D R A F T

FOR APPROVAL

Uniform Personal Data Protection Act

Uniform Law Commission

MEETING IN ITS ONE-HUNDRED-AND-THIRTIETH YEAR
MADISON, WISCONSIN
JULY 9 – 15, 2021

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.

June 30, 2021

Uniform Personal Data Protection 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*
Peter Winn	U.S. Department of Justice
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

Uniform Personal Data Protection Act

Table of Contents

Uniform Personal Data Protection Act

Prefatory Note

Participation in today's digital economy involves the aggregation and use of much more information about individuals than generally appreciated by those individuals. For a generation, Internet content has been financed in large part by targeted advertising requiring the collection of information about both knowing and unknowing participants. Lending, insurance, and Internet commerce more generally have also come to increasingly rely on the intensive use of a greater quantity of personal data. Social media platforms encourage the voluntary posting of personal information, and that data, too, is used in ways that participants do not fully anticipate or appreciate. Technologies that monitor an individual's activities, location, and conversations have become commonplace in the digital economy. This information, collected in very large data sets, allow correlations and discernment of patterns that are applied to targeting and decision-making that may or may not be procedurally sound or acceptable to our communities. In the modern data economy, personal data not only permits a transaction to take place, but the data itself becomes a business asset to be bought and sold.

Until recently, personal information privacy or autonomy in the United States was primarily concerned with protecting individuals from unreasonable governmental intrusion. State common law developed by the mid-twentieth century against "highly offensive" intrusion and misappropriation of name or likeness – rooted in response to paparazzi photographic activity and balanced with First Amendment sensibilities. However, in the late 1960s and early 1970s, American scholars and lawmakers began to develop and recognize "Fair Information Practice Principles" (FIPPs). These principles encourage data collectors to receive consent from data subjects (or at least provide notice) before data is collected or repurposed, and they encourage data collectors to recognize an individual's right to access, correct, or delete personal data. A version of these principles was implemented in federal sectoral privacy laws such as the Fair Credit Reporting Act ("FCRA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the Privacy Act (which regulates how the federal government itself collects and uses personal data).

The European Union ("EU"), with its organizational recognition of privacy as a human right, applied FIPPs to the creation and automated processing of databases of personal information regardless of sector or context in its 1995 Data Protection Directive. This directive was refined for an EU-wide General Data Protective Regulation ("GDPR"), which went into effect in 2018. The GDPR speaks in terms of "processing" of "personal data," whether "collected from" the individual ("data subject") (Art. 13) or not (Art. 14) and appears to include information made "available" publicly. Thus, it may be said that under the GDPR and EU organizational law, the data subject has some ownership interest in their personal data, however collected. The GDPR thus imposes obligations on data collectors and data processors to inform consumers of how their data will be used, to secure their consent for each collection and use, and to delete the data upon request. Together, these obligations greatly constrain the collection and use of personal data, and the free movement of data within the EU.

In the United States, by contrast, the collection and productive use of information (including personal information) implicates free speech rights and is thus protected to some degree from government regulation. The application of the First Amendment to collection of information was exemplified in Sorrell v. IMS Health Inc., 564 U.S. 552 (2011), where data collected and analyzed by private companies was found to be speech and thus protected from governmental regulation unless justified by a significant governmental interest.

By 2018, discussions about omnibus privacy protection in the United States were premised on the FIPPs (including security, notification/transparency, access, correction and deletion "rights" outside tradition U.S. notions of "privacy"). In that context, the California Consumer Privacy Protection Act ("CCPA") adopted a comprehensive personal data protection act adopting many of the approaches of the GDPR. The Virginia Consumer Data Protection Act ("VCDPA") adopts a similar model. However, efforts in other states have faltered because of the significant compliance costs that these laws impose on businesses and, indirectly, their customers.

