D R A F T

FOR DISCUSSION ONLY

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

SEPTEMBER 17, 2020 SESSION

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

September 4, 2020

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

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

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

OTHER PARTICIPANTS

JANE BAMBAUER	Arizona, *Reporter*
MICHAEL AISENBERG	Virginia, *American Bar Association Advisor*
DANIEL R. MCGLYNN	New Mexico, *American Bar Association Section Advisor*
STEVEN L. WILLBORN	Nebraska, *Style Liaison*
TIM SCHNABEL	Illinois, *Executive Director*

Copies of this act may be obtained from:

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

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

TABLE OF CONTENTS

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

INTRODUCTION

The Collection and Use of Personally Identifiable Data Act (CUPID) regulates enterprises that collect and use personal data from their consumers. The increasing capacity of information technology along with the growing sophistication of data analytics permits personal data to be used for a wide variety of purposes. Most fundamentally, personal data is critical to many business transactions. Financial transactions, for example, require the collection of background credit information. Loyalty programs require the collection and retention of purchasing histories. Online purchases of goods and services require personal data to authenticate the purchaser and permit delivery. Social media outlets enable us to share our news and photos with friends and associates. And, increasingly, the connection of devices to the internet, from our cell phones and virtual assistants to our automobiles and kitchen appliances, provides the opportunity for the collection of significant amounts of information about our everyday activities.

Beyond the mere collection of our personal information, various data points can be analyzed together using sophisticated algorithms to produce a profile of our activities and to predict our preferences, our health, our attitudes and our lifestyles. For example, it is reported that on-line sellers, using profile data, can set an individualized price for each buyer close to the maximum they would pay for the product. The personal data collected for a particular transaction, when accumulated from all transactions, becomes a valuable business asset that can be sold for use for other purposes. Some business models provide goods or services for free or for less cost by relying on the sale of personal data as a primary revenue stream.

The objective of the drafting committee is to produce a uniform act to regulate the collection, retention, and use of personal data in order to recognize people's interests in the personal data collected and used by companies. In the European Union, the General Data Protection Regulation came into effect in 2018 and provides significant rights for data subjects, including the right to know what data about them was being collected and the purpose for the collection, the right to approve or disapprove of the use of their data, the right to correct inaccurate data, and the right to have the data deleted when no longer necessary for the purpose for which it was originally provided. The GDPR sparked interest in such legislation in the United States, both to benefit consumers and to establish more uniform global rules for handling personal data. California has adopted a comprehensive regulatory regime known as the California Consumer Privacy Act (CCPA) which came into effect in January 2020. An initiative measure is on the California ballot in November that would expand the regulatory structure over use of personal data. Other states have considered similar proposals. No comprehensive statute has been adopted although some specific privacy related measures have been enacted. For example, Illinois has a statute regulating biometric data and Vermont has a statute requiring registration of data brokers. While several proposals have been introduced in Congress, it does not appear that they will be adopted anytime soon.

There are several major sector specific federal data privacy regimes in place, including the Graham-Leach-Bliley Act (financial data), HIPPA (medical data), the Fair Credit Reporting

Act, the Federal Family Educational Rights and Privacy Act (student data) and several others. Similarly, in some states there are more limited privacy regimes applicable to specific industries or activities.

The Committee Process

The project has attracted over 200 observers from a wide variety of technology and other industries interested in data collection as well as from consumer groups. The Committee was able to have one pre-COVID-19 in-person meeting in February which was attended by over 50 observers. Since then we have had several Zoom sessions with active observer participation. We have received numerous thoughtful and detailed position papers from them.

An initial framework draft was refined based on the February discussion and was considered at two meetings conducted remotely. On April 14th, the committee held a 90 minute video meeting, with the primary goal of soliciting observer comments on the revised draft. A day long video meeting was then scheduled for April 24th with the primary objective to obtain committee adoption of a first reading draft for submission to the Conference. Between April 14th and April 23rd we received numerous detailed comments, suggestions, and concerns from a variety of stakeholders. Fortunately, most of these came as specific suggestions for revision of the text of the Act but some urged us to reconsider our basic approach.

