[UNIFORM] PERSONAL DATA PROTECTION AND INFORMATION SYSTEM SECURITY ACT

TABLE OF CONTENTS

[UNIFORM] PERSONAL DATA PROTECTION AND INFORMATION SYSTEM SECURITY ACT

PREFATORY NOTE

A torrent of technological innovation promises to sweep away restraints on individual energy and ingenuity at the same time it threatens to overwhelm the delicate framework of trust within which data about individuals is collected and processed. In order to safeguard that trust in the face of spectacular advances in information technology, a fundamental reevaluation of the rights and obligations of individuals and those who collect and process data about those individuals is needed. That reevaluation requires careful consideration of both the benefits consumers enjoy when technological innovation is channeled into responsible, productive uses and the costs imposed on consumers by inappropriate, careless or even malign uses of technological innovation.

The Uniform Personal Data Protection and Information System Security Act safeguards consumer trust by requiring those who do business with consumers to observe widely accepted principles of fair information and privacy practices (FIPPs), to limit their use and disclosure of consumers' data to purposes that are compatible with the original purposes for which the data was collected and for which consumers have either expressly or impliedly consented. The Act also sets clear rules for how consent must be obtained for non-compatible uses and prohibits uses that exceed the boundaries of consumer consent.

The Act counterbalances technological innovation with governance innovation to create a dynamic framework within which consumer trust can be preserved even in the face of as yet unimagined scientific and technological advances. One of the Act's principal governance innovations is to distinguish between personal data protected by stringent privacy protections and personally identifiable information protected by more flexible security requirements. The Act requires the use of personal data, within structured systems and retrievable using unique identifiers, to comply with the FIPPs. For systems of personally identifiable information, the Act requires appropriate security protections and privacy risks assessments.

By calibrating the level of privacy protection required with the risk of harm to the consumer whose personal information is being used, this distinction between different categories of information about consumers moderates compliance costs for business while increasing privacy protections for consumers. The distinction also harmonizes the Constitutional protections accorded to the free exchange of publicly available information under the First Amendment with the need to maintain trust between consumers and businesses that collect personal data from and have a relationship with them. Furthermore, the Act incorporates these new privacy protections into the existing well-understood state and federal system of consumer protection, which the Act harmonizes seamlessly with the existing federal and state system of sectoral privacy laws.

The Act, therefore, restores trust by requiring businesses to observe widely accepted fair information practice principles (FIPPs) and by imposing appropriate security projections, ensuring that

businesses will have sustainable access to the information they need to compete and innovate successfully.

The essential features of the Act. The essential features of the Act are:

(1) the Act does not seek to regulate all information available to businesses about consumers, regardless of how it is obtained, but to protect personal data collected from a consumer by an entity in a relationship with a covered entity by requiring the consumer's consent to the use of the personal data so provided;

(2) the Act reasonably permits businesses to use the personal data provided by consumers for uses, other than the original use, as long as that use is compatible with the original purposes for which the personal data was provided;

(3) the Act also permits businesses to use the personal data provided by the consumer for non-compatible uses, if and only if, the business gives the consumer sufficient notice and information about the non-compatible use and the consumer has the opportunity to withhold consent;

(4) the Act extends additional protections to the use of sensitive personal data and prohibits the misuse of personal data to cause a consumer harm;

(5) the Act requires businesses to give consumers information about any personal data they collected from a consumer and how they can access and correct the personal data, unless it is publicly available information;

(6) the Act requires that businesses must have appropriate safeguards to protect all of the information they have about consumers;

(7) the Act provides for a robust safe harbor for voluntary consensus standards, recognized by the state's Attorney General, which apply privacy protections and information system security requirements appropriately to defined sectors and in specific contexts; and

(8) the Act is enforced by the Attorney General though state consumer protection laws, a familiar and well-understood protection of consumers from deceptive and unfair business practices.

Seven fundamental governance innovations in the Act. The Act avoids problems that have bedeviled other legal privacy frameworks through seven governance innovations:

(1) by regulating only data collected from a consumer in connection with a relationship with a covered entity;

(2) by explicitly excluding publicly available information from the FIPP provisions;

(3) by distinguishing between personal data, to which privacy protections apply, and systems of personal identifiable information, to which information security and privacy risk assessment requirements apply;

(4) by implying consumer consent for uses compatible with the original use;

(5) by creating a safe harbor for voluntary consensus standards for tailoring the Acts requirements appropriately for defined sectors and in specific contexts;

(6) by enforcing the Act through the state's consumer protection laws; and

(7) by deeming businesses in compliance with substantially-similar state, federal and international privacy laws and international privacy frameworks to be in compliance with the Act.

First, personal data provided by a consumer in the context of a relationship between the consumer and covered entity. The Act defines a "covered entity" as "a person that *collects personal data from a consumer, in connection with a relationship with the consumer*."

These two requirements, that the business collect the personal data from the consumer and in connection with a relationship with the consumer, operate together to limit the scope of the Act to a constitutionally defensible and manageable level.

The Act distinguishes between personal data *provided by the consumer to the business*, and any other personal data lawfully available to the business about the consumer, some of which is publicly available. Personal data provided by the consumer to the business enjoys the protection of the Act's provisions implementing FIPPs. In this way, the Act is in accord with the legitimate privacy concerns of a reasonable consumer. A reasonable consumer has a legitimate interest in the privacy of personal data *provided to a business by the consumer*. The Act protects this privacy interest by insuring that the consumer consents to the use, and that the consumer may refuse to permit any non-compatible use, after receiving sufficient prior notice and information. The Act protects a reasonable consumer's expectation that sensitive personal data will receive special privacy protections and that personal data will not misused to harm the consumer.

Furthermore, regulating collecting personal data from a consumer *in the context of a relationship between a consumer and a covered entity* recognizes an implied contract between them to use the consumer's personal data in accordance with the consumer's consent and protects the legitimate government interest in insuring that businesses do not exploit their relationship with consumers. Government regulation of information provided in the context of a relationship has received broad constitutional latitude. *See, e.g., Snepp v. United States*, 444 U.S. 507 (1980) (agreement to submit writings to pre-publication review allowed for prior judicial restraint preventing publication); *Cohen v. Cowles Media Co.*, 501 U.S. 663 (1991) (upholding liability against journalist who breached confidential relationship with a source). Thus, basing the Act's privacy protections on personal data provided by the consumer to the business and on the relationship between the consumer and the business places the Act's constitutionality on firm ground.

Laws like the EU's General Data Protection Regulation ["GDPR"] and the California Consumer Privacy Act ["CCPA"], that purport to regulate all personal information generally, however, are often constitutionally infirm. The reason is that publicly available information enjoys First Amendment protection, *see, e.g., Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011) ("the creation and dissemination of information [is] speech within the meaning of the First Amendment."), and a

restriction on speech cannot be justified "by merely asserting a broad interest in privacy." *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999). "Privacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it." *Id.* As a result, courts have struck down, on First Amendment grounds, laws limiting disclosure of even highly personal data, such as the names of rape victims, judges and juveniles involved in legal proceedings, legislators' names, home addresses, and phone numbers, realtors' home phone numbers, and an individual's social security number, when the data is publicly available and related to matters of public concern.