Online services are most efficient when data can cross state borders. A uniform approach to personal data protection is therefore valuable. However, large international companies are subject to the GDPR and have invested considerable resources in bringing their data practices into compliance. Companies doing business in California will need to comply with the extensive regulatory structure of the California statute. The cost of compliance has required that California and Virginia limit their rules to large data collectors or processors. Smaller firms are expressly exempt. Thus, consumer data protection in these U.S. states is at once burdensome for larger companies and not applicable to smaller ones.

The Uniform Personal Data Protection Act ("UPDPA") provides a reasonable level of consumer protection without incurring the compliance and regulatory costs associated with the California and Virginia regimes. Some provisions of the Act are applicable to all data collectors and processors within the state and thus provide overall a more extensive data protection regime. The Act recognizes the need to create an omnibus privacy law to protect personal data from the excesses and abuses of an unregulated data economy by small actors as well as large. The Act shares many of the recognizable elements of the CCPA, VCDPA and GDPR. Generally following FIPPs, the UPDPA establishes rights for data subjects to access and correct personal data and obligations for controllers and processors to provide transparency, to draft privacy and security impact assessments, and to responsibly restrict the use of personal data.

However, this Act differs from the CCPA, CDPA, and the GDPR by recognizing that the economy, the general public, and consumers themselves are often well-served by allowing expected uses of data to proceed without consent, and by permitting firms to make useful innovations that will be unexpected when first implemented. The Act is unique among U.S. privacy regulations by using the concept of compatibility introduced in the Privacy Act and applied in GDPR. A controller can process personal data without consent if the processing is aligned with the ordinary expectations or direct interests of data subjects. Consent is only required for data practices that are *incompatible* with expectations or clear interests of the data subject. The act requires a data collector to be transparent as to its compatible uses and avoids

the largely wasteful process of seeking consent for processing that is already within the expectations of the consumer.

The Act does require consent for processing that is incompatible with the expectations and direct interests of consumers. For this processing, a firm must provide notice and an opportunity for the consumer to withhold consent. The Act requires explicit consent for the incompatible processing of certain sensitive pieces of data. And it prohibits certain types of processing that create a high risk of harm to consumers.

The Act distinguishes between two types of controllers—collecting controllers and third-party controllers—and establishes that collecting controllers (who typically have a direct relationship with the data subject) provide the means for data subjects to access and correct their personal data. Any request for correction would then be transmitted by the collecting controller to downstream controllers and processors. This focuses responsibility for access and correction on the entity known by the data subject and with a preexisting established relationship. It is a fair limit to the reach of FIPPs-based data subject rights.

The Act addresses the need for uniformity, both for compliance and consumer protection, in a variety of ways. Compliance with other legislative privacy regimes, such as GDPR or CCPA, and that provide similar data protection to this Act, will be deemed to be sufficient to comply with this Act. The Act also recognizes and exempts from its terms processing governed by industry-specific federal regimes.

Adapting a comprehensive data protection act that will be applied in a wide variety of different industries presents a challenge. For example, what might be a compatible use for a small retailer may not be such a use for a large on-line seller. The Act addresses this problem by incorporating a mechanism for creation of voluntary consensus standards. The development of these standards for particular industries is a well-established process at the federal level and has been adopted for the Child On-line Privacy Protection Act. It establishes a process whereby all stakeholders of an industry—not only industry members but also consumers and persons representing the public interest – negotiate a set of specific standards that reasonably interpret the requirements of the Act within a specific context. Once established and recognized by the state's Attorney General, any controller or processor can explicitly adopt and comply with the voluntary consensus standard. Moreover, there is an expectation that a voluntary consensus standard approved in one UPDPA state will be applicable in the others.

The Act incorporates the enforcement and remedial provisions of existing consumer protection acts in the various states. Enforcement of the Act is primarily a function of the state Attorney General.

Altogether, the provisions of this act provide substantial protection to data subjects while reflecting pragmatism and optimism about the data-driven economy. The Act is pragmatic by keeping compliance costs manageable and by avoiding obvious conflicts with the First Amendment. The Act is optimistic by leaving room for unexpected, beneficial innovations in the creative use of personal data. And the Act avoids high compliance and regulatory costs associated with more restrictive regimes.

