A. GENERAL.

1. The Act applies broadly. The Uniform Personal Data Protection Act applies fair information practices to the collection and use of personal data from consumers by businesses. The Act applies broadly to any entity that collects and maintains personal data.

2. But is not regulatory. However, the Act avoids the high compliance costs for businesses and the substantial enforcement costs for states associated with regulatory regimes modeled after the European General Data Privacy Regulation (“GDPR”) and the California Consumer Privacy Act (“CCPA”). A substantial downside of a highly regulatory approach is that it stifles competition. A small firm can't compete with Google if the privacy regulations are onerous. Consumers benefit from more competition.

3. The Act balances interests of consumers and businesses. The Act takes fresh look at the privacy issues that data practices over the Internet have engendered. While the Act provides consumers with significant protections for the use of consumers’ data, it also permits flexibility and innovation that can lead to consumer benefits. The Act gives consumers the right to access and correct or amend their personal data held by others and protects them from unexpected, potentially risky uses of their data without their consent.

B. THE TYPES OF BUSINESSES COVERED ARE DATA CONTROLLERS AND DATA PROCESSORS.

The businesses subject to the Act are data controllers and data processors.

1. A controller determines the purpose and means of data processing. Section 2(3).

2. A processor performs operations on personal data at the direction of the controller. Section 2(12). But, if a processor goes off on its own, it becomes a controller and is treated as such.
3. There are two types of controllers:
   
a. *Collecting controllers*, which collect personal data directly from data subjects. Section 2(1).

b. *Third-party controllers*, which collect data from collecting controllers or other third-party controllers and determine the purposes and means of the additional processing. Section 2(21).

4. The Act imposes greater duties on collecting controllers because those controllers are the ones that have a direct relationship with the data subjects.

C. **THE TYPE OF DATA COVERED IS PERSONAL DATA.**

1. The data to which the Act applies is “personal data”. There are two types of “personal data”:

   a. Data described by a *direct identifier*, which is commonly used to identify an individual, such as a name, physical address, e-mail address, recognizable photograph, and telephone number. Section 2(6).

   b. *Pseudonymized data*. Pseudonymized is data which personal identifiers have been removed, but which is linked, or which can be linked, to an individual, and may be accessed by use of a code for purposes of individualized communication or treatment. Section 2(14).

2. Pseudonymized data is a form of personal data that provides more privacy and security. So the Act encourages businesses to convert data into pseudonymized data by making this data subject to fewer restrictions than data with direct identifiers, notably by not requiring the business to provide copies of or to correct or amend pseudonymized data unless it is maintained with sensitive data.

3. The Act does not apply to “deidentified data,” which is data that has been modified to remove all direct identifiers and to reasonably ensure that the record cannot be linked to an identified data subject by a person that does not have personal knowledge or special access to the data subject’s information. Section 2(5), (10).
D. TYPES OF DATA PRACTICES COVERED. Sections 7, 8, 9.

The Act creates three categories of a business’s uses of a data subject’s information — (1) compatible data practices; (2) incompatible data practices; and (3) prohibited data practices — and states different rules for each category.

1. A “compatible data practice” is one that is consistent with the data subject’s interests or reasonable expectations or which would directly benefit the data subject. Sections 2(2), 7.

   a. The Act permits a compatible data practice without the data subject’s consent. This applies to personal data that includes “sensitive data” because the premise is that the use of the data is consistent with reasonable expectations of, or would directly benefit, the data subject.

   b. Requiring consent imposes significant burdens on businesses and consumers. We all have experienced privacy notices or “I accept” buttons attached to long legal documents. This is unnecessary if the data is used exclusively in ways that are compatible with data subject’s expectations and interests or that would directly benefit the data subject.

   c. Businesses may avoid the costs of consent if they use data exclusively in ways that are compatible with consumer expectations and best interests. This incentivizes use of compatible data practices.

