may be appealed to [the appropriate state court] as provided for in [the state's equivalent of 5 U.S.C. Section 706].

(d) Not later than [180 days after the effective date of this [Act]], the [Attorney General] shall adopt regulations under [the state's administrative procedures act] to establish a procedure for recognition of voluntary consensus standards under this [Act].

(e) A voluntary consensus standard recognized by any member state in an interstate compact under Section 14 shall be deemed recognized under this Section.

(f) The [Attorney General] may recognize a voluntary consensus standard if the [Attorney General] of another state has recognized the standard under a law substantially similar to this [Act].

(g) The General Data Protection Regulation (EU), the California Consumer Privacy Act, and any other substantially similar privacy framework that the [Attorney General] determines to be substantially similar to, or more protective than, this [Act] constitute and shall be recognized by the Attorney General as a voluntary consensus standard. A firm that voluntarily complies with these laws will be in compliance with this act.

(h) The [Attorney General] may adopt a regulation under [the state's administrative procedures act] to set a fee to be charged any person that makes a request under subsection (b). The fee must reasonably reflect the costs expected to be incurred by the [Attorney General] acting on a request under subsection (b).

SECTION 14. INTERSTATE COMPACT FOR RECOGNITION OF VOLUNTARY CONSENSUS STANDARDS.

(a) Upon certification by the [Attorney General] that a federal law has authorized an

Commented [HJ62]: Query whether it is worthwhile going through the procedures for voluntary standard adoption if AGs are free to reject them for any reason if their state is not part of a compact.

Commented [HJ63]: This should maybe be the first paragraph, as it will be used more often

Commented [HJ64]: Must federal law be enacted? What is the purpose of adopting a voluntary standard if it must be recognized by each state AG until a federal privacy law passes? (This law may well preempt state privacy laws.)

interstate compact of states that have enacted a law substantially similar to this [Act] for the recognition of voluntary consensus standards, this state adopts the interstate compact when the [Attorney General] provides notice in a record of the adoption.

(b) Once effective, the interstate compact continues in force and, except as otherwise provided for in subsection (c), remains binding on this state.

(c) A member state of an interstate compact under subsection (a) may withdraw from the compact by repealing subsections (a) and (b) of this section. The withdrawal may not take effect until one year after the effective date of the repeal law and until written notice of the withdrawal has been given by the Governor and [Secretary of State] of the withdrawing state to the Governor and [Secretary of State] of each other member state.

(d) A state withdrawing from the interstate compact under subsection (c) is responsible for all assessments, obligations, and liabilities that extend beyond the effective date of the withdrawal.

(e) An interstate compact is dissolved when the withdrawal of a member state reduces the membership in the compact to fewer than five states. On dissolution, the compact has no further effect, and the affairs of the compact must be concluded and assets distributed in accordance with the provisions of the compact.

SECTION 15. ENFORCEMENT BY [ATTORNEY GENERAL].

(a) An [act or practice] by a person to which this [act] applies is a violation of [the state's consumer protection law] if the act or practice:

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

(2) deprives an individual of a right under this [act].

(b) The authority of the [Attorney General] to bring an action to enforce [the state's

consumer protection law] includes enforcement of this [act].

(c) The [Attorney General] may adopt rules to implement this [act] under [the state's administrative procedure act].

(d) In adopting rules and in bringing an enforcement action under this section the [Attorney General] shall consider the need to promote predictability for covered entities and uniformity among the states by:

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

(2) giving deference to any voluntary consensus standards developed consistent with the requirements of this [act].

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

Need another legislative note about the state's administrative procedure act.

SECTION 16. PRIVATE CAUSE OF ACTION.

(a) A person may bring a private action for equitable relief, including an injunction, against a controller or processor that processes the individual's personal data in violation of this [act] and in a manner that would be reasonably likely to cause identifiable harm.

(b) A person may bring a private action for damages against a controller, processor, or person that knowingly engages in a prohibited data practice in violation of this [act] in a manner that would reasonably foreseeably cause, or is likely to cause, any of the following:

(1) financial, physical, or reputational injury to a person;

(2) physical or other intrusions upon the solitude or seclusion of a person or a person's private affairs or concerns, where such intrusion would be highly offensive to a reasonable person;

(3) increased risk of subjecting a person to discrimination in violation of any state or

Commented [JH65]: This defeats uniformity

Commented [JH66]: We oppose a private right of action

Commented [HJ67]: Likelihood is a somewhat fuzzy standard that may raise standing issues.

federal anti-discrimination law applicable to the covered entity; or

(4) other substantial injury to a person.

(c) At least thirty days prior to filing an action under this section, a written demand for relief, identifying the claimant and reasonably describing the violation of the act relied upon and the injury suffered, shall be mailed or delivered to the covered entity. Any covered entity receiving such a demand for relief that, within thirty days of the mailing or delivery of the demand for relief, makes a written tender of settlement which is rejected by the claimant may, in any subsequent action, file the written tender and an affidavit concerning its rejection.

(d) If the court in any subsequent action finds for the claimant and also finds that the relief tendered by the covered entity was reasonable in relation to the injury claimed by the claimant, the claimant's relief shall be limited to the amount tendered. In all other cases, if the court finds for the claimant, recovery shall be in the amount of actual damages.

(e) If the court finds the violation of this [act] was a willful or knowing violation or that the refusal to grant relief upon demand was made in bad faith with knowledge or reason to know that the act or practice complained of violated this [act], the court may award up to three times the actual damages.

Comment

The private right of action is structured to permit claims for damages only if the controller or processor has knowingly engaged in a prohibited data practice or in an incompatible data practice that has been clearly defined as such. This ensures that there will be clarity in the law before a company will face significant liability risk.

SECTION 17. 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.

Commented [JH68]: This is unclear and open-ended,

Commented [JH69]: This is very different than a Rule 68 offer of judgment and creates an incentive to litigate desite a settlement offer.

SECTION 18. 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 19. 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 20. EFFECTIVE DATE. This [act] takes effect [180 days after the date of enactment].