In April two members of the drafting committee and a small number of observers presented an alternative draft to the Committee. This alternative draft departed in significant ways from the committee draft. This draft was much less prescriptive, narrowed the scope of the regulatory footprint both in terms of who was regulated and what data was protected, recognized compliance with other similar privacy regimes as sufficient, and incorporated a voluntary consensus process to develop other permissible compliance regimes. It presented a very different framework and philosophy for addressing personal data privacy. **The alternative draft is found on the ULC website under the "2020 August 6 Web Conference" tab.**

The Committee held two meetings in August 2020 to consider which of the competing drafts it was willing to pursue. The first meeting was with observers. While some were attracted to the alternative, others were opposed and preferred the committee draft. A second meeting, with only the committee present, convened a week later. Most thought there were attractive elements of both drafts and that some middle ground seemed appropriate. Obviously, we have not had the opportunity to develop these thoughts.

The first reading draft was presented to Commissioners at an informal session on August 19, 2020, and we received helpful comments. Some style suggestions from that meeting are incorporated in the current draft, but there was not time for the committee to consider substantive suggestions. A note in the comment to each section herein preserves those suggestions for further deliberation. Accordingly, the committee draft is what is before you for this first reading.

The Current Draft

The current "first reading" draft is still very much a work in progress. The Drafting Committee has voted to submit this to the Conference for your comments, but no committee vote has been taken to approve any section or the work as a whole. This draft, like most first reading drafts, is designed to solicit comments from other Commissioners and, importantly, keep this project on schedule for a final reading in the summer of 2021.

During the coming year, the Committee will consider the alternative draft. It raises very significant contrasts of framework and approach to personal data privacy. There is considerable churn within the academic and external constituencies as to which approach is both efficient but still effectively protects legitimate privacy interests. Most current U.S. privacy law presumes that personal data may be freely collected and processed in the absence of any specific law forbidding it, and most such laws are limited to particular narrow industries or types of information (health, financial services, students, etc.). Commercial privacy generally has been governed by a "notice and choice" model under which the further use of a consumer's personal data is often disclosed in terms of service or privacy policies which the consumer seldom reads.

Processing of data can include subsequent disclosures to or uses by third parties for unrelated purposes. In theory, the consumer may "opt out" of these practices by choosing not to use a product or service, thus exercising a weak form of consent when they use services that collect data. This model has come under increasingly strong criticism for failing to offer sufficient protection. European law, seen most recently in the GDPR, begins with the opposite presumption, that individuals have inherent rights in their personal data, and it may be collected and processed only when specifically allowed by law. One of those legally authorized methods is obtaining "opt-in" affirmative consent from a consumer, but this is largely limited to uses connected with the particular purposes for which the personal data was collected in the first place. There have been criticisms of the European model for its inflexibility that does not adequately reflect the realities of the marketplace. In some cases its terms, if applied in the United States, may be inconsistent with the First Amendment. Recent proposals in state legislatures and Congress have tried to chart a middle course between these extremes of contractual consent or personal rights. The Committee will continue to deliberate about the optimal balance.

Even though they begin with opposite presumptions, most existing models end up relying heavily on a form of individual consent. That traditional reliance on consent, particularly but not exclusively in the online world, generally provides little protection for data subjects and little guidance for business enterprises in processing personal data. A third approach might be to focus rather on general standards that should be met when data collectors utilize personal data. Given the diversity of enterprises that collect and process personal data, a standards-based approach might announce some floor of regulatory expectations but require particular industries to adopt codes of conduct or voluntary consensus standards and then to hold them accountable for compliance with those standards. These requirements would apply independently from individual consumers' consent.

The current committee draft moves toward less focus on notice and consent as the basis for privacy protection. The alternative draft provides an even more dramatic departure, emphasizing that uses of data consistent with the expectations of consumers when making the disclosure are impliedly consensual without specific notice where as other, non-compatible uses, must be fully disclosed.

It is likely that any act addressing these issues will blend these perspectives. The committee welcomes your views on this fundamental question. It will be central to the Committee's deliberations in the year ahead.

Significant issues that remain for Committee consideration are noted in the comments to the appropriate sections of the act. We welcome Commissioner comments on these or any other elements.

One final note. In recent weeks we have had a transition in our Reporter. Bill McGeveran provided significant guidance to the Committee during the first year but his obligations as Associate Dean of the Minnesota Law School during the adjustment to the pandemic made it impossible for him to continue. Jane Bambauer of the University of Arizona Law School has agreed to join us as a Reporter and we look forward to having her talent and expertise applied to this project.