Uniform Personal Data Protection Act

Section 1. Title

This [act] may be cited as the Uniform Personal Data Protection Act.

Section 2. Definitions

In this [act]:

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

(2) "Compatible data practice" means processing consistent with Section 7.

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

(4) "Data subject" means a resident of this state who is identified or described by personal data.

(5) "Deidentified data" means personal data that is modified to remove all direct identifiers and to reasonably ensure that the record cannot be linked to an identified data subject by a person that does not have personal knowledge or special access to the data subject's information.

(6) "Direct identifier" means information that is commonly used to identify a data subject, including name, physical address, email address, recognizable photograph, telephone number, and Social Security number.

(7) "Incompatible data practice" means processing that may be performed lawfully under Section 8.

(8) "Maintains", with respect to personal data, means to retain, hold, store, or preserve personal data as a system of records used to retrieve records about individual data

subjects for the purpose of individualized communication or decisional treatment.

(9) "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.

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

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

(12) "Processor" means a person that processes personal data on behalf of a controller.

(13) "Prohibited data practice" means processing prohibited by Section 9.

(14) "Pseudonymized data" means personal data without a direct identifier that can be reasonably linked to a data subject's identity or is maintained to allow individualized communication with, or treatment of, the data subject. The term includes a record without a direct identifier if the record contains an internet protocol address, a browser, software, or hardware identification code, a persistent unique code, or other data related to a particular device. The term does not include deidentified data.

(15) "Publicly available information" means information:

(A) lawfully made 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 a 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.

(16) "Record" means information:

(A) inscribed on a tangible medium; or

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

(17) "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 access an account remotely;

(C) a credit or debit card number or financial account number;

(D) a Social Security number, tax-identification number, driver's license number, military identification number, or an identifying number on a governmental-issued identification;

(E) geolocation in real time;

(F) a 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 knows or has reason to know is under 13 years of age.

(18) "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 procedure.

(19) "Stakeholder" means a person that has, or represents a person that has, a direct interest in the development of a voluntary consensus standard.

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

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

Comment

The Act regulates the processing of personal data. The Act uses the terms "information," "record," and "personal data" as increasingly specific categories. Information would include all

potentially interpretable signs and symbols, in any form, that create knowledge about any subject. A "record" is information that is recorded in an electronic or tangible medium. Records are a subset of information. "Personal data" is the subset of records that describe an individual. The Act avoids using the term "data" on its own, as this would be coterminous with "record," References to "data" only appear in phrases such as "personal data" or "compatible data practice" that are defined terms in this Act.

The Act recognizes the distinction between controllers and 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 be within the scope of the Act under 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 act exempts public records, lawfully obtained. Laws providing for the collection, retention, and use of public records may contain privacy and security requirements or limits on how the records may be accessed and used. This act does not interfere with those other provisions.

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 processor that conducts business in

this state or produces products or provides services purposefully directed to residents of this state and:

(1) maintains personal data about more than [50,000] data subjects during a calendar year, excluding data subjects whose data is collected or maintained solely to complete a payment transaction;

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

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

(4) maintains personal data, unless it processes the personal data solely using compatible data practices.

(b) This [act] does not apply to an agency or instrumentality of this state or a political subdivision of this state.

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

(1) publicly available information;

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

(3) disclosed as required or permitted by a warrant, subpoena, or court order or rule, or otherwise as specifically required by law;

(4) subject to a public-disclosure requirement under [cite to state public records act]; or

(5) processed in the course of a data subject's employment or application for employment.

Comment

The definition of "personal data" limits that term to data describing residents of this state. This section further constrains the scope of the Act by limiting the controllers and processors obligated to comply with the act. 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 and risky uses of data, both by large and small controllers and processors.

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.