Finally, these limitations insure that the cost to businesses of compliance is reasonable and reduce the resources needed by the government to enforce it. Laws like the GDPR and the CCPA, however, result in unreasonably high compliance costs for businesses and require massive resources for government agencies to enforce.

Second, excludes publicly available information from FIPP provisions. The Act also limits the scope of the Act by explicitly excluding solely publicly available information from regulation by the FIPP provisions which require businesses to allow consumers to access and correct personal data and from the prohibited uses provision. A collection of publicly available information about a consumer, however, is protected by the Act's information system security requirements.

As explained above, publicly available information is protected by the First Amendment and consumers do not have a legitimate privacy interest in publicly available information. Thus, applying the FIPP provisions or the prohibited use provision to publicly available information would be unconstitutional.

Third, distinguishes between personal data and personally identifiable information. The Act distinguishes between personal data and personally identifiable information for purpose of regulation. **"Personal data"** means data about a consumer, such as financial activity, medical history, employment, or other personal attributes, and which contains the consumer's identifier. "Identifier" means any information that is routinely used to retrieve data about a particular consumer, such as the consumer's name, physical address, email address or Social Security number.

Personal data, if provided to the business by the consumer in a relationship with a business, is protected by the Act's provisions implementing FIPPs. The Act requires consent for the use by the business of such personal data, which includes compatible uses, requires notice, information, and an opportunity to withhold consent for any proposed non-compatible use, and requires affirmative consent for every use of sensitive personal data. In addition, a business must inform customers of the business' procedures for how the consumer can access and correct the customer's personal data, and for how the consumer can hold the business accountable for, and redress, any harm caused by the unauthorized use or disclosure of the personal data. Furthermore, the business must inform customers of the categories of personal data maintained by the business, the sources of personal data, each compatible use made of personal data, each non-compatible use proposed to be made of personal data and any required notice and information about the proposed non-compatible use, including the opportunity to withhold consent to a non-compatible use.

In applying FIPPs to only personal data, and not to all other information about a consumer, the Act appropriately limits the scope of regulation to only data likely to be used to make decisions about

the consumer, recognizes the mutual interest of businesses and consumers in sustaining a relationship of trust that arises from appropriate use of the personal data and accurate decisionmaking, and avoids the intractable problems associated with trying to apply FIPPs to all information about a consumer.

"Personally identifiable information," however, is much broader and includes information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a particular individual, including personal data and publicly available information.

Here, too, consumers and businesses have a mutual interest in making sure that the maintenance and storage of personally identifiable information is protected from theft and use or misuse by third parties, so the Act requires security protections and risk assessments for such information systems.

Fourth, compatible use. The Act implies customers consent to any compatible use. Compatible use is the processing of personal data that is sufficiently related to the original purpose for which the personal data was collected that it is reasonable to imply a consumer's consent to the processing. The Act establishes factors to consider to determine if other uses are considered compatible, including the context of the consumer's relationship with the covered entity, the type of transaction in which the personal data was collected, the type and nature of the personal data which was collected, and the risk of any negative consequences of the proposed use or disclosure of the personal data on the consumer. The Act also establishes that certain uses of personal data collected from the consumer is compatible, including effectuating a transaction with a consumer with the consumer's knowledge or participation and compliance with legal obligations of the covered entity.

The Act's implied consent for compatible uses of the personal data the customer provided the business is a reasonable accommodation that balances the legitimate privacy interests of the consumer with rapid technological development and innovation. At the time the customer provides personal data to a business and consents to its use, future development of compatible uses is unknown. Some privacy laws required consent for each future use, when it is reasonable in some cases to assume that the customer would consent if the new use is sufficiently related to the original purpose for which the personal data was collected. Requiring consent for each future compatible use unnecessarily stifles innovation and substantially increases cost with no net benefit to the customer. However, if a future use is non-compatible, then the Act requires the customer's consent.

Fifth, robust safe harbor for voluntary consensus standards. 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.

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.

Sixth, enforcement through consumer protection laws. The Act is enforced through a state's consumer protection laws, which is a familiar and well-understood protection of consumers from deceptive and unfair business practices. These consumer protection laws provide for enforcement by the state's Attorneys General and, in some states, by a private cause of action.

By utilizing a state's consumer protection law as the enforcement mechanism for the Act, the Act is integrated into a well-established state enforcement regime with existing enforcement personnel, established procedures, and well-developed legal standards. This ensures effective enforcement and reduces novel questions and unexpected legal developments.

Seventh, interoperability. The Act avoids unnecessary conflicts with existing state and federal laws, in principle, by linking its enforcement to the state consumer protection framework. But the Act goes farther by providing that, if the requirements of the Act are inconsistent with any federal or state laws that currently regulate specific sectors, the Act is not applicable in that instance. The Act also requires that voluntary consensus standards reasonably reconcile the Act with other applicable federal and state laws. Finally, the Act deems businesses in compliance with the requirements of the Act, if they are in compliance with other general privacy and/or information system security laws, such as the GDPR and the CCPA, as well as international privacy frameworks, such as the voluntary Cross-Border Privacy Rules system of the Asian Pacific Economic Cooperation Region of 27 countries and the US-EU Privacy Shield framework, and other similar laws or frameworks.

These interoperability provisions of the Act with existing state, federal and international privacy laws and international frameworks substantially reduces the compliance cost to covered entities already in compliance with sector or context specific laws, general privacy laws enacted in other states or internationally, or international privacy frameworks.

Conclusion, a new and innovative approach to privacy protection. The flexibility of the Act allows it to protect consumer privacy in ways fundamentally different from the rigid, top-down bureaucratic approach that characterizes the GDPR and the CCPA and, as a result, the Act is more likely to achieve higher compliance at a reduced cost.

The result is a legislative framework that represents a new and innovative approach to privacy

law that is flexible enough to accommodate the rapid pace of technological innovation and that is strong enough to ensure that competition and innovation do not come at the expense of misuse or abuse of personal data or exposure of information systems to exfiltration or theft.

[UNIFORM] PERSONAL DATA PROTECTION AND INFORMATION SYSTEM SECURITY ACT

SECTION 1. SHORT TITLE. This [act] may be cited as the [Uniform] Personal Data Protection and Information System Security Act.

SECTION 2. DEFINITIONS. In this [act]:

(1) “Compatible use” means the processing of personal data in a manner that is sufficiently related to the original purpose for which the personal data was collected that it is reasonable to imply a consumer’s consent to the processing. To the extent that a third party has an indirect relationship with a consumer, because of a relationship with a covered entity allowing the third party access to personal data collected from the consumer, the third party is a covered entity, whether or not the consumer is aware of the relationship.

(2) "Consumer" means an individual who through commerce seeks or acquires any goods, services, including a digital services, money, or credit for a personal, family, or household purpose.

(3) “Covered entity” means a person that:

(A) collects personal data from a consumer, in connection with a relationship with the consumer;

(B) collects personal data on the behalf of a person under subparagraph (A); and

(C) alone, or jointly with others, determines the purposes for the collection of the personal data.

(4) “Digital services” means information technology that, in the context of individual personal use, person to person communications, or multiparty interactive forums, provides consumers capacities to search, blog, podcast, or otherwise interact with individuals, sellers of goods and services, or content providers, whether or not the consumer is charged for the service.