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

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

SECTION 2. DEFINITIONS. In this [act]:

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

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

(3) "Deidentified", with respect to information, means lacking capacity to identify, describe, or be associated with a particular individual, if the data processor or data controller does not attempt to restore the capacity of the information to identify, describe, or be associated with the individual and, to prevent others from doing so, implements the following:

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

(B) a business process that specifically prohibits reidentification of the individual; and

(C) a business process that reasonably prevents inadvertent release of the information.

(4) "Device" means a physical object that connects to the Internet.

(5) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

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

(7) “Personal data” means information that identifies or describes a particular individual or can be associated with a particular individual with reasonable effort, whether or not the data has been collected directly from the individual. The term includes a probabilistic inference about the individual, including an inference derived from profiling or information that identifies a household or device if it can be associated with a particular individual with reasonable effort. The term includes a unique identification number, an Internet protocol address, and other data related to a device if the data can be associated with a particular individual by using reasonable effort. The term does not include deidentified data.

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

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

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

(A) a person has a reasonable basis to belief that information is lawfully made available to the general public if the person has taken steps to determine that the information is of the type that is available to the general public and that the data subject who can direct that the information not be made available to the general public has not done so., and

(B) "Widely distributed media" means information that is available to the general public, including information from a telephone book or online directory; a television, Internet, or radio program; the news media; or a Web site that is available to the general public on an unrestricted basis. A Web site is not restricted merely because an internet service provider or a site operator requires a fee or password, so long as either the Web site makes the information available to the general public or the consumer provides access to the information to the general public. .

(11) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(12) "Sensitive data" means:

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

(B) biometric or genetic information; or

(C) personal data about an individual known to be under [13] years of age.

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

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

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

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

(15) "Targeted advertising" means advertising displayed to an individual on the basis of profiling.

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

Need legislative note for paragraphs 12(C) and 14.

Comment

The reach of a data privacy act is driven by the definition of "personal data". This term can be as narrow as information that specifically identifies an individual or as broad as any piece of information without identifying characteristics but when combined with other such information identifies a specific individual. There is also data that starts out identifying an individual but through technological means has been de-identified. This latter category does not identify a person but can generally be re-identified.

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

The alternate draft is limited to data that clearly identifies an individual for privacy purposes but broadens the definition when there is an obligation to keep such data secure. The committee has been encouraged to consider a tiered approach with some data having more protection than others.

The current draft has a category of "sensitive data" which is personal data that has a clear and important link to personal privacy. And it includes data about children. *Informal meeting comment*: It was suggested the Committee think about whether addresses should be included as "sensitive" data for persons subjected to domestic abuse or federal judges.

A broad definition of personal data also must account for data that may be ambiguous as to the individual it identifies. An IP address on a home computer identifies a household but not necessarily the user of the computer at any point in time. The GPS in an automobile or a personal assistant on a cell phone may not identify the driver or user. These issues remain before the committee.

SECTION 3. SCOPE.

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

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

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

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

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

(1) personal health information as defined in the Health Insurance Portability and Accountability Act, Pub. L. 104-191 if the custodian of the information is regulated by that act;

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

(3) publicly available information;

(4) Personal information collected, used, processed or disclosed by a financial institution that processes information to the extent such personal information is subject to the

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

(5) personal information regulated by the Federal Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232 [, as amended];

(6) a state or local government; or

(7) personal data on employees collected or retained by an employer if the data is directly related to the employment relationship.

(c) The [Attorney General] by rule may exempt information or activity from all or a part of this [act] if the collection, processing, transfer, or retention of the information or the activity is regulated by law directed at consumer privacy or data security other than this [act].

(d) This [act] does not apply to the collection, authentication, maintenance, retention, disclosure, sale, processing, communication, or use of personal information necessary to:

(1) initiate or complete a transaction in goods or services which an individual requested;

(2) 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;

(3) assist a person or government agency acting under paragraph (2); or

(4) comply with or defend a legal claim:

(A) setting a requirement, standard, or expectation to limit or prevent corruption, money laundering, or violation of export controls; or

(B) related to an action under paragraph (2).

