April 13, 2021

Harvey Perlman, Chairman
Collection and Use of Personally Identifiable Data Drafting Committee
Uniform Law Commission
111 N. Wabash Avenue, Suite 1010
Chicago, IL 60602

Dear Chairman Perlman:

The Main Street Privacy Coalition (MSPC), a coalition of 19 national trade associations representing more than a million American businesses,[1] and the NFIB Small Business Legal Center[2] appreciate the ongoing work the Uniform Law Commission (ULC) Collection and Use of Personally Identifiable Data Drafting Committee (Committee) has undertaken to draft uniform model privacy legislation. Our organizations further appreciate the robust discussion on these issues that took place during the March 12-13, 2021 meeting and the subsequent draft of the Collection and Use of Personally Identifiable Data Act (CUPIDA).[3]

We remain concerned, however, with the potential for many businesses to be subject to vicarious liability based on the latest draft of CUPIDA. As currently drafted, the collecting controllers remain liable for incompatible or prohibited data practices and for simple failures to comply with the law on the part of third-party controllers or processors.

Our organizations offer these comments outlining our remaining concerns and attach a redline of suggested language changes to the current draft of CUPIDA for the Committee's consideration. We urge the Committee to make changes to ensure that no business is vicariously liable for another's conduct, both because such liability is not appropriate and because it creates loopholes that will prevent the bill from being effective in protecting consumers' privacy.

II. COMMENTS ON CUPIDA

A. A Vicarious Liability Structure Does Not Work for Privacy Law.

[1] From retailers to Realtors®, hotels to home builders, grocery stores to restaurants, and gas stations to convenience stores, its member companies interact with consumers day in and day out. Collectively, the industries that MSPC trade groups represent directly employ nearly 34 million Americans and constitute over one-fifth of the U.S. economy by contributing $4.5 trillion to the annual U.S. gross domestic product. *See* https://mainstreetprivacy.com/about/ for a complete list of the members of the Main Street Privacy Coalition.

[2] The NFIB Small Business Legal Center is a public interest law firm representing the interests of millions of small businesses across the country in our nation's courts and providing them with helpful legal resources.

[3] *See* National Conference of Commissioners on Uniform State Laws, Collection and Use of Personally Identifiable Data Act (March 31, 2021)(hereinafter "CUPIDA").

Our organizations remain concerned that CUPIDA requires a collecting controller to be liable for a third-party controller and/or processor's activity if they "knew or should have known" about the incompatible and/or prohibited data practices. Vicarious liability models do not make sense in a privacy law. The notion that one "controller" actually controls the activities engaged in by another "controller" or processor is false; it is a legal fiction.

The vicarious liability framework established in Sections 8 and 9 of the latest CUPIDA draft obligates the smallest entities serving customers and holds them liable for failures by processors and third-party controllers.[4] This not only is an unfair shifting of liability onto businesses least capable of absorbing it, but the structure of the proposed law itself fails to set sufficient incentives to protect customer data for the nations' largest businesses who process the greatest amount of consumer data in serving millions of smaller businesses.

The liability provisions in Sections 8 and 9 should be limited such that each business in the chain is responsible for its own data practices. Our suggested modifications, which are shown in our accompanying redlined version of the Committee's latest draft of CUPIDA (see pp. 18-21), will ensure that controllers who comply with CUPIDA are not penalized for failures of third-party controllers and processors to comply with it.

Furthermore, the provisions of Section 4 and 5 require a collecting controller to depend on the third-party controller or processor to respond with a copy of the personal data so that the collecting controller can comply with the law. Third-party controllers and processors, however, are not required by the provisions in Section 4 and 5 to provide a copy of the personal data to a collecting controller. The absence of such a requirement will allow third-party controllers and processors to only provide partial data or simply refuse to provide data without any effective remedy for consumers and with unmerited liability for collecting controllers. This not only hurts consumers – because their rights requests will be ineffective – but it also unfairly shifts the burden and liability for such failures onto the collecting controller. We have suggested textual corrections to address our concerns with Section 4 and 5 in the accompanying redlined version of CUPIDA (see pp. 8-11).

B. GLBA Compliance Provisions Create Further Vicarious Liability Risks.

We appreciate the Committee's removal of the exemptions from Section 3 in lieu of deemed compliance provisions in Section 11. We remain concerned, however, that the deemed compliance for financial institutions and other entities subject to the Gramm-Leach-Bliley Act (GLBA) is too broad and creates liability risks for the businesses that are subject to CUPIDA and exchange data directly or indirectly with businesses subject to GLBA. We therefore recommend in the accompanying redline that the deemed compliance be limited to Sections 7 and 8 (Incompatible and Prohibited Data Practices) because those are the aspects of processing subject to GLBA (see p. 23).

As the Committee discussed in its March 13 meeting, GLBA does not provide for any of the consumer rights established in Section 5 of CUPIDA. By limiting the deemed compliance for financial institutions and other entities as we suggest the redline, it would ensure that consumers'

[4] *Id*. at Section 8(c) and Section 9(c).

requests under Section 5 are honored and other parties would not be held vicariously liable for any of these entities' failures to respond to such requests.

By way of example, when a retailer accepts a credit card for payment, the transaction information is transmitted to a processor and ultimately a credit card company like Visa or Mastercard. In fact, in many cases a retailer does not maintain a record of the data once it has been shared with the processor or credit card company, but those entities may do so. This leaves the retailer in the position of being liable for executing the consumer rights established in Section 5 without having the ability to comply due to the processor or credit card company not being required to comply.

C. The Committee Should Protect Loyalty Programs.

We believe Section 7(c) of CUPIDA should include a savings clause for loyalty programs. We support privacy legislation that preserves the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships, including rewards and loyalty programs. Loyalty programs typically use customer purchase histories in order to provide discounts to repeat customers. Those programs are very popular, benefit consumers, and should not be made illegal by privacy law. We recommend including language from the recent privacy law enacted by Virginia in Section 7(c) of CUPIDA.[5] We have proposed textual edits based on this language in the accompanying redline of CUPIDA (see p. 15).

D. CUPIDA Should Establish Exclusive State Attorney General Enforcement (Option B)

We appreciate the Committee striking language in the latest draft of CUPIDA that would have established a private cause of action. We, however, remain concerned with the Committee's adoption of language that would subject violations of CUPIDA's provisions to state consumer protection act enforcement provisions that may, in turn, provide private causes of action for violations. We continue to support Option B from the options the Committee previously offered as the best enforcement option, which would authorize the attorney general of a state to act as the exclusive authority to enforce CUPIDA's provisions. We believe that this exclusive attorney general enforcement mechanism is highly appropriate for new areas of laws in states that have lacked them (such as data privacy regulations). We anticipate that there will be great uncertainty among the businesses as to the meanings of the terms and the extent of the requirements in CUPIDA absent an established set of legal interpretations in a state that adopts this model act as its new privacy law. We therefore continue to urge the Committee to reconsider the language in the current draft and instead to adopt Option B from the previous draft in the final draft of CUPIDA.