Processors and controllers who do not conduct business or market products and services to this state are outside the scope of the act.

Section 4. Controller and 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 to the data subject on request;

(2) correct or amend a data subject's personal data on the data 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 is an incompatible data practice under Section 8;

(5) abstain from using a prohibited data practice;

(6) conduct and maintain data privacy and security risk assessments under Section 10; and

(7) provide redress for an incompatible data practice or prohibited data practice the controller performs or is responsible for performing while processing a data subject's personal data.

(b) A processor shall:

(1) on request of the controller, provide the controller with a data subject's personal data or enable the controller to access the personal data at no cost to the controller;

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

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

(4) conduct and maintain data privacy and security risk assessments in accordance with Section 10; and

(5) 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.

(c) A controller or processor is responsible under this [act] for an incompatible data practice or prohibited data practice committed by another if:

(1) the practice is committed with respect to personal data collected by the controller

or processed by the processor; and

(2) the controller or processor knew the personal data would be used for the practice and was in a position to prevent it.

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.

Subsection (c) makes clear that an actor in a supply chain that violates the act can expose their business partners to liability risk if those partners had sufficient information to know what the actor was doing. Actual knowledge is required. This ensures that all actors have incentive to avoid working with irresponsible firms, to refuse to process data in a manner that is prohibited, and to end relationships with downstream processors or third party controllers that violate the act.

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 in 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) Unless personal data is pseudonymized and not maintained with sensitive data, the collecting controller, with respect to personal data initially collected by the controller and maintained by the controller or a third-party controller or processor, shall:

(1) establish a reasonable procedure for a data subject to request, receive a copy of, and propose an amendment or correction to personal data about the data subject;

(2) establish a procedure to authenticate the identity of a data subject who

requests a copy of the data subject's personal data;

(3) comply with a request from an authenticated data subject for a copy of personal data about the data subject [not later than 45 days] [within a reasonable time] after receiving it or provide an explanation of action being taken to comply with the request;

(4) on request, provide the data subject one copy of the data subject's personal data free of charge once every 12 months and additional copies on payment of a fee reasonably based on administrative costs;

(5) make an amendment or correction requested by a data subject if the controller has no reason to believe the request is unreasonable or excessive; and

(6) confirm to the data subject that an amendment or correction has been made or explain why the amendment or correction has not been made.

(b) A collecting controller shall make a reasonable effort to ensure that a correction of personal data performed by the controller also is performed on personal data maintained by a third-party controller or processor that directly or indirectly received personal data from the collecting controller. A third-party controller or processor shall make a reasonable effort to assist the collecting controller, if necessary to satisfy a request of a data subject under this section.

(c) A controller may not deny a good or service, charge a different rate, or provide a different level of quality to a data subject in retaliation for exercising a right under this section. It is not retaliation under this subsection for a controller to make a data subject ineligible to participate in a program if:

(1) the corrected information requested by the data subject makes the data subject ineligible for the program; and

(2) the program's terms of service specify the eligibility requirements for all

participants.

(d) An agreement that waives or limits a right or duty under this section is 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 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 in most cases. The only time a collecting controller will have to provide access and correction to pseudonymized data is if the data contains sensitive data, *and* the collecting controller maintains the data so that it can and will be re-associated with an individual at a later date (or transmits the pseudonymized data to a third party for its use in this way.) A collecting controller that stores user credentials and profiles of its customers can avoid the access and correction obligations if it segregates its data into a key code and a pseudonymized database so that the data fields are stored with a unique code and no identifiers. The separate key will allow the controller to reidentify a user's data when necessary or relevant for their interactions with the customers. Likewise, a collecting controller that creates a dataset for its own research use (without maintaining it in a way that allows for reassociation with the data subject) will not have to provide access or correction rights even if the pseudonymized data includes sensitive information such as gender or race. A retailer that collects and transmits credit card data to the issuer of the credit card in order to facilitate a one-time credit card transactions is not maintaining this sensitive pseudonymized data.