Need a legislative note for brackets in (a)(1) and (a)(2) and for "as amended."

Comment

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

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

Subsection (a): Limited to larger entities. Limiting the requirements of the act to larger entities is a feature of the GDPR and CCPA enactments. Both acts are highly prescriptive in their requirements and compliance is costly. The committee has deferred direct consideration of whether such an exemption will be necessary until it finalizes the regulatory obligations imposed by the act.

Informal meeting comments: It was observed that this section refers to "commercial activities" whereas the definition of "person" includes non-profits. The committee will need to determine whether non-profits should be included within the scope of this act. It was also observed that controllers may transition over the course of time between below to above the thresholds so that some transition period would be appropriate to permit compliance. Any threshold related to "data subjects" would need to determine if it applies only to subjects within the state.

Subsection (b): Relationship with existing privacy regimes. One of the significant challenges is how to blend the act's requirements with existing privacy regimes. This remains an issue before the Committee. For example, one issue involves the federal Graham-Leach-Bliley Act which regulates financial data collected by financial and other institutions. The current draft exempts personal data already regulated by GLB or any other data activity if the financial

institution voluntarily complies with GLB. The alternative draft would have a broadly worded exemption for covered entities that comply with not inconsistent regulatory regimes.

Employment data. The current draft exempts data collected by an employer about an employee in the context of the employment relationship. It has been argued this is too narrow and should extend to other forms of agency relationships. The alternative draft would apply only to transactions between consumers and the consumer-facing entities and would thus not apply to data derived from non-consumer transactions.

Business-to-business data. It has been urged upon us to exempt all business-to business data from the act. The question is whether a broad exemption may incorporate transactions that contain personal data. We will consider whether a narrower exemption makes sense in this setting. The alternative draft would incorporate this exemption.

Publicly available data. The current draft exempts publicly available data which is broadly defined. It is argued that not to do so would raise serious First Amendment objections. However, data algorithms can take widely diverse and sometimes non- personally identifiable public data to profile an individual on matters that otherwise would be private.

Note: The alternative draft incorporates the concept of "compatible use" which essentially the processing and use of personal data if the use or processing is necessary or expected in order to initiate or complete the transaction out of which the data was voluntarily collected. This concept, if adopted by the committee, may reduce the need for specific exemptions.

SECTION 4. INDIVIDUAL RIGHTS OF INDIVIDUALS GENERALLY. With respect to an individual's personal data, an individual may require a data controller to:

(1) confirm whether the controller has retained or is processing the data;

(2) provide a copy of the data in accordance with Section 5;

(3) correct an inaccuracy in the data retained or processed by the controller; or

(4) subject to Section 3(d), delete the data.

Comment

This section states the primary rights of individuals in their personal data. These are rights common to most data privacy statutes and permit the data subject to some control over their personal data as long as that control does not interfere with the data collectors legal obligations or the purposes for which the data was collected. This section must be read in light of section 11 which requires the data controller to minimize the amount of data collected in relation to the purpose for which it is collected, section 12 which requires that when data is collected, the data subject is informed of the purpose for which the data is to be used, and section 13 which limits the use of data to the purpose disclosed.

Informal meeting comments. The question was raised whether the introductory sentence to this section should read "may".

SECTION 5. INDIVIDUAL RIGHT OF INDIVIDUAL TO COPY OF PERSONAL DATA.

(a) Subject to subsection (b), on request of an individual, a data controller shall:

(1) provide one copy of the individual's personal data to the individual free of charge once every twelve months; and

(2) on payment of a reasonable fee based on actual administrative costs, provide additional copies.

(b) If a request by an individual under subsection (a) is manifestly unreasonable or excessive, a data controller may refuse to act on the request.

(c) If a data controller collects an individual's personal data directly from the individual, the controller, to the extent technically feasible, shall provide a copy of the data to the individual in a way that enables the individual to transmit the copy to another data controller by automated means.

Comment

Informal meeting comments: One commissioner wondered why the data subject could not just as easily keep a copy of the data, but this assumes that the controller doesn't add to or inaccurately transcribe data provided.

SECTION 6. RIGHTS OF INDIVIDUAL RELATED TO TARGETED ADVERTISING AND PROFILING.