2. A “prohibited data practice” is one that poses a substantial risk of harm to data subjects, including processing likely to cause embarrassment, harassment, or financial harm and data storage that fails to provide reasonable data security. The Act prohibits controllers or processors from engaging in prohibited data practices. Sections 2(13), 9.

3. An “incompatible data practice” is one that is not a compatible data practice or a prohibited data practice. Section 2(17). It is not likely to cause either substantial benefit or substantial harm. The Act permits an incompatible data practice after the data subject is given notice and has consented.

   a. *Type of consent depends on whether there is sensitive data.* The type of consent for an incompatible data practice depends on whether the incompatible data practice involves “sensitive data.” This includes information such as race, religious belief, gender, sexual orientation, citizenship, immigration status, geolocation in
real time, criminal record, medical diagnoses, Social Security Number, numbers of government issued identification, and information pertaining to children under 13. Section 2(17).

b. **Opt-out requirement if no sensitive data:** If the incompatible data practice does not include “sensitive data”, the controller must give the consumer notice and the opportunity to withhold consent. Section 8(b).

c. **Opt-in requirement if sensitive data:** If the incompatible data practice includes “sensitive data,” the controller must obtain the consumer’s express consent in a signed record for each practice. Section 8(c).

d. **Controller may require consent.** A controller may condition access to goods or services to consent to an incompatible data practice and may offer a reward or discount in exchange. Section 8(d)

4. **Examples:**

a. **Public mobility data for health risks.** Using pseudonymized personal data such as location data for COVID risk assessment is a compatible data practice because it is for generalized research. Section 7(b)(6). Using data for targeting COVID exposure risk assessments and notifications is a form of tailored communication and is likely to benefit the data subject. Section 7(c), (a). However, if a company uses personal data such as location data or COVID risk to deny entry to a building or to increase the price of a service, that use of data would be incompatible and would require consent.

b. **Targeted advertising.** Using personal data for targeted advertising, or other tailored messaging, is a compatible data practice, which may be done without consent. Permitting targeting advertising without consent not only relieves businesses of the burdens of obtaining consent; it also benefits consumers, who receive free content and services that might not otherwise be provided. There are those who would like to disrupt the business models of many companies who provide goods and services for free or for nominal price in return for use of personal data for targeted advertising. The Act does not disrupt those models.
c. **Differential treatment.** Using the data for differential offers, agreements, or treatment is an incompatible data practice, which may be done only with consent.

d. **Selling data for marketing purposes.** Selling data (in identified form) for marketing purposes that are not within the reasonable expectations of the consumer is an incompatible data practice.

e. **Selling or sharing data for unrestricted purposes.** A company shares a data user’s geolocation data with his spouse or employer for unlimited and unrestricted use. This is an incompatible data practice requiring consent. Moreover, if the company knows that the recipient will use the data for a prohibited practice, such as to publicly shame and humiliate the data subject, the company will be held responsible for the prohibited act.

E. **BUSINESSES SUBJECT TO THE ACT. Section 3(a).**

1. **Directed to state residents.** The Act applies to the activities of a controller or processor that conduct business in the enacting state or produce products or provide services purposefully directed to residents of the state.

2. **Threshold of activities determined by each state.** The Act allows each state to determine the threshold of activity by businesses for the law to apply to them by placing these thresholds in brackets. The law applies to controllers and processors that “maintain” personal data of more than [50,000] data subjects or earn more than [50] percent of their gross annual revenue from “maintaining” personal data from data subjects as a controller or processor. Each state may substitute its own numbers for those in brackets.

3. **General applicability for incompatible or prohibited data practices.** The Act also applies to all controllers or processors, without limitation to number of data subjects or income, if they maintain personal data for incompatible (or prohibited) data practices. Thus, small businesses are exempt from the Act as long as they use only “compatible” data practices.