E. The Committee Should Consider Addressing Drafting Errors.

We would also like to raise remaining issues that we consider drafting errors in CUPIDA. The "processor" definition in CUPIDA is drafted in such a way that it expects a processor will only receive data from a controller. Likewise, the definition for "third-party controller" is drafted in a

[5] Consumer Data Protection Act, 2021, ch. 36, 2021 Va. Laws 59.1-571, https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0036 (codified at Va. Stat. Ann. § 59.1-571 et seq.).

way that it expects a third-party controller can only receive data from a controller. These definitions should be adjusted to recognize a third-party controller and/or processor can receive data from third-party controllers or processors. Additionally, there should be an exception to Section 5(b) so that an entity is not required to provide a copy of personal data in the event of a fraudulent request. We have suggested textual edits to correct these drafting errors in the accompanying redline of the Committee's latest draft (see pp. 2-5,10).

We also would note in Section 3 that, in order to offer a small business exemption, the number of data subjects must be deceivingly high if this number encompasses payment transactions. For example, a single, "mom-and-pop" convenience store averages more than 494,000 individual transactions per year. Many small businesses therefore will be subject to CUPIDA even if the vast majority of their data processing consists of compatible data practices such as through accepting credit and debit card payments. This provision should be updated so that payment transactions are excluded from the number of data subjects required to meet this threshold. We have suggested an appropriate correction in our accompanying redline of CUPIDA (see p. 7).

III. CONCLUSION

Our organizations appreciate the Committee's diligent work on model privacy legislation and its consideration of the concerns raised above. We welcome the opportunity to provide the Committee with additional information on any of the concerns outlined here.

Very truly yours,

Main Street Privacy Coalition
https://mainstreetprivacy.com

NFIB Small Business Legal Center
https://www.nfib.com/foundations/legal-center/

D R A F T

FOR DISCUSSION ONLY

Collection and Use of Personally Identifiable Data Act

[Proposed new title: Personal Data Protection Act]

Uniform Law Commission

April 23, 2021 Video Committee Meeting

This draft, including the proposed statutory language and any comments or reporter's notes, has not been reviewed or approved by the Uniform Law Commission or the drafting committee. It does not necessarily reflect the views of the Uniform Law Commission, its commissioners, the drafting committee, or the committee's members or reporter.

March 31, 2021

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	North Dakota
David V. Zvenyach	Wisconsin
William H. Henning	Alabama, *Division Chair*
Carl H. Lisman	Vermont, *President*

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:

Uniform Law Commission
111 N. Wabash Ave., Suite 1010
Chicago, IL 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. Title

This [act] may be cited as the Collection and Use of Personally Identifiable Data Act. [Proposed new title: Personal Data Protection Act.]

Section 2. Definitions

In this [act]:

(1) "Collecting controller" means a controller that initially collects personal data from a data subject.

(2) "Compatible data practice" means processing consistent with the ordinary expectations or clear best interests of data subjects based on the context of data collection.

(3) "Controller" means a person that, alone or with others, determines the purpose and means of processing.

(4) "Data" means information in a record.

(5) "Data subject" means an individual who is a resident of this State to whom personal data refers.

(6) "Deidentified data" means personal data that has been modified to remove all direct identifiers and has undergone a deidentification process that reasonably ensures the data cannot be linked to an identified individual by a person that does not have personal knowledge or special access to the data subject's private information.

(7) "Direct identifier" means commonly recognized information that identifies a data subject, including name, physical address, email address, recognizable photograph, telephone number, and Social Security number.

(8) "Incompatible data practice" means processing that is not a compatible data

practice or a prohibited data practice.

(9) "Maintains" with respect to personal data means to retain, hold, store, or preserve personal data as a system of records used to retrieve data about individual data subjects for the purpose of individualized communications or decisional treatment.

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

(11) "Personal data" means information that identifies or describes a particular data subject by a direct identifier or is pseudonymized data. The term does not include deidentified data.

(12) "Processing" means performing~~, or directing a data processor to perform,~~ an operation on personal data, including collection, transmission, use, disclosure, analysis, prediction, and modification of the data, whether or not by automated means. "Process" has a corresponding meaning.

(13) "Processor" means a person that receives ~~from a controller~~ authorized access to personal data or pseudonymous data and processes the data on behalf of the controller or another processor.

(14) "Prohibited data practice" means processing prohibited by section 9 of this [act].

(15) "Pseudonymized data" means personal data without a direct identifier but that is

(A) reasonably linkable to a data subject's identity, or

(B) is maintained to allow individualized communication with, or treatment of, the data subject.

The term includes information containing an Internet protocol address, browser, software, or

hardware identification code, a persistent unique ID, or other data related to a particular device if a direct identifier is not included. The term does not include deidentified data.

(16) "Publicly available information" means information:

(A) available from a federal, state, or local government record;

(B) available to the general public in widely distributed media, including:

(i) a publicly accessible website;

(ii) a website or other forum with restricted access if the information is available to a broad audience;

(iii) a telephone book or online directory;

(iv) a television, Internet, or radio program; and

(v) news media;

(C) observable from a publicly accessible location; or

(D) that a person reasonably believes is lawfully made available to the general public, if:

(i) the information is of the type generally available to the public; and

(ii) the person has no reason to believe that a data subject with authority to remove the information from public availability has directed the information to be removed.

(17) "Record" means information:

(A) inscribed on a tangible medium; or

(B) stored in an electronic or other medium and retrievable in perceivable form.

(18) “Sensitive data” means personal data that reveals:

(A) racial or ethnic origin, religious belief, gender, sexual orientation, , citizenship, or immigration status;

(B) credentials sufficient to remotely access an account;

(C) an individual’s credit card or debit card number, or financial account number;

(D) a social security number, tax-identification number, drivers license number, military identification number, or an identifying number on any governmentally issued identification;

(E) real-time-geolocation information;

(F) criminal record;

(G) diagnosis or treatment for a disease or health condition;

(H) genetic sequencing information; or

(I) information about a data subject the controller knew or should have known was collected from a child under [13] years of age.

(19) “Sign” means, with present intent to authenticate or adopt a record:

(A) execute or adopt a tangible symbol; or

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

(20) “Stakeholder” means a person who has a direct interest in the development of a voluntary consensus standard or a person that represents such persons.

(21) “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.]

(22) "Third-party controller" means a controller that receives ~~from another controller~~ authorized access to personal data or pseudonymous data and determines the purpose and means of additional processing.

Comment

The Act recognizes the distinction between data controllers and data processors. A controller is the person who determines the purpose and means of data processing. There are two types of controllers. A "collecting controller" is a person who directly collects data from a data subject and thus has a relationship with the data subject. A "third party controller" is a person who obtains personal data not directly from data subjects but from another controller, generally a collecting controller. As long as the person directs the purpose and means of a data processing the person is a data controller. A processor, on the other hand, processes personal data at the direction of a controller; a processor does not determine the purpose of processing of personal data. However, if a person with access to personal data engages in processing that is not at the direction and request of a controller, that person becomes a controller rather than a processor, and is therefore subject to the obligations and constraints of a controller.

The language in (3) that requires the controller to dictate both the "purpose and means" of processing is intended to include within the term "means" the selection of the processor to perform the processing.

