Federal Privacy Law

Section 1 - Short Title; Table Of Contents.

1. Short Title.—This Act may be cited as the “Protecting Rights of Information for which Vestiges of Citizens Yearn” or the “PRIVACY Act”.
2. Table Of Contents.—The table of contents for this Act is as follows:
    a. [INSERT]

Section 2 - Breach Notification

A breach notice [is required] in the event of unauthorized access that is reasonably likely to result in identity theft [Sensitive Personal Information], fraud, or economic loss. Such notice shall be made within a reasonable time.

1. A Covered Entity that owns or licenses computerized data that includes Sensitive Personal Information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data
    a. whose unencrypted Sensitive Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, or,
    b. whose encrypted Sensitive Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or covered entity that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.

Disclosures shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

A covered entity that maintains computerized data that includes Sensitive Personal Information that the covered entity does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

2. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.
3. A covered entity that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
    a. The security breach notification shall be written in plain language, shall be chaptered “Notice of Data Breach,” and shall present the information described

in paragraph under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

b. The format of the notice shall be designed to call attention to the nature and significance of the information it contains.
c. The chapter and headings in the notice shall be clearly and conspicuously displayed.
d. The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.
e. For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

Section 3 - Right to Access

A verifiable consumer can request from a covered entity:

1. Categories and specific pieces of Personal Information the business has collected by the covered entity
2. Deletion of the verifiable consumer’s Personal Information provided to the covered entity by the verifiable consumer
3. Categories, sources, purpose, third-party sharing, and specific pieces of the verifiable consumer’s personal information that has been collected
4. The covered entity may charge a reasonable fee for the processing of the request.
5. A covered entity need only reply to a verifiable consumer request no more than once every six-months.
6. Response by a covered entity is not required when Personal Information is necessary for
    a. Conducting business with the consumer
    b. Security purposes
    c. Repair purposes
    d. Exercise of free speech
    e. Research purposes
    f. Must be in the public interest and in compliance with all other ethics/privacy laws
    g. Solely internal uses
    h. Compliance with legal obligations
    i. Internal uses consistent with context in which consumer provided information

For purposes of this section, a covered entity may use any Personal Information or Sensitive Personal Information collected from the consumer in connection with the covered entity's verification of the consumer's request solely for the purposes of verification.

A covered entity is not obligated to provide information to the consumer pursuant to this section if the business cannot verify that the consumer making the request is the consumer about whom the covered entity has collected Personal Information or Sensitive Personal Information.

Section 4 - Opt-out of collection

Consumers can opt-out of sale of their Personal Information to third parties. Consumers can later re-authorize sale of information.

Covered entities may alter provision of services and pricing if a consumer opts-out of sale of their Personal Information to third parties.

Covered entity must provide notice to consumers of how to opt-out of sale of their Personal Information to third parties.

Section 5 - Right of Action

The United States Federal Trade Commission may enforce this statute against any commercial covered entity. The Department of Justice may enforce this statute against any non-commercial covered entity.

Except as provided in subsection (c), the attorney general of a State, or other authorized State officer, alleging a violation of this Act or any regulation issued under this Act that affects or may affect such State or its residents may bring an action on behalf of the residents of the State in any United States district court for the district in which the defendant is found, resides, or transacts business, or wherever venue is proper under section 1391 of chapter 28, to obtain appropriate injunctive relief.

1. Notice to Commission Required.
    a. A State shall provide prior written notice to the Federal Trade Commission and the Department of Justice of any civil action under subsection (b) together with a copy of its complaint, except that if it is not feasible for the State to provide such prior notice, the State shall provide such notice immediately upon instituting such action.
2. Intervention by the Commission.
    a. The Commission or Department may intervene in such civil action and upon intervening be heard on all matters arising in such civil action; and file petitions for appeal of a decision in such civil action.
3. Limitation.

a. No separate suit shall be brought under this section if, at the time the suit is brought, the same alleged violation is the subject of a pending action by the Federal Trade Commission or the United States under this chapter.

4. State law
    a. In general this chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.

This chapter shall not be construed to preempt the applicability of State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or other State laws to the extent that those laws relate to acts of fraud or computer crime.

Section 6 – Safe Harbor

1. Guidelines
    a. A Covered entity may satisfy the requirements of regulations issued under this chapter by following a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, approved under subsection (b).
2. Incentives
    a. Self-regulatory incentives
        i. The Federal Trade Commission shall provide incentives for self-regulation by operators to implement the protections afforded children under the regulatory requirements described in subsection (b) of that section.
    b. Deemed compliance
        i. Such incentives shall include provisions for ensuring that a covered entity will be deemed to be in compliance with the requirements of this chapter if that person complies with guidelines that, after notice and comment, are approved by the Commission upon making a determination that the guidelines meet the requirements of this chapter.
3. Expedited response to requests
    a. The Federal Trade Commission shall act upon requests for safe harbor treatment within 180 days of the filing of the request and shall set forth in writing its conclusions with regard to such requests.
4. Appeals
    a. Final action by the Federal Trade Commission on a request for approval of guidelines, or the failure to act within 180 days on a request for approval of guidelines, submitted under subsection (b) may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of chapter 5.

Section 7 - Definitions

"Consumer" means a resident of the United States of America.

"Covered entity" means any business or organization as defined in the US Tax Code that receives information on more than 10,000 identified individuals.

"Identified Individual Information" means first name or first initial and last name along with:

1. Alias, postal address, email address, account name, social security number, driver's license number, [or] passport number
2. Specific Geolocation data, or
3. Professional, employment, and education information

"Sensitive Personal Information" means data that has a high likelihood of causing financial harm along with Identified Individual Information.

"Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the covered entity to another covered entity or a third party for monetary or other valuable consideration.

"Personal Information" means data that is not Sensitive Personal Information and identifies, relates to, describes, is capable of being associated with an Identified Individual Information.

"Third party" means a person who is not any of the following:

1. The covered entity that collects personal information from consumers under this chapter.
2. A person to whom the covered entity discloses a consumer's personal information for a purpose pursuant to a written contract, provided that the contract:
    a. Prohibits the person receiving the personal information from: (i)
    b. Selling the personal information.
    c. Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
3. Retaining, using, or disclosing the information outside of the direct covered entity relationship between the person and the covered entity.
4. Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them. A person covered by paragraph (2) that violates any of the restrictions set forth in this chapter shall be liable for the violations. A covered entity that discloses personal information to a person covered by paragraph (2) in compliance with paragraph (2) shall not be liable under this chapter if the person receiving the personal information uses it in violation of the restrictions set forth in this chapter,

provided that, at the time of disclosing the personal information, the covered entity does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

“Verifiable consumer request” means a request that is made by a resident of the United States whom the resident has a relationship with the covered entity.