4. **Maintenance requirement as a limiting principle.** A business must “maintain” the data for a data transaction to count. To be “maintained,” the data must be part of a “system of records used to retrieve records about individual data subjects for the purpose of individualized communication or decisional treatment.” Section 2(8). This is an important limiting provision. It avoids sweeping in data transactions used, for example, purely
for one-time purchases by credit cards or unstructured forms of information such as e-mail communication.

F. EXEMPTIONS FROM THE ACT. Section 3(b), (c).

The following data are exempt from the Act, even if they would otherwise be “personal data”: 

1. Data maintained by an agency, instrumentality, or political subdivision of the state. Section 3(b)

2. The following types of data (Section 3(c)):
   a. Publicly available information.” Section 2(15). Information that is:
      i. Lawfully made available from a federal, state, or local government record, or which a person reasonably believes is lawfully made available to the general public;
      ii. Available to the general public in widely distributed media, such as a website, telephone book, or television or radio program; or
      iii. Observable from a publicly accessible location.
   b. Data processed or maintained solely as part of human-subjects research.
   c. Data subject to a warrant, subpoena, court order or rule, or other law.
   d. Data subject to public disclosure under a state public records act.
   e. Data processed or maintained in the course of a data subject’s employment or application for employment.

G. THE RIGHT OF DATA SUBJECTS TO HAVE CONTROLLERS COPY AND CORRECT OR AMEND PERSONAL DATA. Sections 4 and 5.

1. *Right to copy or correction or amendment.* A data subject has the right to have a copy of the information and to correct or amend the data, and a collecting controller has a duty to do so.
2. *But not for pseudonymized data.* There is an exception for pseudonymized data that is not maintained with sensitive data. This provides an incentive for businesses to convert data with direct identifiers into pseudonymized data.

3. *Request to collecting controller.* The consumer would make the request to the collecting controller, which has directly collected data from consumers, and is in the best position to authenticate the identity of the requester. This avoids unintended increased data security risks.

4. *Collecting controller requests others to correct data.* The collecting controller, in turn, would request processors or third-party controllers to correct the data in their possession. The collecting controller is responsible for ensuring others in the change make the correction. All other downstream recipients of personal data must respond to requests that are transmitted by the collecting controller.

5. *Response time.* The collecting controller must comply with the request within [45] days or a reasonable time. Each state may set a specific time limit or simply provide for a reasonable time.

6. *Copies of data.* One copy would be given free every 12 months.

7. *Correction of data.* The controller would make a correction or amendment requested by a data subject if the controller has no reason to believe the request is inaccurate, unreasonable, or excessive. And either confirm the change was made or explain why it was not.

8. *Retaliation prohibited.* A controller may not retaliate or take any other adverse action against the requester for exercising his or her rights. However, if the corrected information causes a change in treatment—for example, if it renders the consumer ineligible for a loyalty program—this is not considered to be retaliation.

9. *No waiver.* An agreement that waives or limits a right or duty concerning copying or correcting or amending data is unenforceable. Section 5(d).
10. **No right to data deletion.** Unlike the GDPR and CCPA, there is no right to the deletion of data.

   a. Data deletion imposes an onerous, sometimes impossible, burden on controllers since there may be multiple copies of the data, at least in part, with a number of entities.

   b. There are many legitimate reasons why the data should not be deleted, including ensuring compliance with the law.

   c. The European GDPR’s “right to be forgotten” or more recent “right to erasure” would face substantial First Amendment challenges in the United States. See *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975) (Georgia law allowing the father of a deceased rape victim to sue a television station for invasion of privacy by broadcasting the victim’s name violated the First Amendment); *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011) (Vermont statute that restricted the restricted the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors violated First Amendment).

   d. The restrictions on use only for compatible data, or incompatible data with consent, are sufficient protections.

**H. GENERAL OBLIGATIONS OF CONTROLLERS AND PROCESSORS.**

1. **Privacy policy.** To promote transparency and accountability, the Act requires each controller to adopt and comply with a reasonably clear and accessible privacy policy, including information on the categories of personal information maintained or provides to processors; its routine compatible data practices; its incompatible data practices; its procedures to respond to a data subject’s exercise of rights; federal, state, or international frameworks to which the controller complies; and any voluntary consensus standard adopted. Section 6.