The definition of "maintains" is pivotal to understanding the scope of the act. It is modeled after the federal Privacy Act's definitions of "maintains" and "system of records". 5 U.S.C. §552a(a)(3), (a)(5). While many individuals and businesses may accumulate data related to individuals in the form of emails or personal photographs, these records are not maintained as a system for the purpose and function of making individualized assessments, decisions, or communications, and would therefore not qualify under its scope in Section 3.

Personal data and deidentified data are mutually exclusive categories. Deidentified data must meet the standard of risk mitigation that makes data reasonably unlikely to be reidentified. This reasonableness standard is flexible so that it can accommodate advances in technology or data availability that may make reidentification efforts easier over time. Thus, the standard can be expected to rise as the ability to reidentify anonymized datasets rises. However, this is not a strict liability standard, nor is it one intolerant to risk. If reidentification is costly and error-prone, the data can meet the standard for de-identification even if reidentification is possible.

The broad category of "personal data" includes both direct identifying data and pseudonymized data. Data with a direct identifier (like name, social security number, or address) receives the full set of data protections under the act. By contrast, controllers using pseudonymized data are released from the requirement to provide access and correction (except in the case of sensitive pseudonymized data that is maintained in a way that renders the data

retrievable for individualized communications and treatment.)

The definition of a "direct identifier" is limited to information that on its own tends to identify and relate specifically to an individual. The definition provides an illustrative list of examples, but the list is non-exhaustive so that the definition is flexible enough to cover new forms of identification that emerge in the future. A persistent unique code that is used to track or communicate with an individual without identifying them is *not* a direct identifier, even if that unique code can be converted into a direct identifier using a decryption key. Data that includes a persistent unique code (but not the decryption key) is pseudonymized data. Data that does not include direct identifiers or persistent unique IDs maintained for individualized communication and treatment will nevertheless be pseudonymized data (as opposed to deidentified data) if it presents a reasonable risk of reidentification.

Pseudonymized data is itself a large subset of personal data that encompasses two distinct data practices, as identified by each of the clauses in the first sentence of its definition. First, some firms redact or remove direct identifiers and use the rest of the data fields for aggregate analysis or research. This usage of pseudonymized data is analogous to the intended uses of deidentified data, but the data does not qualify as deidentified because it is still "reasonably linkable to a data subject's identity." A second common practice is to maintain data without direct identifiers but with a unique code that permits firms to use the data for "individualized communication with, or treatment of, the data subject." Cookie IDs, browser codes, and IP addresses have historically been used for this purpose. Both types of practices fall under the umbrella term "pseudonymized data" and are covered by many of the data protections of this act. However, pseudonymized data that is not maintained for individualized communication or treatment is not subject to the rights of access and correction. Pseudonymized data that is maintained for individualized communication or treatment is only subject to the rights of access and correction if the data includes sensitive data. Both types of pseudonymized data should have a more limited set of legal restrictions and obligations in order to incentivize the good data hygiene and practice of removing direct identifiers. *See* Paul Schwartz & Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information,* 86 NYU L. REV. 1814 (2011).

The definition of "publicly available information" includes information accessible from a public website as well as information that is available on a nonpublic portion of a website if that nonpublic portion is nevertheless available to a large, non-intimate group of individuals. For example, if an individual shares personal data about themselves in a social media post that is accessible to all connected friends, that information is publicly available and would not fall within the scope of this Act. However, personal data that is shared with a hand-selected subset of friends through a direct message or through a highly constrained post on social media would not be publicly available.

Section 3. Scope

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

and that satisfy one or more of the following conditions:

(1) during a calendar year, maintains personal data concerning more than [ ] data Subjects excluding data subjects whose data is collected to complete a payment transaction;

(2) during a calendar year earns more than [50] percent of its gross annual revenue from maintaining personal data from data subjects as a controller or processor;

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

(4) any other controller or processor that conducts business in this state or produces products or provides services targeted to residents of this state that maintains personal data unless it processes the personal data solely using compatible data practices.

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

(1) publicly available information;

(2) processed solely in the course of a reasonable effort to prevent, detect, investigate, report on, prosecute, or remediate fraud, unauthorized access, or a breach of data security;

(3) processed solely as part of human-subjects research conducted in compliance with legal requirements for the protection of human subjects;

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

(5) subject to a public disclosure requirement under [cite to state public records act].

Comment

This section limits the scope of the Act by limiting the controllers and processors obligated to comply and by limiting the type of data subject to the Acts provisions. Personal data

privacy legislation can impose significant compliance costs on controllers and processors and thus most proposals contain limits similar to those in subsections (1), (2), and (3) which limit their provisions to larger controllers or processors—ones who either process data on a significant number of data subjects or earn a significant amount of their revenue from processing personal data. The threshold numbers are in brackets and each State can determine the proper level of applicability. The main goal of the act is to ensure data is secured and used in responsible ways, and the primary compliance mechanisms imposed are the obligation to publish a privacy policy and to conduct a privacy assessment in order to make their data practices transparent. Similarly, these firms must respond to consumer access and correction rights. The result of the limitations in (a) (1)-(3), however, is to put personal data at risk when collected by smaller firms. Thus, this act also applies to smaller firms, but relieves them of the compliance obligations as long as they use the personal data only for compatible purposes.

By moving away from data subject consent as the basis for data processing and recognizing that data collectors are entitled to process data for compatible uses, some significant compliance costs are accordingly reduced, while placing limits on incompatible or unexpected uses of data.

The processing of publicly available information is excluded from the act. There are significant First Amendment implication for placing limits on the use of public information. "Publicly available information" is defined in Section 2 of this act.

Section 4. Controller and Data Processor Responsibilities; General Provisions

(a) A controller shall:

(1) if a collecting controller, provide under Section 5 a copy of a data subject's personal data, and if a third-party controller, provide under Section 5 a copy of a data subject's personal data at the request of a collecting controller;

(2) correct or amend a subject's personal data on the subject's request under Section 5;

(3) provide notice and transparency under Section 6 about the personal data it maintains and its processing practices;

(4) obtain consent for processing that, without consent, would be an incompatible data practice under Section 8;

(5) not process personal data using a prohibited data practice;

(6) conduct a data privacy and security assessment under Section 10; and

(7) provide redress for an incompatible data practice or prohibited data practice

that the controller knowingly performs ~~or is responsible for performing~~ while processing a subject's personal data.

(b) A data processor shall:

(1) provide under Section 5 a copy of the data subject's personal data at the request of a controller;

(2) correct an inaccuracy in a data subject's personal data on request of a controller;

(3~~2~~) abstain from processing personal data or pseudonymized data for a purpose other than one requested by the controller;

(4~~3~~) conduct routine data privacy assessments in accordance with Section 10; and

(5~~4~~) provide redress for an incompatible or prohibited data practice the processor knowingly performs in the course of processing a data subject's personal data at the direction of the controller.