Subpart (c) ensures that a data subject who exercises a right to access or correction is not penalized through diminished services or access for asserting 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 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. For a denial to be prohibited by this section it must be in retaliation for a data subject's exercise of a right to access or correct data. Not every change in service following a correction of data is discriminatory. For example, a loyalty or membership club that

requires members to live in a certain region may make a member ineligible for benefits if the correction to the data shows an address outside the region. Similarly, a correction of data that shows a significant increase in the data subject's risk profile may justify an increase in insurance premium rates. Neither of these or similar actions would be "retaliation" under this section.

Section 6. Privacy Policy

(a) A controller shall adopt and comply with a reasonably clear and accessible privacy policy that discloses:

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

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

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

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

(5) the procedure for a data subject to exercise a right under Section 5;

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

(7) any voluntary consensus standard adopted by the controller.

(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 shall publish the privacy policy on the website.

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.

The act does not require a controller to adopt and comply with a single or comprehensive set of voluntary consensus standards. However, if the controller does adopt such a standard, that should be stated in the privacy policy.

Section 7. Compatible Data Practice

(a) A controller or processor may engage in a compatible data practice without the data subject's consent. A controller or processor engages in a compatible data practice if the processing is consistent with the ordinary expectations of data subjects or is likely to benefit data subjects substantially. The following factors apply to determine whether processing is a compatible data practice:

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

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

(3) the type and nature of the personal data that would be processed;

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

(5) the effectiveness of a safeguard against unauthorized use or disclosure of the personal 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 or processor;

(4) permits appropriate internal oversight of the controller or external oversight by a government unit or the controller's or processor'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 that may provide a public benefit;

(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;

(E) legal liability of the controller; or

(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) any other purpose determined to be a compatible data practice under subsection (a).

(c) A controller may use personal data, or disclose pseudonymized data to a third-party controller, to deliver targeted advertising and other purely expressive content to a data subject. Under this subsection a controller may not use personal data or disclose pseudonymized data to be used to offer terms, including terms relating to price or quality, to a data subject that are different from terms offered to data subjects generally. Processing personal data or pseudonymized data for differential treatment is an incompatible data practice unless the processing is otherwise compatible under this section. This subsection does not prevent providing special considerations to members of a program if the program's terms of service specify the eligibility requirements for all participants.

(d) A controller or processor may process personal data in accordance with the rules of a voluntary consensus standard under Sections 12 through 14 unless a court has prohibited the processing or found it to be an incompatible data practice. To permit processing under a voluntary consensus standard, a controller must commit to the standard in its privacy policy.

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, an enforcement agency 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, seemed inappropriate. 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 this act different in substance from the GDPR, which restricts data repurposing unless __ the controller 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, including programs offering special rewards, premium features, discounts, or club-card privileges, 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 (b).

Section 8. Incompatible Data Practice

(a) A controller or processor engages in an incompatible data practice if:

(1) the processing is not a compatible data practice under Section 7 and is not a prohibited data practice under Section 9; or

(2) is otherwise a compatible data practice but is inconsistent with a privacy policy adopted under Section 6.

(b) A controller may process personal data that does not include sensitive data using an incompatible data practice if at the time personal data is collected about a data subject, the controller provides the data subject with notice and information sufficient to allow the data subject to understand the nature of the incompatible data processing and a reasonable opportunity to withhold

consent to the practice.

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

(d) Unless processing is 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) 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 may not engage in a prohibited data practice. Processing personal data is a prohibited data practice if the processing is likely to:

(1) subject a data subject to specific and significant:

(A) financial, physical, or reputational harm;

(B) embarrassment, ridicule, intimidation, or harassment; or

(C) physical or other intrusion on solitude or seclusion if the intrusion would be highly offensive to a reasonable person;

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

(3) constitute a violation of other law, including federal or state law against discrimination;

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

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

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

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

(2) the data subject expects the personal data to be maintained in identified form by the controller performing the reidentification; or

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

Comment

Subsection 9(a) prohibiting certain practices applies to controllers. Under the act, it is controllers who determine the nature of processing activities.