(5) “Disclosure,” with respect to personal data, means to release, transfer, provide access to, or

divulge the data to a person not employed by the covered entity. “Disclose” has a comparable meaning.

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

(7) “Government unit” means a public corporation or government, or government subdivision, agency or instrumentality.

(8) “Identifier” means information routinely used to retrieve data about a consumer, including, but not limited to:

(A) a first and last name;

(B) a home or other physical address, including the name of the street or municipality;

(C) an electronic mail address;

(D) a Social Security number, telephone number, account or license number, or other data assigned to a consumer or a consumer’s electronic device;

(E) an Internet protocol address; or

(F) data linked to a particular browser or device in the possession of a consumer, if used to identify personal data of the consumer.

(9) “Information system” means a collection or grouping of personally identifiable information, which is under the custody, care, or control of a covered entity, and in which personally identifiable information is maintained or stored.

(10) “Materially” means to a substantial or significant extent or degree.

(11) “Person” means an individual, estate, trust, partnership, business or nonprofit entity, or other legal entity. The term does not include a government unit.

(12) “Personal data” means any item, collection, or grouping of data about a consumer,

including, but not limited to, education, financial activity, medical history, employment, or other personal attributes, and which contains an identifier of the consumer.

(13) "Personally identifiable information" means information, including personal data or publicly available information, regardless from whom it is collected, that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to the individual.

(14) "Process," with respect to personal data, means the collection, use, disclosure, maintenance, storage, erasure, analysis, or modification of personal data, or the use or disclosure of personal data to generate a new form of personal data. "Processing" has a corresponding meaning.

(15) "Publicly available information" means information lawfully made available to the public from federal, state, or local government records, or from generally accessible and widely-distributed media.

(16) "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.

(17) "Sensitive personal data" means personal data that contains a consumer's date and place of birth, mother's maiden name, racial or ethnic origin, a government-issued identification number, including a social security number or a driver's license number, insurance plan numbers, financial account numbers, past, present or future medical condition or treatment, genetic data, unique biometric data, precise geolocation data, or other similar personal data.

(18) "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.

(19) "Stakeholder" means a person with a demonstrated interest in, or a person or governmental unit that is materially affected by, the outcome of the voluntary consensus standard setting process.

(20) "System of personal data" means a collection or grouping of personal data, or personal data coupled with any other information:

(A) under the custody, care, or control of a covered entity; and

(B) from which, as part of the routine activities of the entity, personal data is retrieved by means of an identifier.

(C) The term does not include a collection or grouping of personal data consisting solely of publicly available information, or information derived exclusively from publicly available information, which was not provided to the covered entity by the consumer.

(21) "Use," with respect to personal data, means the employment, application, examination, or sharing of personal data among the workforce of a covered entity and its affiliates.

(22) "Voluntary consensus standard" means a standard developed by a voluntary consensus standards body.

Comment

Section 2(1) Compatible Use—When a business collects personal data from a consumer for the purposes of commercial transaction, a relationship arises based on their mutuality of interests, in which there is an understanding, an implied contract, that the business will limit the use of the personal data to purposes that are *compatible* with the purpose for which the data was originally collected. This mutuality of interests limits ethical information practices to *only compatible uses* of a consumer's personal data and is the core idea of the Fair Information Practice Principles, which is the basis of all commercial information privacy laws.[1]

[1] *Records, Computer and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, U.S. Department of Health, Education and Welfare (July, 1973) ("HEW Report"). In rejecting the concept of privacy as individual control of personal information, the HEW Report noted that:

The definition of the term "*compatible use*" is derived from Section 552a(a)(7) of the Privacy Act of 1974, which, regarding disclosures, is defined as "the use of such record for a purpose which is *compatible* with the purpose for which it was collected." The idea of a compatible use also plays a central role in the GDPR, where Article 6(4) provides that processing of personal data is not based on the data subject's consent if it is not "compatible with the purpose for which the personal data have been collected."

The close relationship between compatibility and consent in the GDPR makes clear that whether a use or disclosure of personal data is or is not compatible is equivalent to the question whether the use or disclosure is one for which an individual's consent can reasonably be implied. *Implied consent*, of course, is not a function of the subjective intent of any individual. As noted by Section 5(I) of the American Law Institute's Principles of Law, Data Protection, the express [subjective] consent of an individual is not required for the use or disclosure of personal data in a way that is *compatible* with the purposes for which it was originally collected. Compatibility is thus related to the *objective concept of consent*—when consent can be reasonably implied for the use or disclosure of personal data given the original purpose and the nature and context of the relationship. This objective notion of consent reflects normative social understandings about the mutuality of interests between the consumer and the business, as well as other controlling legal obligations and social norms.

By tying the concept of *compatibility* to (objective) reasonably implied consent, the Act can then establish meaningful individual (subjective) consent requirements for the exceptional cases—the *non-compatible uses*. While the GDPR recognizes the relationship of consent to compatibility, it fails to distinguish between the subjective and objective concepts of consent. The confusion of these concepts, together with threats of punishment by government authorities, transforms the natural relationship of mutual trust between the consumer and the business into an adversarial relationship. Businesses assume a defensive posture with consumers and try to document individual consent for everything, turning consent into a meaningless "checkbox" ritual. This Act restores trust, by allowing the notion of compatibility to reflect the mutual interests of individuals with organizations processing data about them, resulting in a reasonable and appropriate use of that personal data by covered entities, consistent with law.

Section 2(2) Consumer—The definition of consumer is based on the standard definition

---

> Records of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals. In fact, it would be inconsistent with this essential characteristic of mutuality to assign the individual record subject a unilateral role in making decisions about the nature and use of his [or her] record. . . . Similarly, it would be equally out of keeping with the mutuality of record-generating relationships to assign the institution a unilateral role in making decisions about the content and use of its records about individuals.

Id at 40.

of the term used in most consumer protection statutes, with the addition of the term "digital services.". The term "digital services" is defined in Section 2(4).

Section 2(3) Covered Entity—The definition of a covered entity ensures that the Act regulates personal data *collected from a consumer* in the context of a *relationship between* a consumer and a covered entity. To the extent that a third-party has an indirect relationship with a consumer, because of a relationship with a covered entity allowing the third-party access to personal data about the consumer, the third party is a covered entity, whether or not the consumer is aware of the relationship.

The close tie to a relationship between a consumer and a business relates back to the mutual relationship of trust between the covered entity and consumer that is the guiding principle underlying the Act as a whole. Keeping the Act closely tied to the relationship between consumer and covered entity keeps the scope of the Act within appropriate limits, the cost to business of compliance reasonable, and the resources needed by the government to enforce it realistic. Laws like the GDPR and the CCPA that purport to regulate personal information directly, outside of the context of a relationship, result in unreasonably high compliance costs for business, and the need for massive resources by government agencies to enforce.

Furthermore, In the United States, universal data protection frameworks that regulate information directly, risk trenching on First Amendment freedoms. *See, e.g.*, S*orrell v. IMS Health Inc*., 564 U.S. 552, 570 (2011) ("the creation and dissemination of [private] information is speech for First Amendment purposes. . . . the State may not infringe these rights to protect a generalized interest in consumer privacy.") By contrast, government regulation of personal information in the context of a relationship receives broad constitutional latitude by the Supreme Court. *See, e.g., Snepp v. United States*, 444 U.S. 507 (1980) (agreement to submit writings to pre-publication review allowed for prior judicial restraint preventing publication); *Cohen v. Cowles Media C*o., 501 U.S. 663 (1991) (upholding under rational basis test finding of liability against journalist who breached confidential relationship with a source).