Comment

This Part clarifies the different obligations that collecting controllers, third party controllers, and data processors owe to individuals. Third party controllers, including data brokers, are firms that decide how data is processed. They are under most of the same obligations as collecting controllers. However, they are not under the obligation to respond to access or correction requests. A right of access or correction imposed on third party controllers would increase privacy and security vulnerabilities because third party controllers are not able to verify the authenticity of the request as easily as collecting controllers. However, collecting controllers must transmit credible collection requests to downstream third party controllers and data processors who have access to the personal data requiring correction.

This Act does not obligate controllers or processors to delete data at the request of the data subject. This is substantially different from the GDPR, the California Consumer Privacy Act, and several privacy bills recently introduced to state legislatures. There is a wide range of legitimate interests on the part of collectors that require data retention. It also appears difficult given how data is currently stored and processed to assure that any particular data subject's data is deleted. The restriction on processing for compatible uses or incompatible uses with consent should provide sufficient protection.

Section 5. Right to Copy and Correct Personal Data

(a) A collecting controller shall establish a reasonable procedure for a data subject to

request a copy of currently maintained personal data relating to the subject or an amendment or correction of the subject's personal data, unless the personal data is pseudonymized and is not maintained with sensitive data. The procedure must include a method to authenticate the requesting data subject's identity to ensure the security of the data.

(b) Subject to subsection (c), on request of a data subject that is not reasonably believed to be fraudulent, a collecting controller shall:

(1) provide one copy of currently maintained personal data relating to the subject free of charge once every 12 months and a copy of any correction made at the data subject's request;

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

(3) make a requested correction if~~:~~

~~(A) the controller does not have reason to believe the request for correction is fraudulent; and~~

~~(B)~~ the correction is reasonably likely to affect a decision that will materially affect a legitimate interest of the data subject; and

(4) ~~make a reasonable effort to ensure that a~~ communicate the request for a correction ~~performed by the collecting controller also is performed on personal data maintained by~~ to any third-party controller or processor that directly or indirectly received personal data from the collecting controller.

(c) If a request by a data subject under subsection (a) is unreasonable or excessive, a collecting controller:

(1) may refuse to act on the request; and

(2) must notify the subject of the basis for a refusal.

(d) A collecting controller shall comply with a request under subsection (a) promptly. If

Commented [A1]: We suggest removing Section 5(b)(3)(A) and instead adding language in Section 5(b) to indicate that a collecting controller does not need to reply to a request to provide a copy of maintained data in the event the request is fraudulent in addition to responding to a request for a correction if the collecting controller believes that request is fraudulent.

the controller does not comply with the request [not later than 45 days] [within a reasonable time] after receiving it, the collecting controller shall provide the data subject who made the request an explanation of the action being taken to comply with the request.

(e) A third-party controller or processor receiving a request ~~from a controller~~ to supply a copy of or correct personal data that it currently maintains shall supply such copy or make the correction, or enable the controller to make the correction, if the controller or processor does not have reason to believe the request for correction is fraudulent. A third-party controller or processor shall ~~make a reasonable effort to ensure that~~ ~~such a~~ communicate such a request to ~~correction also is performed by~~ any other third-party controller or processor that directly or indirectly received personal data from it and that is currently maintaining the personal data.

(f) A controller may not discriminate against a data subject for exercising a right under this section by denying a good or service, charging a different rate, or providing a different level of quality.

(g) Except as provided in subsection (c), an agreement that waives or limits a right or duty under this section is contrary to public policy and unenforceable.

Comment

The requirement to provide a copy of data or to initiate a data correction applies only to collecting controllers. These are the firms that already necessarily have a relationship with the data subject such that a secure authentication process would not unduly burden their business. A collecting controller must transmit any reasonable request for data correction to third party controllers and processors and make reasonable efforts to ensure that these third parties have actually made the requested change. Any third-party controller that receives a request for correction from a collecting controller must transmit the request to any processor or other third-party controller that it has engaged so that the entire chain of custody of personal data is corrected.

A collecting controller that controls and maintains personal data from several sources, only some of which were originally collected by the collecting controller, must nevertheless provide access to and correction of all personal data that the collecting controller has associated with the data subject. Thus, if a collecting controller comingles personal data collected directly from the data subject with data that has been collected or accessed from other sources (including public sources and from other firms who share federated data) but is linked data subject, the

access and correction rights apply to the entire set of personal data.

Access and correction rights do not apply to pseudonymized data unless the data is kept for the purpose of retrieving the data for individualized communication or treatment *and* contains at least one sensitive piece of data.

Subpart (f) ensures that a data subject who uses a right to access or correction is not penalized through diminished services or access for using their rights. This anti-discrimination provision is narrower than those appearing in statutes that also provide a right to deletion. A variety of firms follow a business model that provides their services for free or at a reduced rate in exchange for their customers providing personal data. This provision does not affect such a business model.

Section 6. Privacy Policy

(a) A controller shall adopt and comply with a reasonably accessible, clear, and meaningful privacy policy that discloses the following about personal data it maintains:

(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 providing the data;

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

(4) incompatible data practices that, with consent of the data subject, will be applied to personal data by the controller or an authorized processor;

(5) the procedure by which a data subject may exercise a right under Section 5;

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

(7) a voluntary consensus standard the controller has adopted and complies with.

(b) The privacy policy under subsection (a) must be reasonably available to a data subject at the time personal data is collected about the subject.

(c) If a controller maintains a public website, the controller must publish the privacy policy on the website.

(d) At any time, the [Attorney General] may review the privacy policy of a controller.

Comment

The purpose of the required privacy policy is to provide data subjects with a transparent way to determine the scope of the data processing conducted by collecting controllers. While consent to compatible data practices is not required, the privacy policy does assure that data subjects can understand what those practices are for a particular controller and may choose not to engage with that controller or its affiliates. Thus, this helps to promote an autonomy regime for individuals with high levels of privacy concern without requiring burdensome consent instruments. The privacy policy also permits consumer advocates and the Attorney General to monitor data practices and to take appropriate action.

Controllers and processors must describe all of the personal data routinely maintained about data subjects including pseudonymized data. They must also describe compatible data practices and incompatible data practices employed with consent under Section 8 that are currently in routine use. Because the privacy policy requirement applies only to "maintained" data, controllers do not have to provide disclosures related to personal data (whether directly identified or pseudonymized) that are not used as a system of records for individualized communications or treatment. For example, email systems or pseudonymized statistical data typically would not be subject to this privacy policy requirement.

Controllers and processors do not have to explicitly state compatible data practices that are not routinely used. For example, a 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.

Subsection (b) requires the privacy policy to be reasonably available to the data subject at the time data is collected. This does not require providing a data subject with individual notice. Placement of the privacy policy on a public website or posting in a location that is accessible to data subjects is sufficient.

Section 7. Compatible Data Practice

(a) A controller or processor may engage in a compatible data practice without the data subject's consent. The following factors apply to determine whether processing of personal data constitutes a compatible data practice:

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

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

(3) the type and nature of the data collected;

(4) the risk of a negative consequence on the data subject of the proposed use or disclosure of the data;

(5) the effectiveness of a safeguard against unauthorized use or disclosure of the data; and

(6) the extent to which the practice advances the economic, health, or other interests of the data subject.