2. **Security risk assessment.** Controllers and processors must conduct and maintain a data privacy and security risk assessment that is appropriate to the scope of the business of the controller or processor. Section 10.

3. **Self-assessment is confidential.** To encourage honest self-reflection, the Act shields the content of the self-assessment from disclosure in subsequent litigation.
I. COMPLIANCE WITH OTHER LAWS PROTECTING PERSONAL DATA IS COMPLIANCE WITH THIS ACT. Section 11.

1. **Compliance with at least as protective statutes suffices.** The Act allows controllers or processors to avoid the costs of multiple compliance protocols by recognizing compliance with other similar or more restrictive laws as compliance with this Act.

2. **Two types of compliance through other statutes.** A controller or processor is deemed in compliance with this Act in two situations:

   a. Per se compliance if the controller or processor is subject to one of several federal laws, which apply to specific sectors: (1) Health Insurance Portability and Accountability Act; (2) Fair Credit Reporting Act; (3) Gramm-Leach-Bliley Act of 1999; (4) Drivers Privacy Protection Act of 1994; (5) Family Education Rights and Privacy Act of 1974; (6) Children’s Online Privacy Protection Act of 1998.

   b. Compliance with a law of another jurisdiction that the state’s attorney general determines is at least as protective of personal data that this Act. Thus, a company will not wind up having to comply with a patchwork of state laws. So, if the company satisfies the heightened requirements of a law like the CPPA, it will be in compliance with this Act.

J. DEVELOPMENT BY STAKEHOLDERS OF VOLUNTARY CONSENSUS STANDARDS AND RECOGNITION BY ATTORNEYS GENERAL. Sections 12-15.

1. **Tailored voluntary consensus standards.** The Act encourages the development of voluntary consensus standards by which data controllers, processors, data subjects and other interested stakeholders can engage together to develop rules for specific applications, services, or contexts, tailored to the context of particular industries.

2. **Recognition required.** The voluntary consensus standard must be recognized by the state’s attorney general.

3. **Compliance with consensus standards suffices.** Compliance with a recognized voluntary consensus standard will satisfy a corresponding requirement of this Act.
4. **Analogies.** There are analogous situations in which states have kept a complex framework of standards up to date, including consumer product safety codes, construction codes, and secured transaction filing rules, which have been harmonized by Section 9-526 of the Uniform Commercial Code.

5. **Role of NAAG.** It is hoped that the efforts of the state attorneys general will be coordinated by the National Association of Attorney General, which has a working group on personal data protection with a wide membership.

6. **Future proofed.** As innovations in artificial intelligence, driverless vehicles, and other unforeseen technologies take place, the Act will not have to be constantly updated.

**K. ENFORCEMENT. Section 16.**

1. **State consumer codes incorporated.** That Act incorporates enforcement provisions of existing state consumer protection acts that authorize state attorneys general to monitor personal data practices and to seek redress for violations of the Act.

2. **Rulemaking by attorney general.** The Act also authorizes the state’s attorney general to promulgate rules to implement the Act, including consideration of rules and practices in this area by other states.

3. **Coordination of enforcement by states.** The Act encourages uniformity of enforcement in the enacting states by authorizing state attorneys general directly, or through the National Association of Attorneys General, to coordinate their regulatory and enforcement policies.

4. **States decide whether to permit private right of action.** The Act encourages states to determine for themselves whether a private right of action should be authorized for violation of the act and provides bracketed language to prohibit such rights of action, which would leave enforcement to the state attorney general.

**L. OTHER LAWS ARE NOT AFFECTED. Section 17.**

1. The Act does not create or affect a cause of action under other law of the state.

2. Thus, it does not supplant acts based on traditional common law or other statutory law, for example, defamation, right to privacy, and intentional infliction of emotional harm.