Section 2(4) Digital services—Digital services are included in the definition of consumer to clarify that a consumer includes an individual seeking digital services.

Section 2(8) Identifier— The use of the term "identifier" is borrowed from language of computer science, where it is used to denote a term that identifies *a person* or *thing*. Linking an *identifier* to information about a person is essential if the principles of fair information practices are to be administrable within a system of FIPPs based on privacy rights, because these privacy rights were originally designed to apply only within a pre-existing nexus in which an identifier is used to retrieve information about a person in a structured database, usually to make decisions about the person, triggering intuitions of fairness and due process.

The Privacy Act of 1974 captures the idea of an identifier by using term "identifying particular" in its definition of "record" at 5 U.S.C. 552a(a)(4). Because this phrase is awkward and has let to confusion by the court decisions that have interpreted it, the Act adopts the term "identifier" to denote terms directly identify a unique individual. For example, the term "Barack Obama" is an identifier. Descriptions using more general attributes, such as "former President of

the United States," "former Senator of Illinois," "former president of the Harvard Law Review," or "married to his law school classmate," may be used to refer to a unique person, but only when additional context is implicitly understood. That said, the concept of an identifier is a functional one to denote any means in which personal data routinely and regularly retrieved to make decisions about the person to whom the data pertains. For example, numerical data used to identify a particular device in the possession of a consumer may be an identifier if it is regularly used to retrieve personal data about a particular consumer in a system of personal data.

Section 2(9) Information System—An "information system" is composed of computers and people that process information. This concept in the Act is based on Section 208 of the E-Government Act, and the Federal Information Security Management Act, both enacted in 2002. Section 208 of the E-Government Act requires privacy impact assessments, focusing on risks to individual privacy, but the risks are evaluated at the overall system level in the same way that the information security provisions of the FISMA and its requirements for notification of breaches also focus on risks not to particular individuals, but to individuals generally as part of the overall management of the information system. Because risks at the system level are not limited to personal data alone – that is information tied to specific identifiers – Section 208 of the E-Government Act and the FISMA use the extremely broad concept of "individually identifiable information." As discussed in the Comments to Section 2(13), Personally Identifiable Information, it is important to avoid conflating the concept of personal data with the concept of personally identifiable information—that is, confusing protecting individual privacy by implementing fair information practice principles, with the controls designed to protect against security risks to an entire information system.

Federal laws that apply to information systems used by the U.S. government carefully distinguish between these difference concepts and, as a result, establish a workable framework within which the privacy interest of individuals in their personal data can be harmonized with the other essential functions of government. Congress recognized, when it enacted the Privacy Act, that it needed to protect individual privacy rights and to establish protections around the nexus of retrievably of records in a system of records. Congress did not attempt to expand the scope of a "record" in the Privacy Act, when it enacted the E-Government Act and the FISMA in 2002, because it recognized implementing a set of privacy protections based on fair information practices using the broad definition of personally identifiable information would create unnecessary confusion and provide little by way of additional privacy protection to individuals. Since 2002, the federal government has operated with two different concepts of personal information: records within systems governed by the Privacy Act, and personally identifiable information within systems governed by the E-Government Act and the FISMA.

Section 2(12) Personal Data— The term "personal data" constitutes the first of the two central privacy concepts in the Act, the other concept being "personally identifiable information." These two terms serve entirely different functions and must not be confused with each other.

The term "personal data" corresponds closely to the term "record" in Section 552a(a)(4) in the Privacy Act of 1974. A "record," in the Privacy Act, must contain information about an individual, as well as a name or other identifying particular. S*ee e.g., Tobey v. N.L.R.B.*, 40 F.3d

469, 471 (D.C. Cir. 1994). In a similar way, personal data in the Act consists of two elements, 1) descriptive information about a consumer, and 2) an "identifier" identifying that consumer which is used to retrieve the desired information. For example, the sentence "Barack Obama is a former President of the United States" constitutes personal data because it combines an identifier (here a personal name) with information about the person identified with that name.

The Act applies FIPPs to *personal data* in systems of personal data. The Act uses a very different concept for the information security and privacy risk assessment requirements for information systems—the much broader concept of *personally identifiable information*, which is discussed below. Personal data is a privacy-rights-based concept, personally identifiable information is a risk-based concept. The two should not be confused with each other.

By using two different definitions of the personal information for two different privacy-related purposes, the Act avoids the intractable problems that characterize other privacy laws like the GDPR and CCPA, which mistakenly try to apply the FIPPs to the broadest possible concept of personally identifiable information. While this broad concept is entirely appropriate for risk management, but it leads to needless confusion, and likely unconstitutionality, when one tries to use it to administer a system of protecting individual privacy rights. For this purpose, a more functional definition like the Act's term *personal data* (or the Privacy Act definition of the term "record") is needed. This concept more closely corresponds to how organizations actually use data to make decisions about people and aligns the obligations in the Act to the actual way businesses use information.

Section 2(13) Personally identifiable Information— The term "personally identifiable information" constitutes the second important privacy concept in the Act. Personally identifiable information or PII means information that can be used to describe an individual, either alone or in combination with other information. The Act uses the term "personally identifiable information" to set out the requirements imposed on covered entities to address security risks in systems of personally identifiable information. By contrast, as noted above, the term "personal data" is used for imposing FIPPs.

The two definition privacy framework of the Act, where different information privacy concepts perform different functions, is based on the dual-definition privacy framework used by the federal government, which uses the term "record" in a system of records, when applying privacy protections based on the FIPPs under the Privacy Act, and which uses the term "personally identifiable information," when managing information security and privacy risks in connection with information systems under Section 208 of the E-Government Act and the Federal Information Security Management Act. *See, e.g.*, NIST SP-800-122 (Guide to Protecting the Confidentiality of Personally Identifiable Information); OMB Circular M-07-16 (Safeguarding Against and Responding to the Breach of Personally Identifiable Information); OMB M-03-22 (Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002).

Section 2(17) Sensitive personal data—For processing of sensitive personal data for a non-compatible use, the Act requires the consumer's consent for each non-compatible use.

Section 2(20) System of personal data—As noted above, the Act defines two different kinds of systems: a "system of personal data" and an "information system." The [Act] uses a system of personal data when it applies the FIPPs to personal data. A system of personal data is characterized by a system of structured data in which personal data is regularly *retrieved* by means of an identifier. A system of personal data thus requires there to be three elements: 1) personal data, 2) an identifier, and 3) a system of personal data in which the identifier is used to retrieve the personal data (or a nexus of retrievability). The result is an appropriate framework for a regulatory structure designed to focus on the concerns of particular individuals.

This framework is based on the framework established by the Privacy Act of 1974, which applies FIPPs to "records" in "systems of records," where a record consists of an "identifiable particular + personal information" and a "system of records," where an identifiable particular is used on a regular basis to retrieve a "record." As noted, this functional definition allows for a more bounded scope when applying the FIPPs. By contrast, the GDPR's and the CCPA's attempt to apply FIPPs using a broad privacy concept of personally identifiable information, designed for purposes of security and risk management, results in a regime that is extremely costly for businesses to implement and expensive for government agencies to enforce, with little, if any, benefit in additional privacy protections enjoyed by consumers.