(b) A compatible data practice includes processing that:

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

(2) is reasonably necessary to comply with a legal obligation or regulatory oversight of the controller;

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

(4) permits appropriate internal oversight of the controller or external oversight by a government unit or the controller's agent;

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

(6) permits analysis for generalized research or research and development of a new product or service;

(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;

(F) threat to national security.

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

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

(10) is consistent with the ordinary expectations of data subjects or is likely to substantially benefit data subjects.

(c) A controller may use personal data to deliver targeted content and advertising to an individual. The controller also may disclose pseudonymized data to a third-party controller for this purpose. This subsection applies only to targeted delivery of purely expressive content. Personal data or pseudonymized data may not be used for individualized decisional treatment, including to set a price or another term in a transaction. The processing of personal data or pseudonymized data for individualized decisional treatment is an incompatible data practice unless the processing is otherwise compatible under this section. ~~This~~ Nothing in this subsection ~~does not~~shall be construed to prevent a controller from—

(1) providing special considerations to members of loyalty or award programs or require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain; or

(2) offering a different price, rate, level, quality, or selection of goods of services to a consumer, including offering goods or services for no fee, if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(d) A controller may process personal data in accordance with the rules of a voluntary consent standard under Sections 11 through 14 to which the controller has committed in its privacy policy unless a court has prohibited the processing or found it to be an incompatible data

practice.

Comment

Compatible data practices are mutually exclusive from incompatible and prohibited data practices described in Sections 8 and 9. Although compatible practices do not require specific

consent from each data subject, they nevertheless must be reflected in the publicly available privacy policy as required by Section 6.

Subsection (a) provides a list of factors that can help determine whether a practice is or is not compatible. Subsection (b) provides a list of nine specific practices that are per se compatible and do not require consent from the data subject followed by a tenth gap-filling category that covers any other processing that meets the more abstract definition of "compatible data practice." The factors listed in subsection (a) inform how the scope of "compatible data practice" should be interpreted. The catch-all provision in (b)(10) allows controllers and processors to create innovative data practices that are unanticipated and do not fall into the scope of one of the conventional compatible practices to proceed without consent as long as data subjects substantially benefit from the practice. In order to find that data subjects substantially benefit from the practice, a court should ask whether data subjects would be likely to prefer that the processing occur and would be likely to consent to the processing if it were not for the transaction costs inherent to consenting processes.

Practices that qualify as compatible under subsection (b)(10) include detecting and reporting back to data subjects that they are at some sort of risk, e.g. of fraud, disease, or criminal victimization. Another example is processing that is used to recommend other purchases that are complements or even requirements for a product that the data subject has already placed in a virtual shopping cart. Both of these examples are now routine practices that consumers favor, but when they first emerged, they seemed creepy. Subsection (b)(10) is intentionally reserving space, free from regulatory burdens, for win-win practices of this sort to emerge. This allowance for beneficial repurposing of data makes CUPIDA different in substance from the GDPR, which restricts data repurposing unless __ and which gives data subjects a right to object to any processing outside certain limited "legitimate grounds" of the controller. (Articles 5(1)(b), 18, and 22 of the General Data Protection Regulation.)

The compatible data practice described in (b)(6) includes the use of personal data to initially train an AI or machine learning algorithm. The actual use of such an AI or machine learning algorithm in order to make a communication or decisional treatment must fall into one of the other categories of compatible data practices in order to be considered compatible.

Subsection (c) 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 based on behavioral advertising rather than using the context of the website alone. This marks a substantial departure from the California Consumer Privacy Act and other privacy acts that have been introduced in state legislatures, including the Washington Privacy Act Sec. 103(5) and the proposed amendments to the Virginia Consumer Data Protection Act Sec. 59.1-573(5). All of these bills permit data subjects to opt out of the sale or disclosure of personal data for the purpose of targeted advertising.

Under subsection (c), websites and other controllers cannot use or share data even in pseudonymized form for tailored treatment unless tailoring treatment is compatible for an entirely different reason. For example, a firm that shares pseudonymized data with a third party controller for the purpose of creating "retention models" or "sucker lists" that will be used by

the third party or by the firm itself to modify contract terms cannot rely on subsection (c), because the processing is used for targeted decisional treatment. The firm also cannot rely on subsection (b)(10) or any other provision of this section because the processing is unanticipated and does not substantially benefit the data subject. (*See* Maddy Varner & Aaron Sankin, *Sucker List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders,* THE MARKUP (February 25, 2020) for an allegation that provides an example of this sort of processing.) By contrast, a firm that runs a wellness-related app and shares pseudonymized data with a third party controller for the purpose of researching public health generally or for assessing a health risk to the data subject specifically would be in a different posture. Like the "sucker list" example, this controller might not be able to rely on subsection (c) because the processing may be used to guide a public health intervention or to modify recommendations that the wellness app gives to the data subject. Nevertheless, the app producer could rely on subsection (b)(10) for processing that changes the function of the app itself because this processing, while potentially unanticipated, redounds to the benefit of the data subject without meaningfully increasing risk of harm. The app producer could rely on subsection (b)(6) for disclosure of pseudonymized data to produce generalized research (which then may be used for general public health interventions.)

Subsection (c) also clarifies that loyalty programs that use personal data to offer discounts or rewards are compatible practices. Although the targeted offering of discounts or rewards would constitute decisional treatment, these are accepted and commonly preferred practices among consumers. Indeed, most loyalty programs would qualify as compatible practices under subsection (b)(1) since customers typically affirmatively subscribe or sign up for them in order to receive discounts and rewards.

Subsection (d) incorporates any data practice that has been recognized as compatible through a voluntary consent process as one of the per se compatible data practices, effectively adding these to the list contained in subsection (c).

Section 8. Incompatible Data Practice

(a) Processing is an incompatible data practice even if it otherwise is a compatible data practice if it contradicts or is not disclosed in the privacy policy of the controller as required by Section 6 of this [act].

(b) ~~If a third party~~A controller or a processor shall not be liable if another controller or processor engages in an incompatible data practice~~, a collecting controller is deemed to have engaged in the same practice if the collecting controller knew or should have known that the personal data would be used for the practice and was in a position to prevent the practice.~~

(c) A controller may not engage in an incompatible data practice unless, at the time the

personal data is collected about the data subject:

(1) the controller, or a previous controller that was a collecting controller, provided sufficient notice and information to the data subject that the subject's personal data may be processed for incompatible data practice; and

(2) the subject had a reasonable opportunity to withhold consent to the practice.

(d) A controller may not process a data subject's sensitive data for an incompatible data practice without obtaining the subject's express, voluntary, and signed consent in a record for each practice.

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

Comment

An incompatible data practice is an unanticipated use of data that is likely to cause neither substantial harm nor substantial benefit to the data subject. (The former would be a prohibited data practice and the latter would be a compatible one.) An example of an incompatible data practice is a firm that develops an app that sells user data to third party fintech firms for the purpose of creating novel credit scores or employability scores.

Subpart (d) assigns responsibility (and, potentially, liability) to controllers who negligently or knowingly provide personal data to others who engage in an incompatible data practice.

Statements in a privacy policy do not meet the standards of notice required in subpart (e).