(a) An individual may restrict a data controller from processing or transferring the individual's personal data for:

(1) targeted advertising; or

(2) profiling that might result in provision or denial of financial or lending

services, housing, insurance, education enrollment, an employment opportunity, health care services, or access to basic necessities.

(b) A data controller may not process or transfer sensitive data for a purpose under subsection (a) unless the controller receives prior affirmative consent from the individual.

Comment

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

SECTION 7. EXERCISING RIGHTS OF INDIVIDUALS.

(a) An individual may exercise a right under section 4 of this [act] by notifying the data controller by any reasonable means of the individual's intent to exercise the right. A parent or legal guardian of a child under age [18] may exercise a right on behalf of the child.

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

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

Need a legislative note for subsections (a)(age) and (b)(alternative language).

SECTION 8. DATA PRIVACY COMMITMENT.

(a) A data controller that collects, uses, processes, or retains personal data of an individual shall adopt a data privacy commitment and file it with the [Attorney General]. The commitment must be approved by the data privacy officer designated by the controller under Section 15, be in clear language reasonably accessible to an individual, and contain:

(1) the precise procedure by which an individual may notify the controller of the individuals exercise or a right under Section 4;

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

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

(4) the manner in which the controller intends to respond to an individual's request to delete personal data;

(5) the procedure for appealing an initial determination by the controller, including supervision of the appeal by the officer;

(6) the procedure for [filing a complaint] with the [Attorney General]; and

(7) any condition on the exercise of a right under Section 4 which:

(A) is necessary by the nature of the controller's business or industry; and

(B) does not adversely affect the substance of the right.

(b) A data controller that adopts a data privacy commitment under subsection (a) shall

publish the commitment on its website and other places where it will be reasonably accessible to an individual.

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

Legislative notes on [filing a complaint] and [Attorney General] (although the latter may have been done earlier and doesn't need to be repeated.

Comment

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

A significant issue in this and following sections is whether the regulatory provisions should apply to just data controllers or also to data processors and to what extent. The current act limits these obligations to data controllers but requires that these obligations be passed on to data processors by an agreement and enforced by data controllers. (Section 14). Data processors argue that the controllers are the consumer-facing entity and that data processors have no relationship with the data subjects. On the other hand, small retailers who collect data may have little leverage over large data processors to enforce contractual provisions. The issue will be further considered by the Committee.

SECTION 9. DUTY OF LOYALTY OF DATA CONTROLLER AND DATA PROCESSOR.

(a) A data controller or data processor may not engage in processing practices that violate this act or otherwise exposes an individual to an unreasonable and material risk of harm.

(b) The [Attorney General] may adopt rules that identify a processing practice as unfair, deceptive, or abusive.

Comment

Informal meeting comments: It was suggested that use of the term "duty of loyalty" may inadvertently raise a host of fiduciary obligations not intended for this circumstance.

There was also a more general comment that phrasing these requirements in terms of "duty" seemed inappropriate.

SECTION 10. DUTY OF DATA SECURITY OF DATA CONTROLLER AND DATA PROCESSOR. A data controller or data processor shall adopt, implement, and maintain reasonable data security measures to protect the confidentiality and integrity of personal data in the possession or control of the controller or processor. Reasonable data security measures include appropriate administrative, technical, and physical safeguards. Data security measures must be evaluated as part of the data privacy assessment under Section 16. Evaluation of the reasonableness of data security measures must take into consideration the magnitude and likelihood of security risks and potential resulting harm, the resources available to the controller or processor, and industry practices among other similarly situated controllers or processors. Reasonable security practices may be derived from best practices promulgated by a professional organization, government entity, or other specialized source.

Comment

Informal meeting comments: It was suggested we should be clear about whether using "best practices" is a safe harbor from enforcement actions.

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

controller.

SECTION 12. DUTY OF TRANSPARENCY OF DATA CONTROLLER.

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

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

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

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

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

(5) the nature and purpose of profiling an individual using personal data; and

(6) procedures by which an individual may exercise a right under Section 4

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

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

(d) A notice under this section must be reasonably available at the time personal data is collected from an individual.

SECTION 13. DUTY OF PURPOSE LIMITATION OF DATA CONTROLLER. A data controller may not process personal data or permit a data processor or other person to process personal data for a purpose that is not disclosed in a notice to an individual under Section 12.