SECTION 3. SCOPE.

(a) This [act] applies to a covered entity that collects personal data from at least [] consumers annually in this state, maintains a system of personal data with at least [] consumers in this state, or maintains an information system with at least [] consumers in this state.

(b) A requirement of this [Act] does not apply to a covered entity if:

(1) the requirement is inconsistent with, or is preempted by, a federal law; or

(2) the requirement is inconsistent with a requirement of the another law of this state applicable to the entity.

(c) This Act does not apply to the use or disclosure of personal data for journalistic, academic, artistic, literary, political or religious expression.

Comment

Section 3(a) establishes the minimum requirements for the application of the Act. This exempts small entities and established the minimum contacts necessary to impose the Act on out-of-state businesses.

Section 3(b) exempts from the scope of the Act existing federal and state laws that are inconsistent with a requirement of the Act.

As noted above, the reconciliation of a universal privacy framework, such as this Act, with the complex and diverse existing system of federal and state sectoral privacy laws, can pose intractable problems for privacy statutes like the CCPA, which attempt to regulate all information directly. Although the Act avoids such problems in principle by linking its requirements to the federal and state consumer protection framework, the Act also addresses this problem successfully in four other ways: first by providing in Section 2(b) that the Act does not apply if there is an inconsistent federal or other state laws, second by providing in Section 12(b) that a voluntary consensus standard must reconcile this Act with the requirements of other applicable federal and state laws, third, by providing in Section 13 that, for recognition, the Attorney General must find that the voluntary consensus standard reasonably reconciled this Act with other federal and state laws, and fourth, by providing also in Section 13 that a covered entity may comply with a substantially similar law and be in compliance with this Act.

Section 3(c) exempt from the scope of the Act non-commercial activities protected by the First Amendment.

SECTION 4. PROTECTIONS FOR PERSONAL DATA.

(a) A covered entity may not process a consumer's personal data, collected from that consumer, without a signed request in a record by the consumer, or a prior consent in a record from the consumer, unless the processing is for a compatible use.

(b) A covered entity that maintains a system of personal data shall, with respect to the system of personal data:

(1) establish a reasonable procedure to notify a consumer, at the consumer's request, whether the system contains the consumer's personal data, and how a consumer can request a copy of the data.

(2) establish a reasonable procedure for a consumer to access, if necessary, and to correct the accuracy of a consumer's personal data, when it may be used to make decisions materially affecting a legitimate interest of the consumer;

(3) establish a reasonable procedure to establish accountability for, and to redress, any harm caused by the covered entity's unauthorized use or disclosure of a consumer's personal data; and

(4) make transparent to a reasonable consumer, by publication on an Internet web-site

or similar means:

(A) the name and location of the system;

(B) the title and business address of the individual or office of the covered entity responsible for the system of personal data.

(C) the categories of personal data maintained in the system;

(D) the sources of personal data in the system.

(E) each compatible use, if any, made of personal data in the system;

(F) each non-compatible use, if any, made of personal data in the system and the required notice and information about the non-compatible use, including a reasonable opportunity to withhold consent to a non-compatible use;

(G) the policies and practices of the entity regarding storage, retrievability, access controls, retention, and disposal of personal data in the system; and

(H) the state, federal or international privacy laws or international privacy frameworks, state or federal sector-specific privacy laws and recognized voluntary consensus standards the entity is in compliance with.

Comment

Section 4(a) establishes a general requirement of express written consent for processing of personal data and that consent includes compatible uses. This section is based on Section 552a(b) of the Privacy Act of 1974, as well as the HIPAA regulations. The Privacy Act establishes a framework where agencies are not required to obtain individualized consent for routine uses that are compatible. Under the HIPAA regulations, covered entities are not required to obtain consent for disclosures of patient medical information for treatment, payment, oversight, operations, and other specific exceptions, but must obtain express written consent for any non-compatible disclosure. This is also the recommended approach of the American Law Institute's Principles of Law, Data Protection.

Thus, under the Act, the processing of personal data is constrained by the concept of "compatibility," which appropriately bounds behavior. Under this framework, uses and disclosures that are compatible with the purpose for which personal data was originally collected do not need

individualized consent. The concept of "compatibility" allows for the appropriate use of personal data by the covered entity to carry out a variety of different missions, without transgressing what the concept of reasonably implied consent encompasses. The Act uses the term "compatible use," instead of the term "routine use" that is found in the Privacy Act, because certain disclosures may be infrequent or unusual, yet still be compatible with the purposes for which the data was originally collected. As noted previously, the concept of *compatibility* is a closely related to the concept of *implied consent*. The question whether a use or disclosure is or is not compatible—that is, a disclosure for which one could reasonably imply consent—is ultimately an objective question reflecting society's judgment about appropriate and inappropriate secondary uses, not one that turns on an individual's subjective mental state.

By making express written consent a requirement for a non-compatible use, where implied consent would be inappropriate, the Act provides the consumer with the power needed to exercise appropriate control over the consumer's personal data. As a result, absent express consent the incompatible use cannot lawfully take place. Implying that consent for compatible uses was within express consent avoids the unnecessary danger of overusing the concept of consent, which occurs when privacy laws require some form of consent (either opt-in or opt-out) for both compatible and incompatible uses, which reduces consent to a "check-box" ritual leaving consumers with little or no real choice as a practical matter. More meaningful and effective consumer protection is provided when a compatible use does not require an additional express consent by consumer, and the concept of consent is reserved for those contexts where there can be meaningful consent on the part of a consumer. While the concept of compatibility provides higher levels of protection for consumers, it also gives legitimate businesses a straightforward and flexible structure that allows them to adjust their compatible uses in line with the needs of different industry sectors, as well as accommodate unforeseen future developments in technology or the business environment. It balances privacy, the need for business innovation, and the appropriate use of personal data.

Section 4(b) requires covered entities to implement the FIPPs rights of access and correction, to establish redress procedures, and to implement transparency for systems of personal data. Covered entities are required to spell out explicitly their determination of what is and is not a compatible use in their notice of privacy practices so that the judgments implicit in the compatibility determination can be made transparent and inappropriate determinations of compatibility can be challenged. This provision also establishes transparency and accountability requirements through an administrative process for covered entities, requiring them to make their *compatible uses* and *non-compatible uses* transparent by publishing them in their notice of privacy practices. At the same time, this requirement provides covered entities with the flexibility they need to handle personal data appropriately by providing a framework for "good actors" to improve their transparency by communicating to consumers their compatible uses and disclosures of personal data.

SECTION 5. COMPATIBLE USE OF PERSONAL DATA.

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

(1) the context of the consumer's relationship with the covered entity;

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

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

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

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

(b) A compatible use for processing of personal data includes:

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

(2) compliance with legal obligations of the covered entity;

(3) meeting a managerial, personnel, administrative and operational need or other legitimate interest of the entity; and

(4) permitting appropriate internal oversight of the entity or external oversight by a government unit.