Subpart (f) makes clear that a firm may condition services on consent to processing that would otherwise be incompatible. In other words, if the business model for a free game app is to sell data to third party fintech firms, the app developers will have to receive consent that meets the requirements of subpart (d). But the firm can also refuse service to a potential customer who does not consent. This is distinguishable from the California Privacy Rights Act's nondiscrimination provision, which permits variance in price or quality of service only if the difference is "reasonably related to the value provided to the business by the consumer's data." (California Privacy Rights Act Section 11.)

Section 9. Prohibited Data Practice

(a) A controller or data processor may not engage in a prohibited data practice. A prohibited data practice is processing personal data in a manner that is likely to:

(1) inflict on a data subject specific and significant financial, physical, or reputational harm, undue embarrassment or ridicule, intimidation, orharassment;

(2) cause misappropriation of personal data to assume another's identity;

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

(4) constitute a clear violation of federal law or law of this state other than this [act];

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

(6) process without consent under Section 8 personal data in a manner that is an incompatible data practice;

(7) violate a federal or state law against discrimination; or

(8) cause harm to a data subject or another that cannot be cured effectively by consent.

(b) It is a prohibited data practice to collect or create personal data by reidentifying or causing the reidentification of pseudonymized ordeidentified data unless:

(1) the reidentification is performed by a controller or data processor that had previously deidentified or pseudonymized the data;or

(2) the purpose of the reidentification is to assess the privacy risk of deidentified data and the person does not use or disclose reidentified personal data except to demonstrate a privacy vulnerability to the controller or processor that created the deidentified data.

(c) ~~If a third-party~~ A controller or processor shall not be liable if another controller or processor engages in a prohibited data practice~~, a controller is deemed to have engaged in the same practice if the controller knew or should have known that the personal data would be used for the practice.~~

Comment

Reidentification of previously deidentified data is a prohibited practice unless the reidentification fits one of the exceptions in subpart (b). Exception (b)(1) covers controllers or processors that are in the practice of pseudonymizing personal data for security reasons and then reidentify the data only when necessary. This exception covers controllers or processors who already have the right and privilege to process personal data. Exception (b)(2) exempts "white hat" researchers who perform reidentification attacks in order to stress-test the deidentification protocols. These researchers may disclose the details (without identities) of their demonstration attacks to the general public, and can also disclose the reidentifications (with identities) to the controller or processor.

Section 10. Data Privacy and Security Assessment

(a) A controller or data processor shall prepare in a record a data privacy and security risk assessment. The assessment may take into account the controller or processor's size, scope and type of business and the resources available to it. The assessment shall evaluate the:

(1) privacy and security risks to the confidentiality and integrity of the personal data being processed or maintained, the likelihood of occurrence of such risks, and the impact that such risk would have on the privacy and security of the personal data.

(2) efforts taken to mitigate such risks, and

(3) extent to which its data practices comply with the provisions of this [act].

(b) The data privacy and security risk assessment shall be updated if there is a change in the risk environment or in a data practice that may materially affect the privacy or security of the personal data.

(c) A data privacy and security assessment is confidential business information [and is not subject to a public records request or discovery in a civil action]. The fact that a controller or

processor conducted an assessment, the facts underlying the assessment, and the date of the assessment are not confidential information.

Legislative Note: *The state should include appropriate language in subsection (c) exempting a data privacy assessment from an open records request and discovery in a civil case to 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. Compliance with Other Data Protection Laws

(a) A controller or processor complies with this [act] if it complies with a comparable personal data protection law in another jurisdiction and the [Attorney General] determines the law in the other jurisdiction is as, or more protective, of personal data than this [act]. The Attorney General may set a fee to be charged to a person asserting it complies with a comparable personal data law under this subsection, which must reflect the cost reasonably expected to be incurred by the [Attorney General] in determining whether the asserted act is equally or more protective than this [act].

(b) Personal data processing that is subject to the following shall be considered in compliance with this [act]:

(1) the Health Insurance Portability and Accountability Act, Pub. L. 104-191, if the controller or processor is regulated by that act;

(2) processing in connection with an activity 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], a

furnisher of the information, or a person procuring or using a consumer report;

(3) for sections 7 and 8 only, processing by a financial institution that processes personal information to the extent that ~~if~~ the information is subject to and in compliance with the Gramm-Leach-Bliley Act of 1999, 12 U.S.C. Section 24a, et. Seq [, as amended]~~, or is treated as subject to that act's data privacy and security requirements~~;

(4) for sections 7 and 8 only, processing by an entity other than a financial institution to the extent that~~if~~ the personal information is subject to and in compliance with the Gramm-Leach-Bliley Act;

(5) the Drivers Privacy Protection Act of 1994, 18 U.S.C. Section 2721 et seq.[, as amended];

(6) the Family Education Rights & Privacy Act of 1974, 20 U.S.C. Section 1232[, as amended];

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

Legislative Note: *It is the intent of this act to incorporate future amendments to the cited federal laws. In a state in which the constitution or other law does not permit incorporation of future amendments when a federal statute is incorporated into state law, the phrase "as amended" should be omitted. The phrase also should be omitted in a state in which, in the absence of a legislative declaration, future amendments are incorporated into state law.*

Comment

Companies that collect or process personal data, particularly larger ones, have an interest in adopting a single set of data practices that satisfy the data privacy requirements of multiple jurisdictions. It is likely that such firms will adopt practices to meet the most demanding laws among the jurisdictions in which they do business. Compliance costs can be quite burdensome and detrimental to smaller firms that in the ordinary course of business must collect consumer data. The purpose of this section is to permit, in practice, firms to settle on a single set of practices relative to their particular data environment.

This section also greatly expands the potential enforcement resources for protecting consumer data privacy. Adoption of this act confers on the state attorney general, or other privacy data enforcement agency, authority not only to enforce the provisions of this act but also to enforce the provisions of any other privacy regime that a company asserts as a substitute for compliance with this act.

Commented [A2]: We suggest that the exemption outlined in Section 11(b)(3) and Section 11(b)(4) be limited to Section 7 and 8 activities so that a entity subject to GLBA is required to comply with a consumer's request for a copy of data or a correction to data as outlined in Section 5 and communicated by a collecting controller.

33

The Attorney General is authorized to charge a reasonable fee for determining whether a particular law is equally or more protective than this act. It is assumed here that a reasonable consensus will be achieved within the enforcement community that will accept major comprehensive legislation as in compliance with this section. Accordingly, accepting the consensus would not require intensive activity by the Attorney General and would thus not result in a significant fee. Moreover once another law was determined to be in compliance in a particular jurisdiction, it would not require further examination.

Subsection (b) provides per se rules that provide that data subject to specific federal privacy regimes is not governed by this act. This provision does not exempt entities regulated by these federal provisions. Data practices that are not subject to federal regulations under the stated enactments are governed by this act.

Section 12. Compliance with Voluntary Consensus Standard

If the [Attorney General] recognizes a voluntary consensus standard under Section 15, a controller or data processor complies with this [act] if it adopts and complies with the standard.