Reidentification of previously deidentified data is a prohibited practice unless the reidentification fits one of the exceptions in subsection (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 applies to controllers or processors who already have the right and privilege to process personal data. Exception (b)(2) covers controllers who collect pseudonymized data from other controllers with the expectation that the data will be linked to the data subject's identity and maintained in identified form. An example is a credit card issuer that

receives transaction data from a retailer in pseudonymized form (with card number, for example) and subsequently associates it with a specific individual's credit account for billing and other purposes. Exception (b)(3) 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 Risk Assessment

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

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

(2) efforts taken to mitigate the risks; and

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

(b) The data privacy and security risk assessment must 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 risk assessment is confidential and is not subject to [cite to public records laws and discovery rules in a civil action]. The fact that a controller or processor conducted an assessment, the records analyzed in the assessment, and the date of the assessment are not confidential under this section.

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 of Section 10 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.

Under this section, the privacy and risk assessment is a confidential document and should not be subject to disclosure or discovery. The purpose is to assure the assessment is an honest assessment rather than a document produced for possible future litigation. However, the fact that an assessment was completed needs to be available to enforce the subsection. The assessment may also not be used to shield the underlying records analyzed in the assessment from disclosure. These records, however, may be protected from disclosure under other law.

Section 11. Compliance with Other Law Protecting Personal Data

(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 equally or more protective of personal data than this [act]. The [Attorney General] may set a fee to be charged to a controller or processor that asserts compliance with a comparable law under this subsection. The fee must reflect the cost reasonably expected to be incurred by the [Attorney General] to determine whether the comparable law is equally or more protective than this [act].

(b) A controller or processor complies with this [act] with regard to processing that is subject to the following acts or amendments thereto:

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

(2) the Fair Credit Reporting Act, 15 U.S.C. Section 1681 et seq. or otherwise is used to generate a consumer report by a consumer reporting agency as defined in 603(f) of the Fair Credit Reporting Act, 15 U.S.C. Section 1681a(f), a furnisher of the information, or a person procuring or using a consumer report;

(3) the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801 et. seq.;

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

(5) the Family Education Rights and Privacy Act of 1974, 20 U.S.C. Section 1232g; or

(6) the Children's Online Privacy Protection Act of 1998, 15 U.S.C. Section 6501 et seq.

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 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 under subsection (a) as a substitute for compliance with this act.

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 may not require extensive reexamination in other jurisdictions.

Subsection (b) provides exemptions for processing subject to specific federal privacy regimes. Data practices that are not subject to federal regulations under the stated enactments are governed by this act. A firm that maintains personal data solely for processing covered by the scope of federal privacy laws identified in subsection (b) are deemed compliant with this entire

Act. For example, a financial institution or medical facility that collects personal data and processes it for the purposes of delivery or billing related to financial or medical services is exempt from the obligations of the Act. But if the same firm processes personal data for the purpose of behavioral advertising, all of the notice, access, correction, and processing obligations of this Act will apply with respect to that processing.

Section 12. Compliance with Voluntary Consensus Standard

A controller or processor complies with a requirement of this [act] if it adopts and complies with a voluntary consensus standard that addresses that requirement and is recognized by the [Attorney General] under Section 15.

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 procedures 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.

An industry may adopt a comprehensive set of voluntary consensus standards to govern their privacy compliance policies or it may adopt a more specific standard that responds to one or more compliance requirement. For example, stakeholders of a particular industry may agree on the practices to be deemed “compatible practices” under this act, but leave other requirements to individual entity decision-making.