(c) A covered entity may use or disclosure a consumer's personal data:

(1) to an officer or employee of the entity who have a need for the data in the performance of the officer's or employee's duties;

(2) to a government unit responsible for regulation of the covered entity, or civil or criminal law enforcement, for an authorized purpose of a government unit;

(3) to a government unit for an authorized governmental purpose if the disclosure is permitted by law.

(4) under the order or rules of a court; or

(5) for a purpose otherwise permitted or required by law.

Comment

Section 5(a) consists of the factors to use in determining whether any particular form of processing of personal data constitutes a compatible use.

Section 5(b) contains a non-exclusive list of purposes for processing of personal data that are considered compatible uses.

Section 5(c) consists of a non-exclusive list of types of uses or disclosures of personal data that are considered compatible uses.

These general factors, purposes and types of uses create a framework for deciding whether a particular processing of personal data will be compatible. However, opinions about compatibility often diverge and whether a use is compatible can be different for defined sectors and in specific contexts. Accordingly, the Act establishes an analytical framework for decision and does not give one party or the other control over the determination.

However, the Act contemplates that much of the work of determining the application of these requirements for defined sectors and in specific contexts, and with the desired specificity, will be established through recognized voluntary consensus standards pursuant to Sections 8 through 13 of the Act, through a consensus process where disagreements about the question of compatibility will be reconciled in a voluntary consensus standard setting process. The voluntary consensus standards developed from this process, once recognized by the Attorney General as substantially complying with the requirements of this Act, will enjoy a compliance safe harbor to the extent they are adopted and complied with by covered entities.

SECTION 6. NON-COMPATIBLE USE OF PERSONAL DATA.

(a) A covered entity shall not process personal data collected from a consumer for a non-compatible use unless, at the time the personal data was collected from the consumer:

(1) sufficient notice and information was provided to the consumer by the entity, or by another covered entity that collected the personal data, to convey to a reasonable consumer that the consumer's personal data might be used for the non-compatible use; and

(2) the consumer had a reasonable opportunity to withhold consent to that non-compatible use.

(b) A covered entity shall not process a consumer's sensitive personal data collected from that consumer for a non-compatible use without obtaining the consumer's express, voluntary, and signed consent in a record for each such non-compatible use.

Comment

Section 6(a) prohibits a covered entity from using personal data for a non-compatible use without providing the consumer notice and adequate information about the nature of the proposed non-compatible use and a reasonable opportunity to withhold consent for it.

Section 6(b) gives heightened protection for sensitive personal data by prohibiting a covered entity from using sensitive personal data for a non-compatible use without obtaining the express, voluntary, written consent of the consumer for each non-compatible use.

SECTION 7. PROHIBITED USE OF PERSONAL DATA.

(a) Except for personal data consisting solely of publicly available information, or derived exclusively from publicly available information, a covered entity may not disclose personal data in a manner that would reasonably, foreseeably and unlawfully:

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

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

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

(4) cause an increased risk of subjecting a person to discrimination if the discrimination would violate a state or federal anti-discrimination law.

Comment

Section 7 specifies prohibited disclosures of personal data that will cause certain consumer harms. The Section does not apply to disclosure of personal data, if it is publicly available information, because of First Amendment concerns explained above.

Section 7(a)(1) prohibits a covered entity from using personal data to inflict specific and significant financial, physical, or reputational harm to the legitimate interests of a person.

Section 7(a)(2) prohibits disclosure that would cause misappropriation of personal data for the purposes identity theft.

Section 7(a)(3) prohibits covered entities from engaging in the tortious use of personal

data to intrude on the solitude or seclusion of a person's private affairs in a manner that would be highly offensive to a reasonable person.

Section 7(a)(4) prohibits covered entities from using personal data to subject a person to an increased risk of unlawful discrimination.

SECTION 8. INFORMATION SYSTEM SECURITY.

(a) A covered entity may not maintain or store personally identifiable information in an information system unless the entity:

(1) implement appropriate administrative, technical, and physical safeguards to provide reasonable security measures to protect the confidentiality, integrity, and accessibility of the information in the system; and

(2) conducts a reasonable risk assessment of the information in the system considering:

(A) the information to be collected;

(B) why the information is to be collected;

(C) the intended use of the information by the covered entity; and

(D) the persons with whom the information is to be shared.

(b) In evaluating the reasonableness of the information system security measures and risk assessment under subsection (a), the following factors must be considered:

(1) the magnitude and likelihood of security risks and the potential resulting harms to consumers resulting from security breaches;

(2) the resources available to the covered entity; and

(3) industry practices among similarly situated covered entities.

Comment

Section 8 establishes information security requirements and risk assessments for information systems containing personally identifiable information. Information systems containing publicly available information are required to comply with this Section.

Section 8(a)(1) establishes a duty for a covered entity to use reasonable measures to protect the information security of its information systems, following the basic principles of computer security—confidentiality, integrity and accessibility—which are found in standards issued by the National Institute of Standards and Technology for computer security. This requirement is based on the Federal Information Security Management Act of 2002 (FISMA).

Section 8(a)(2) requires covered entities to conduct privacy risk assessments for their information systems, tracking the requirements of Section 208 of the E-Government Act of 2002 and Article 35 of the GDPR.

Section 8(b) establishes standards for the reasonableness of a covered entity's information security measures and risk assessments.

SECTION 9. COMPLIANCE WITH RECOGNIZED VOLUNTARY CONSENSUS STANDARDS.

A covered entity complies with a requirement of Sections 4 through 8 of this [Act], and any regulations under these sections, by complying with a voluntary consensus standard for that requirement which is recognized by the [Attorney General] under Section 13.

Comment

Section 9 authorizes covered entities to use a recognized voluntary consensus standard as a safe harbor for compliance with the Act. These voluntary consensus standards will tailor the application of the requirements of the Act for defined sectors and in specific contexts. The voluntary consensus standard must be developed by a voluntary consensus standards body through a process under Section 12, and recognized by the Attorney General under Section 13. This safe harbor provision is based on the safe harbor provisions of the CPSA, 15 U.S.C sec. 2056, the recognition by the Food and Drug Administration of "recognized consensus standards" under the Food, Drug, and Cosmetic Act, 21 U.S.C. 301 and Section 6503 of the COPPA, 15 U.S.C. § 6503. It is also closely related to the safe harbor for "codes of conduct" found in Articles 40 and 41 of the GDPR.

Since 1987, leading standard setting organizations, like the American National Standards Institute, the International Standards Organization and the International Electrotechnical Commission, have published information security and privacy standards for operators of information systems to use in different contexts, which are used by the private sector as well as by state and federal governments. During this period, a bewildering number of standards were developed, covering security processes, internal controls, cryptographic and other security mechanisms, identity management, biometrics, and privacy impact assessments, as well as for notice and consent.

The use by federal and state government agencies of these standards—a kind of public-private partnerships—dates back to 1918 when the American Engineering Standards Committee was created as a joint venture of private sector standards organizations and the federal government to streamline and coordinate the development of the voluntary standards essential to the war effort. The American Engineering Standards Committee eventually became the American National Standards Institute (ANSI), a private organization that today continues to coordinate the U.S. standard setting system in partnership with federal and state government officials.

Furthermore, there are a wide variety of standards for information security, including those published by the National Institute for Standards and Technology (NIST), the ISO/IEC 27000-series of information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission, and the ANSI/ISA 62443 series of information security standards, created by the International Society for Automation (ISA).