Comment

Developing detailed common rules for data practices applicable to a wide variety of industries is particularly challenging. Data practices differ significantly from industry to industry. This is reflected in a number of specific federal enactments governing particular types of data (HIPPA for health information) or particular industries (Graham-Leach-Bliley for financial institutions). The Act imposes fundamental obligations on controllers and data processors to protect the privacy of data subjects. These include the obligations to allow data subjects to access and copy their data, to correct inaccurate data, to be informed of the nature and use of their data, to expect their data will only be used as indicated when it is collected, and to be assured there are certain data practices that are prohibited altogether. No voluntary consensus standard may undermine these fundamental obligations.

On the other hand, how these obligations are implemented may depend on the particular business sector. Developing processes for access, copying, and correction of personal data can be a complex undertaking for large controllers. And consumers have vastly different expectations about the use of their personal information depending on the underlying transaction for which their data is sought. Signing up for a loyalty program is far different than taking out a mortgage. Providing an opportunity for industry sectors, in collaboration with stakeholders including data subjects, to agree on methods of implementing privacy obligations provides the flexibility any privacy legislation will require. There is some experience, primarily at the federal level, of permitting industries to engage in a process to develop voluntary consensus standards that can be compliant with universal regulation and yet tailored to the particular industry.

Voluntary consensus standards are NOT to be confused with industry codes or other forms of self-regulation. Rather these standards must be written through a private process that assures that all stakeholders participate in the development of the standards. That process is set out in the following sections. Any concerns regarding self-regulation are also addressed in this

act by requiring the Attorney General to formally recognize standards as being in substantial compliance with this Act. Thus there must be assurance that any voluntary consensus standard fully implements the fundamental privacy protections adopted by the act.

The act creates a safe harbor for covered entities that comply with voluntary consensus standards, recognized by the state Attorney General, that implements the Act's personal data privacy protections and information system security requirements for defined sectors and in specific contexts. These voluntary consensus standards are to be developed in partnership with consumers, businesses, and other stakeholders by organizations such as the American National Standards Institute, and by using a consensus process that is transparent, accountable and inclusive and that complies with due process. This safe harbor for voluntary consensus standards is modeled on Articles 40 and 41 of the GDPR, which provides for recognition of industry "codes of conduct," the Consumer Product Safety Act ("CPSA"), 15 U.S.C. § 2056, *et seq.*, which uses voluntary consensus standards to keep consumer products safe, and the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § § 6501-6506, which uses such standards to protect children's privacy online. This provision of the Act is in conformity with the Office of Management and Budget (OMB) Circular A-119, which establishes policies on federal use and development of voluntary consensus standards. Thus there is not only precedent for the adoption of voluntary consensus standards but actual experience in doing so.

By recognizing voluntary consensus standards, the Act provides a mechanism to tailor the Act's requirements for defined sectors and in specific contexts, enhancing the effectiveness of the Act's privacy protections and information system security requirements, reducing the costs of compliance for those sectors and in those contexts, and, by requiring that the voluntary consensus standard be developed through the consensus process of a voluntary consensus standards body, the concerns and interests of all interested stakeholders are considered and reconciled, thus ensuring broad-based acceptance of the resulting standard. Finally, by recognition of voluntary consensus standards by the Attorney General, the Act ensures that the voluntary consensus standard substantially complies with the Act.

Voluntary consensus standards also provides a mechanism to provide interoperability between the act and other existing data privacy regimes. The Act encourages that such standards work to reasonably reconcile any requirements among competing legislation, either general privacy laws or specific industry regulations. For example, it would provide an opportunity for firms that process both financial, health, and other data to attempt to create a common set of practices that reconcile HIPPA and GLB regulations with that applicable under this act for other personal data.

Section 13. Content of Voluntary Consensus Standard

A stakeholder may initiate a process to develop a voluntary consensus standard for compliance with a requirement of this [act]. A voluntary consensus standard may address any data practice, including:

(1) identification of compatible data practices for an industry;

(2) the process and method for securing consent of a data subject for an incompatible data practice;

(3) a common method for responding to a request by a data subject for access to or correction of personal data, including a mechanism for authenticating the subject;

(4) a format for a data privacy policy that will provide consistent and fair communication of the policy to data subjects;

(5) a set of practices that provides reasonable security to personal data maintained by a controller or data processor; and

(6) any other policy or practice that relates to compliance with this [act].

Comment

This section clarifies the policies and practices that seem most appropriate for voluntary consensus standards and most likely to differ among industry sectors. The list of policies and practices is not intended to be exclusive. The section, however, does make clear that any such standards must remain consistent with the act's privacy protection obligations on controllers and processors.

Section 14. Process for Development of Voluntary Consensus Standard

The [Attorney General] may recognize a voluntary consensus standard that is developed by a voluntary-consensus-standards body through a process that:

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

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

(B) gives fair consideration to each comment by a stakeholder;

(C) responds to each good-faith objection by a stakeholder;

(D) attempts to resolve each good-faith objection by a stakeholder;

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

(F) informs each stakeholder of the disposition of each objection and the reason for the disposition;

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

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

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

(5) includes a right for a stakeholder to file a statement of dissent.

Comment

This section outlines the process required for the adoption of voluntary consensus standards in order to allow them to be considered a safe harbor under this act. The process is consistent with OMB A-119 and has been utilized by industries and accepted by federal regulatory agencies. The development and operation of the process required by this section is the responsibility of the voluntary consensus organization that facilitates development of the standards. The role of the Attorney General would be only to assure that the resulting standards were developed by such a process.

Section 15. Recognition of Voluntary Consensus Standard

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

(1) protects the rights of data subjects under Sections 5 through 9; and

(2) is developed by a voluntary consensus standards body through a process that substantially complies with Section 14 of this [Act]; and

(3) reasonably reconciles the requirements of this [act] with the requirements of other federal and state law.

(b) The [Attorney General] shall adopt rules under [cite to state administrative procedure act] that establish a procedure for filing a request under this [act] to recognize a voluntary consensus standard. The rules may:

(1) require the request to be in a record demonstrating that the standard and process through which it was adopted comply with this [act];

(2) require the applicant to indicate whether the standard has been recognized as appropriate elsewhere and, if so, identify the authority that recognized it; and

(3) set a fee to be charged to the applicant, which must reflect the cost reasonably expected to be incurred by the [Attorney General] in acting on a request.

(c) The [Attorney General] shall determine whether to grant or deny the request and provide the reason for a denial. In making the determination, the [Attorney General] shall consider the need to promote predictability and uniformity among the states and give appropriate deference to a voluntary consensus standard developed consistent with this [act] and recognized by a privacy-enforcement agency in another state.

(d) The Attorney General may withdraw recognition of a voluntary consensus standard if the Attorney General finds that its provisions or its interpretation is not consistent with this [act].

(e) A voluntary consensus standard recognized by the Attorney General shall be available to the public.

Comment

This section makes clear that the basic privacy interests of consumers will be protected throughout any voluntary consensus standards process. Each state Attorney General or other data privacy enforcement agency must assure that the rights accorded to consumers under this Act with respect to their personal data are preserved. To be recognized as compliant with this act, the Attorney General must determine that the standards were adopted through a process outlined in Section [ ], which will assure that all stakeholders including representatives of data subjects are involved. The Attorney General must also confirm that the standards are consistent with the act's imposed obligations on controllers and processors. And the Attorney General must find the

standards reasonably reconcile other competing data privacy regimes.