SECTION 14. DATA PROCESSING BY AGREEMENT.

(a) Processing of personal data by a data processor that is not the data controller must be governed by an agreement in a record between the processor and controller which sets out the nature and purpose of the processing, the type of personal data subject to processing, including identification of any sensitive data, the duration of the processing, and the rights and duties of both parties. The agreement must include the following terms:

(1) The processor shall follow the instructions of the controller regarding the processing of the data and adopt appropriate technological or organizational measures to perform its duties under this [act].

(2) The processor may not process personal data for a purpose other than the purpose of the processing provided in a notice under Section 12 to an individual and for purposes stated in the agreement.

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

(4) The processor may not transfer the personal data to another data processor or other person without the permission of the controller. A transfer to another processor must be

governed by an agreement in a record that imposes the same duties on the recipient of the personal data that are imposed on the processor in the agreement between the controller and the processor, even if the recipient is not subject to this [act].

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

(c) Processing personal data without an agreement that substantially complies with this section is subject to enforcement under Section 19. A data controller that authorizes the processing of information by another without an agreement reasonably consistent with this section is subject to a private cause of action under Section 20.

Need a legislative note for [unfair act and practice] in (c).

Comment

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

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

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

SECTION 15. DATA PRIVACY OFFICER.

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

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

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

(d) If a data privacy officer designated under subsection (a) spends a reasonable amount of time fulfilling the responsibilities under this [act] of data controllers and data processors, the officer may perform other duties for the controller, processor, or other persons. If the officer is not an employee of the controller or processor, the controller or processor and the officer shall execute an agreement in a record which specifies the officer's duties. An individual may serve as an officer for more than one controller or processor.

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

Comment

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

SECTION 16. DATA PRIVACY ASSESSMENT.

(a) A data controller or data processor shall prepare in a record a data privacy assessment of each processing undertaken by the controller or processor

(b) A data controller or data processor shall complete a data privacy assessment about each processing not less than every two years. The controller or processor shall update the assessment when a change in processing may materially affect the risks, harms, or benefits of

processing.

(c) A data privacy assessment must evaluate the:

(1) type of personal data being processed;

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

(3) scale of the processing activity;

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

(5) seriousness of privacy risks and likelihood harm to individuals as a result of the processing;

(6) direct or indirect benefits from the processing;

(7) resources reasonably available to the controller or processor to address privacy risks, taking into account revenue generated by the processing; and

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

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

(1) accidental disclosure or theft of personal data or other breach of security;

(2) identity theft;

(3) harassment;

(4) unwanted profiling;

(5) stigmatization or reputational harm;

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

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

person.

(d) A data processor may fulfill its duties under this section by adopting a data privacy assessment completed by a data controller concerning the same personal data.

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

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

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

Also need a legislative note for [an investigation] in subsection (e).

Comment

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

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

SECTION 17. NONDISCRIMINATION.

(a) Subject to subsection (b), a data controller may require as a condition for access to its

goods or services that an individual permit processing of the consumer's personal data.

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

Comment

Nondiscrimination provisions have been subject to considerable concern. To the extent an individual's interest in privacy is considered a "right", it would follow that the exercise of that right should not result in discrimination. However, there are businesses whose business plan is built on providing goods and services in exchange for access to personal data. As long as this is made clear to individuals, they should not be entitled to the goods or services without being willing to make the exchange. However, this should not implicate their right to access the data held about them or to correct inaccurate data. The section acknowledges here that the right to delete or withhold data cannot be subject to the nondiscrimination mandate.

SECTION 18. WAIVER PROHIBITED.

(a) Except as otherwise provided in subsection (b), an agreement that waives or limits a right or duty under this [act] is contrary to public policy and is unenforceable,

(b) Subsection (a) does not apply to a provision under Section 14(b).

SECTION 19. ENFORCEMENT BY [ATTORNEY GENERAL].

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

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

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

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

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

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

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

(2) giving deference to any voluntary consensus standards adopted by an industry under a process that is fair, open, allows balanced participation by interested parties, including representatives of individuals, and provides an independent appeal procedure.