As the scope of government health, safety and environmental regulation increased in the 1960s, industry reliance on a private standard setting processes came under increased scrutiny as a result of, what was perceived by some to be, a lack of transparency and openness. In order to address these concerns, the private standards development community reformed the private standard setting process, creating what is today known as the consensus process. This consensus process is marked by the inclusion of participants with a wide range of views, transparency, due process, appeals, and the promise that any resulting standard reflects a true consensus among all stakeholders. These principles are described in OMB Circular A-119 and embodied in ANSI's Essential Requirements

Some statutes refer to these as "voluntary" standards, such as in Section 2056(b) of the CPSA, which requires reliance on "voluntary consumer product safety standards," developed by industrial standard setting organizations, rather than the adoption of regulations, "whenever compliance with such voluntary standards would eliminate or adequately reduce the risk of injury addressed and it is likely that there will be substantial compliance with such voluntary standards." 15 U.S.C. 2056(b). Other statutes, such as Section 655 of Title 29, the Occupational Health and Safety Act, refer to "national consensus standards." The Food and Drug Act refers to "recognized consensus standards."

This Act uses the term "voluntary consensus standard," because that is the standard term used by industry, by the American National Standards Institute and by the Office of Management and Budget. Voluntary consensus standards do not always reflect full agreement of all the stakeholders, but they do reflect a rough consensus, as defined in the ANSI Essential Guidelines. Such standards are entirely voluntary in the sense that, unlike a statute or regulation, covered entities have a choice whether or not to comply with them or to directly comply with the Act.

The manner in which industry standards are used by regulators in Europe to implement regulations, such as the GDPR, differs markedly from the manner in which voluntary consensus standards are used by regulators in the U.S. Something similar to the U.S. notion of "voluntary consensus standards" is recognized by Article 40 of the GDPR, which uses the term "codes of conduct," and requires supervisory authorities to encourage the drawing up of "codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises." https://gdpr-info.eu/art-40-gdpr/ Article 40 recognizes the potential benefits of developing codes of conduct by particular industries, in order to tailor regulatory requirements to reflect the particular needs and concerns of those specific industry sectors.

SECTION 10. VOLUNTARY CONSENSUS STANDARDS FOR PROTECTIONS FOR PERSONAL DATA.

(a) The [Attorney General] under Section 13 may recognize a voluntary consensus standard for protections for personal data only if the standard:

(1) substantially complies with Sections 4 through 7;

(2) specifies the compatible uses and any non-compatible uses for which consumer consent is not required; and

(3) with respect to compatible use,

(A) demonstrates that the processing of personal data conforms to the standard;

(B) identifies the benefits and material risks to stakeholders arising from the proposed processing of the personal data involved;

(C) ensures that the benefits from the proposed processing of the personal data outweigh material risks, after the risks are mitigated by technological, operational, or other means;

(D) presents supporting analysis for assessment of the benefits and material risks fairly, symmetrically, and with an appropriate level of granularity;

(E) addresses alternatives, after disclosing all key assumptions, data, and models; and

(F) specifies the procedures established to protect the interests of the consumer reasonably, including reasonably appropriate internal controls to ensure effective implementation of the standard by the covered entity.

Comment

Section 10 sets out the requirements for voluntary consensus standard to be a safe harbor for the personal data protections of Sections 4 through 7 of the Act.

SECTION 11. VOLUNTARY CONSENSUS STANDARDS FOR INFORMATION SYSTEM SECURITY. The [Attorney General] under Section 13 may recognize a voluntary consensus standard for information system security only if the standard substantially complies with Section 8.

Comment

Section 11 sets out the requirements for a voluntary consensus standard to be a safe harbor for the information system security requirements of Section 8 of the Act.

SECTION 12. PROCESS FOR VOLUNTARY CONSENSUS STANDARDS BODIES.

(a) The [Attorney General] under Section 13 may recognize a voluntary consensus standard only if the standard is developed by a voluntary consensus standards body through a process that:

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

(A) consists of a diverse range of stakeholders;

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

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

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

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

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

(2) includes, and ensures access by, representatives of all stakeholders to the voluntary consensus standards setting process on a non-discriminatory basis;

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

(4) is equitable and responsive to the requirements of all stakeholders;

(5) includes a reasonable opportunity for broad-based public review and comment on a draft voluntary consensus standard, with consideration of, and response to, comments submitted by

voting members of the voluntary consensus standards body and by public review of the comments, followed by incorporation of any approved changes into the draft standard;

(6) consistently adheres to documented and publicly available policies and procedures that provide adequate notice of meetings and standards development and essential due process procedures, and that provide a fair and impartial process that protects the public interest in transparency, openness, balance, and consensus; and

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

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

Comment

Section 12(a) specifies the procedural requirements for voluntary consensus standards bodies to use to develop voluntary consensus standards that are eligible for recognition as a safe harbor by the Attorney General in Section 13.

Section 12(a) is based on the National Technology Transfer and Advancement Act of 1995 ("NTTAA"), PL 104-113, §12(d) (March 7, 1996), 110 Stat. 775, 15 U.S.C.A. § 272(d), requiring all federal agencies to use standards that are developed or adopted by voluntary consensus standards bodies, using such standards as a means to carry out policy objectives. The NTTAA codified earlier versions of OMB Circular A-119, which, beginning as early as 1982, began to require federal agencies to use voluntary consensus standards in lieu of government regulations.

Since the 1990s, OMB Circular 119 has required a standard setting organization to use a process that was characterized by openness, balance of interest, due process and appeals process, and consensus defined as general agreement but not necessarily unanimity, and that resolved objections by all interested parties, as long as all objections have been fairly considered, each objector is advised of the disposition of his or her objection(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments. Section 12(a) places the same requirements on voluntary consensus standard bodies under this Act.

ANSI accredited standards bodies are already committed to respect the procedural safeguards embodied in the ANSI Essential Requirements, which incorporate the requirements of OMB Circular 119, so voluntary consensus standards produced by such accredited bodies will

have already met the requirements of this Section. Standard setting bodies that observe similar procedural safeguards, without being ANSI-accredited, may also use a process that complies with the requirements of this Section.

Section 12(b) requires the voluntary consensus standards body, in developing a voluntary consensus standard, to reasonably reconcile the requirements of the Act with the requirements of other applicable federal and state laws.

As noted above, the reconciliation of a universal privacy framework, such as this Act, with the complex and diverse existing system of federal and state sectoral privacy laws, can pose intractable problems for privacy statutes like the CCPA, which attempt to regulate all information directly. The Act, however, addresses this problem successfully in several ways, including this section. Voluntary consensus standards should be most effective in resolving this problem since they allow for a genuine reconciliation of these different legal frameworks to take place—which can only be done in a granular and specific way—which voluntary consensus standards are designed to do. Thus, the Act generally, and especially this subsection, protects covered entities from the risk that a general privacy law will generate irreconcilable conflicts with the legal obligations they already follow under pre-existing laws applicable to that sector.

SECTION 13. RECOGNITION OF VOLUNTARY CONSENSUS STANDARDS BY [ATTORNEY GENERAL].