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 the development of a voluntary consensus standard for compliance with this [act]. A voluntary consensus standard may address any requirement including:

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

(2) the procedure 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 identity of the data subject;

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

(5) practices that provide reasonable security for personal data maintained by a controller or 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. Procedure for Development of Voluntary Consensus Standard

The [Attorney General] may not recognize a voluntary consensus standard unless it is developed through a consensus procedure that:

(1) achieves general agreement, but not necessarily unanimity, and:

(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; 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) On filing of a request by any person, the [Attorney General] may recognize a voluntary consensus standard if the [Attorney General] finds the standard:

(1) does not conflict with any requirement of Sections 5 through 10;

(2) is developed through a procedure that substantially complies with Section 14; and

(3) reasonably reconciles a requirement of this [act] with the requirements of other law.

(b) The [Attorney General] shall adopt rules under [cite to state administrative procedure act] or otherwise establish a procedure for filing a request under subsection (a). The rules may:

(1) require that the request be in a record demonstrating that the standard and procedure 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) After notice and hearing, the [Attorney General] may withdraw recognition of a voluntary consensus standard if the [Attorney General] finds that the standard or its implementation is not consistent with this [act].

(e) A voluntary consensus standard recognized by the [Attorney General] is a public record under [cite to state public records law].

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 14, 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. Applicability of [Consumer Protection Act]

(a) The enforcement authority, remedies, and penalties provided by the [cite to state consumer protection act] apply to a violation of this [act].

(b) The [Attorney General] may adopt rules under [cite to state administrative procedure act] to implement this [act].

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

(1) consult with Attorneys General or other personal-data-privacy-enforcement agencies in other jurisdictions that have an act substantially similar to this [act];

(2) consider 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 voluntary consensus standards developed consistent with this [act], that have been recognized by other Attorneys General or other personal-data-privacy-enforcement agencies.

[(d) In an action or proceeding to enforce 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: *Include subsection (e) only if the state's applicable consumer protection act does not provide for the recovery of costs and attorney's fees.*

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 existing 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. The authorization of voluntary consensus standards provides a mechanism for achieving uniformity.

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 to 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, section 9-526 demonstrates that legislation can successfully encourage state officials to cooperate as a substitute for federal dictates. The National Association of Attorneys General has a data privacy working group involving representatives from several states that could facilitate uniform application of these principles.

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. Similarly, the application of remedies or sanctions in an individual case is left to the discretion of the Attorney General, as is true for other consumer protection enforcement actions. Whether there is a violation of the Act normally does not depend on the knowledge or mental state of the actor. However, whether the actor knows or has reason to know that a particular data practice is incompatible or prohibited should influence determination of the appropriate remedy or sanction. If the actor engages in a data practice that has been determined to violate the act in a previous enforcement action or judicial decision, knowledge of wrongdoing should be presumed.

Many states have adopted some form of private remedy for violations of their existing 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).

The authorization or prohibition of a private cause of action in recent data privacy proposals has been a significant point of controversy. As section 17 makes clear, this act adopts existing state law and practice with regard to enforcement remedies and actions including whether a private cause of action is appropriate. Each state may have its own tradition for particular remedial structures. Section 17 defers to how each state has resolved these issues for violation of its existing consumer protection acts. Each state is free to determine whether its existing policies should be applicable to violations of this Act.

Nothing in this act is intended to displace traditional common law or other statutory remedies for invasions of privacy or other wrongs.

A state may adopt subsection (d) if the recovery of costs by the Attorney General is not otherwise authorized. Subsection (d) allows the Attorney General to recover the reasonable costs of investigation and prosecution of cases under this act if the Attorney General prevails. Attorney 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 recently in Virginia.

Section 17. Limits of Act

This [act] does not create or affect a cause of action under other law of this state.

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 creatures 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, or supersedes the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001 et seq.[as amended], 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).

[Section 20. Severability

If a 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 the state lacks a general severability statute or a decision by the highest court of this state adopting a general rule of severability.*

Section 21. Effective Date

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

Legislative Note: *A state may wish to include a delayed effective date to allow time for affected agencies and industry members to prepare for implementation and compliance.*