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

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

Comment

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

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

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

The act also seeks to encourage the adoption and implementation of voluntary consensus standards by industries as long as they are adopted in an open, fair, and balanced process. The criteria are modeled on the Office of Management and Budget Circular a-119 which governs federal administrative agencies. This section represents a tentative move in the direction of voluntary consensus standards. The alternative draft has a more elaborate implementation of such a process which will be considered by the Committee. The focus must be to assure that consumer representatives have a strong voice in development of standards and to protect against

the standard setting process being used to unfairly advantage some firms and disadvantage others.

SECTION 20. PRIVATE CAUSE OF ACTION.

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

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

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

(3) increased risk of subjecting a person to discrimination in violation of any state or federal anti-discrimination law applicable to the covered entity; or

(4) other substantial injury to a person.

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

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

(d) If the court finds the violation of this [act] was a willful or knowing violation or that the refusal to grant relief upon demand was made in bad faith with knowledge or reason to know

that the act or practice complained of violated this [act], the court may award up to three times the actual damages.

(e) In addition, the court shall award such other equitable relief, including an injunction, as it deems to be necessary and proper.

Comment

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

Sections 20 and 21 attempt to respond to both concerns. Section 20 requires the plaintiff not only prove a violation of the Act but also that the defendant acted negligently in the face of the likelihood the violation would cause harm. The plaintiff is limited to recovery of those actual damages the plaintiff can prove. Moreover, the plaintiff must thirty days prior to filing an action make a demand of settlement on the defendant. The defendant has an opportunity to make a reasonable response which may include correction of the violation or a monetary settlement or both. If in the subsequent action a court finds the settlement offer reasonable, the plaintiff's relief is limited to that relief.

It is only upon proof in addition that the violation was willful or knowing violation or the settlement offer was made in bad faith that the plaintiff may recover three times the damage award. Even here, the plaintiff's award is tied to actual damages.

The alternative draft provides an even more narrow authorization for private relief and more elaborate pre-trial procedures to permit firms to correct violations.

Informal meeting comments: Suggestions were offered during the informal meeting which will be considered by the Committee as it continues to deliberate. These suggestions include: (a) consider authorizing a private action on behalf of competitors of the offending firm, (b) authorize interim relief that might end the controversy, including cease and desist orders related to the violation, and (c) consider attorneys fees and costs and how they might be appropriately allocated.

SECTION 21. PRIVATE CAUSE OF ACTION: WILFUL AND REPEATED VIOLATIONS.

(a) A person may bring a private action for damages against a controller or processor that processes the person's personal data as part of a course of conduct that constitutes a willful and repeated violation of this Act, likely to cause the person physical, emotional, or economic harm.

(b) For purposes of this section, "willful and repeated" means the knowing performance of multiple violations over a substantial period of time. A single violation is not performed "repeatedly" merely because it may involve the data of multiple persons.

(c) Damages available to a person under this section are limited to actual damage or [$100], whichever is greater.

Comment

Section 21 provides a private cause of action for willful and repeated violation that are a likely to cause harm. In this circumstance statutory damages are provided if actual damages cannot be shown. The section makes clear that a "repeated" violation does not include one violation that affects multiple parties. Rather it requires multiple violations over a period of time. The attempt of this section is to limit the private cause of action, and the statutory damage provision, to the data broker who purposefully violates the act and uses personal data to cause injury to data subjects.

Informal meeting comments: In subsection (b) it was suggested to change "may" to "might". It was also pointed out that we do not address multiple disclosures about the same person and whether that would fit the "repeated" definition.

SECTION 22. UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

SECTION 23. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT. This [act] modifies, limits, and supersedes the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001, et seq.,

but does not modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

[SECTION 24. SEVERABILITY. If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act] which can be given effect without the invalid provision or application, and to this end the provisions of this [act] are severable.]

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

SECTION 25. EFFECTIVE DATE. This [act] takes effect [180 days after the date of enactment].

Legislative Note: *The effective date depends on the time entities would need to bring themselves into compliance with the Act. To the extent the act requires adjustments in technology and publications, a later effective date is appropriate.*

Comment

Entities in California after enactment of the CCPA had almost two years to achieve compliance before the Act became effective. It may also be true that some sections of the Act might lend themselves to earlier effectiveness. The committee thus is reserving proposing an effective date or dates until it decides on the substantive provisions.