Any industry or firm seeking to establish a set of voluntary consensus standards would have the burden of convincing the Attorney General that the standards comply with this section. It is recognized that this standard setting process can be expensive and thus the incentive for particular industries to participate will be determined in part by their expectation that standards will be treated consistently from state to state. Thus, the act contains provisions that encourage the Attorney General of each state in which this act is adopted to collaborate with Attorneys General from other states.

The Attorney General is encouraged to work with other states to achieve some uniformity of application and acceptance of these standards. While the act recognizes the State's inherent right to determine the level of data privacy protection it does encourage the Attorney General to take the actions of other states into account.

Currently the National Association of Attorneys General has created a forum through which various state Attorney Generals offices share policies and enforcement actions related to consumer protection including specifically data privacy. This activity suggests it is realistic to believe that consistency across states can be achieved.

The section also authorizes the Attorney General to charge a fee commensurate with the expense of reviewing requests for recognition of voluntary consensus standards. Such a fee is appropriate to assure adequate resources for this process and as a cost of seeking a safe harbor from otherwise applicable legislation.

Section 16. Enforcement

(a) The enforcement provisions of [cite to state consumer protection act] apply to a violation of this [act].

(b) A knowing violation of this [act] is subject to all remedies, penalties, and authority granted by [cite to state consumer protection act]. A person that engages in conduct that had previously been determined by the Attorney General or a court to be a prohibited data practice, or that engages in conduct that had previous been determined by the Attorney General or a court to be an incompatible practice without having received the consent of data subjects as required by Section 8, is presumed to have knowingly violated this act. Any other violation of this [act] is subject to enforcement by injunctive relief or cease and desist orders.

(c) The [Attorney General] may adopt rules to implement this [act] under [cite to state

administrative procedure act].

(d) In adopting rules under this section, the [Attorney General] shall consider the need to promote predictability for data subjects, regulated entities and uniformity among the states consistent with this [act] and is encouraged to:

(1) consult, if deemed appropriate, with Attorneys General or other personal data privacy enforcement agencies in other jurisdictions that enact an act substantially similar to this [act];

(2) consider any suggested or model rules or enforcement guidelines promulgated by the National Association of Attorneys General or any successor organization;

(3) consider the rules and practices of Attorneys General or other personal data privacy enforcement agencies in other jurisdictions; and

(4) consider any voluntary consensus standards developed consistent with the requirements of this [act], particularly if such standards have been recognized and accepted by other Attorneys General or other personal data privacy enforcement agencies.

(e) In any action or proceeding to enforce a provision of this Act by the [Attorney General], in which the [Attorney General] prevails, the [Attorney General] may recover reasonable expenses and costs incurred in investigation and prosecution of the case.

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

Legislative Note: *In subsection (b) the state should cite to the state's administrative procedure act or other act regulating the adoption of rules and regulations.*

Comment

The challenge in uniform state legislation when agencies are given the power to adopt implementing rules and regulations is to continue to assure a reasonable degree of uniform application and enforcement of the substantive provisions. This is not a unique problem here where the state Attorney General or any other personal data privacy enforcement agency will be required to implement and enforce standards that are, by their nature, flexible so they may be

implemented by diverse industries. Nor is this a problem limited to data privacy protection. Every state has adopted a general consumer protection law that governs transactions of interstate businesses within the state. The enforcement provision here is modeled after these "little FTC acts" and merely provides detail and specificity related to data privacy.

What remains uniform by adopting this act is the acknowledgement of the rights of consumers to obtain access to data held about them, to correct inaccurate data, and to be informed of the uses to which their data may be put. The distinction in this act between compatible, incompatible, and prohibited uses of personal data would create a uniform approach to the use of personal data although the very concept of "compatible" use is dependent on the nature of the underlying transaction from which the data is collected.

In order to encourage as much uniformity as possible, the state Attorney General is encouraged by subsection (c) to attempt to harmonize rules with those in other states that have adopted this act. The Attorney General may also consider voluntary consensus standards that have been approved in other states, but, of course, there is no requirement that he accept them unless they have been previously approved in this state. These provisions are derived from section 9-526 of the Uniform Commercial Code which has been successful in harmonizing the filing rules and technologies for security interests by state filing offices. While there is not a direct analogy between privacy enforcement and filing rules, the potential, it demonstrates that legislation can successfully encourage state officials to cooperate as a substitute for federal dictates.

The section applies to general policies and not to the decision to bring a particular enforcement action. The latter decision is one for prosecutorial discretion.

Subsection (e) allows the Attorney General to recover the reasonable costs of investigation and prosecution of cases under this act if the Attorney General prevails. Attorneys fees are not included because in most instances those are the salaries of regular office legal staff. However, the salary costs associated with a particular case would be included in the reasonable costs of investigation and prosecution. A comparable provision was adopted in Virginia.

Many states have adopted some form of private remedy for some violations of their consumer protection acts. In some states private causes of action are authorized only for violations of established rules rather than the general prohibition against unfair or deceptive acts. Others may impose procedural requirements such as requiring plaintiffs to engage with the Attorney General before bringing a suit. See, National Consumer Law Center, Unfair and Deceptive Acts and Practices (9th ed. 2016). As section 17 makes clear, this act defers to existing state law and practice with regard to whether this act creates a private cause of action. But even in states that allow for private causes of action, the plaintiffs must be prepared to show that the violation was a knowing violation which will generally require the plaintiffs to show that the defendant had notice that the practice or omission that they committed was illegal. Nothing in this act is intended to displace traditional common law or other statutory remedies invasions of privacy or other wrongs.

Section 17. Limits of Act

This [act] does not create, affect, enlarge, or diminish any cause of action under law of this state other than this [act].

Comment

The use of personal data can be implicated in traditional causes of action for defamation, right to privacy, intentional infliction of emotional suffering, or similar actions. In some states these actions remain at common law; in others they are creates of statutes. This section assures that those causes of action remain unaffected by this act.

Section 18. Uniformity of Application and Construction

In applying and construing this uniform act, a court shall consider the promotion of uniformity of the law among jurisdictions that enact it.

Section 19. Electronic Records and 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.[as amended][, as in effect on [the effective date of this [act]], but does not modify, limit, or supersede 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in 15 U.S.C. Section 7003(b).

Legislative Note: *It is the intent of this act to incorporate future amendments to the cited federal law. In a state in which the constitution or other law does not permit incorporation of future amendments when a federal statute is incorporated into state law, the phrase "as amended" should be omitted. The phrase also should be omitted in a state in which, in the absence of a legislative declaration, future amendments are incorporated into state law.*

[Section 20. Severability

If any provision of this [act] or its application to a person or circumstance is held invalid, the invalidity does not affect another provision or application that can be given effect without the invalid provision.]

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 21. Effective Date

This [act] takes effect [180 days after the date of enactment].

Legislative Note: *The legislative drafter may wish to include a delayed effective date of at least 60 days to allow time to all applicable agencies and industry members to prepare for implementation and compliance.*