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

(1) substantially complies with th requirements of Section 10 or Section 11;

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

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

(4) reasonably balances the interests of, and the probable costs and benefits to, consumers, covered entities, other materially affected persons, and the public of implementation of the standard; and

(5) with respect to a compatible use:

(A) appropriately balances the interests of consumers in their personal data

with the interests of stakeholders and any other entities making lawful use of the personal data;

(B) does not unduly hamper innovation or competition; and

(C) does not unduly restrict access to personal data for authorized governmental activities involving regulation of financial markets, public health or welfare, enforcement of criminal laws, or the protection of national security.

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

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

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

(e) A voluntary consensus standard recognized by an interstate compact under Section 15 shall be deemed recognized under this Section.

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

(g) Upon notice in a record to the [Attorney General] by a covered entity that the entity complies with the General Data Protection Regulation (EU), the California Consumer Privacy Act, or other substantially similar law, or the Asia Pacific Economic Cooperation Cross Boarder Privacy Rules System, the US-EU Privacy Shield Framework, or other substantially similar framework, administered by the International Trade Administration of the U. S. Department of Commerce to

facilitate cross-boarder information transfers, the entity shall be deemed in compliance with this [Act].

(1) If the [Attorney General] determines that the law or framework, claimed to be substantially similar to this [Act], is not substantially similar to this [Act], the [Attorney General] shall give the entity notice in a record of that determination and the entity shall be required to comply with the requirements of this [Act].

(2) A violation by the entity of the requirements of any substantially similar law or framework, the subject of the notice by the entity to the [Attorney General] under this subsection shall be a violation of this [Act].

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

Comment

Section 13(a) provides for the requirements for the Attorney General to recognize a voluntary consensus standard for a safe harbor.

Section 13(b), (c), provides the procedures for the Attorney General to recognize a voluntary consensus standard and establishes an expedited process for obtaining judicial review of this decision. These sections are based on Section 6503(b)(3) of the Children's Online Privacy Protection Act.

Section 13(d) authorized the Attorney General to adopt regulations to govern the process of recognizing voluntary consensus standards.

Section 13(e) deems a voluntary consensus standard recognized by an interstate compact under Section 15 to be recognized as a voluntary consensus standard under Section 13.

Section 13(f) allows the Attorney General to recognize a voluntary consensus standard recognized by the Attorney General of another state with a law substantially similar to this Act.

Section 13(g) establishes a framework of interoperability of the Act with other substantially similar state and international privacy laws and international privacy frameworks by providing that, if a covered entity complies with such a law or framework, the covered entity shall be deemed in compliance with this Act.

Section 13(h) allows the Attorney General to charge a reasonable fee for the costs involved in recognizing voluntary consensus standards. This provision seeks to relieve the financial burden on the Attorney General of administering the recognition process.

SECTION 14. ENFORCEMENT.

(a) A violation of this [Act] constitutes an [unlawful practice] under [cite to the state's consumer protection act].

(b) The [Attorney General] shall enforce this [Act], and any regulations adopted under this [Act], in the same manner, by the same means, with the same jurisdiction, powers, and duties, and with the same enforcement authority, as provided in [cite to the state's consumer protection law].

[(c) A person may bring a private cause of action against a covered entity for actual damages as provided in [cite to the state's the consumer protection law] for:

(1) a knowing and intentional violation of Section 7; or

(2) a the willful and repeated violation of any provision of this [Act], other than Section 7.

(d) In subdivision (c)(2), "willful and repeated" means multiple knowing violations of the [Act] over a substantial period of time.

(e) Before the filing a [complaint] under subsection (c), a person shall give the covered entity notice in a record that the entity has [30] days in which to correct the violation, mitigate any injury and resolve the claim.]

(f) In a civil proceeding claiming a violation of a provision of this [Act], other than Section 7, there is a rebuttable presumption that a covered entity is in compliance with the [Act], if the entity has obtained a certification of the entity's compliance with a recognized and applicable voluntary consensus standard from the voluntary consensus standard body which developed the standard or from an accredited and independent certification organization.

(g) The [Attorney General] may adopt regulations under [cite to the state's administrative procedures act] to carry out the provisions of this [Act].

Comment

Section 14(a) aligns the scope of the Act's protections for personal data, and personally identifiable information, with the established scope of state consumer protection laws by providing that a violation of this Act constitutes an unlawful practice under the state's consumer protection act.

Providing for enforcement of the Act through the state's consumer protection act integrates the Act into an already existing and familiar legal, bureaucratic and enforcement regime. It also reduces jurisdictional conflicts with a large number of the existing sectoral federal and state privacy laws, such as the Privacy and Security Rules under the Health Insurance Portability and Accountability Act; the Fair Credit Reporting Act, the Gramm-Leach-Bailey Act, the Bank Secrecy Act and Right to Financial Privacy Acts, the Family Educational Rights and Privacy Act, the Children's Online Privacy Protection Act;,the Telephone Consumer Protection Act of 1991, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, the Employment Retirement Income Security Act, the Family and Medical Leave Act, the Occupational Safety and Health Act, and the Electronic Communications Privacy Act of 1986, as well as their many state counterparts, and state common law breach of confidentiality torts, such as invasion of privacy, intrusion on seclusion, public disclosure of private facts, false light, and appropriation of identity for commercial purpose.

These existing federal and state sectoral laws and common law legal doctrines have a settled place in the American legal system and enjoy high compliance rates. However, advocates of a "universal" privacy law regime criticize the U.S. sectoral legal system and seek to replace them, not because of the adequacy of the privacy protections provided by these sectoral laws, but because of perceived gaps in the privacy protections existing laws provide. Aligning the Act with the existing state consumer protection framework fills in these gaps, creating a more comprehensive framework. Thus, the Act is designed to fill the gaps in existing privacy laws, not replacing them. This results in turning the scattered privacy law coverage into a seamless quilt of legal protection.

Section 14(b) authorizes the Attorney General to bring enforcement actions for violations of any provision of the Act under the provisions of the state's consumer protection law.

Section 14(c) is optional depending on whether a particular state's consumer protection act already provides for a private cause of action. If it does, the private cause of action, under Section 14(c), is governed by the applicable provisions of the state's consumer protection act, subject to the additional requirements in Sections 14(c), (d) and (e).

Section 14(d) defines "willful and repeated" for purposes of a private cause of action under Section 14(c).

Section 14(e) establishes a notice requirement prior to filing a suit asserting a private cause of action under Section 14(c).

Section 14(f) provides a rebuttable presumption, in any suit claiming a violation of the Act, that a covered entity is in compliance with the Act, if the covered entity has received a certificate of compliance with an applicable recognized voluntary compliance standard from an accredited certification organization.

Section 14(g) authorized the Attorney General to adopt regulations to carry out the provisions of the Act.

SECTION 15. INTERSTATE COMPACT FOR RECOGNITION OF VOLUNTARY CONSENSUS STANDARDS.

(a) Upon certification by the [Attorney General] that a federal law has authorized an interstate compact of states that have enacted a law substantially similar to this [Act] for the recognition of voluntary consensus standards, this state adopts the interstate compact when the [Attorney General] provides notice in a record of the adoption.

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

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

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

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

Comment

This provision establishes the framework for, and approval of, an interstate compact to recognize voluntary consensus standards under the Act.