STATE OF NEW YORK

3163

2023-2024 Regular Sessions

IN SENATE

January 30, 2023

Introduced by Sen. HOYLMAN-SIGAL -- read twice and ordered printed, and when printed to be committed to the Committee on Consumer Protection

AN ACT to amend the general business law, in relation to restricting the disclosure of personal information by businesses

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "right to know act".

§ 2. The legislature hereby finds and declares that the right to privacy is a personal and fundamental right protected by the United States Constitution. All individuals have a right of privacy in information pertaining to them.

This state recognizes the importance of providing consumers with transparency about how their personal information has been shared by businesses. For free market forces to have a role in shaping the privacy practices and for "opt-in" and "opt-out" remedies to be effective, consumers must be more than vaguely informed that a business might share personal information with third parties. Consumers must be better informed about what kinds of personal information are purchased by businesses for direct marketing purposes. With these specifics, consumers can knowledgeably choose to opt-in or opt-out or choose among businesses that disclose information to third parties for direct marketing purposes on the basis of how protective the business is of consumers' privacy.

Businesses are now collecting personal information and sharing and selling it in ways not contemplated or properly covered by the current law. Some web sites are installing up to one hundred tracking tools when consumers visit web pages and sending very personal information such as age, gender, race, income, health concerns, and recent purchases to third-party advertising and marketing companies. Third-party data broker companies are buying, selling, and trading personal information obtained

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD02240-01-3

from mobile phones, financial institutions, social media sites, and other online and brick and mortar companies.

Some mobile applications are sharing personal information, such as location information, unique phone identification numbers, and age, gender, and other personal details with third-party companies.

Consumers need to know the ways that their personal information is being collected by companies and then shared or sold to third parties in order to properly protect their privacy, personal safety, and financial security.

§ 3. The article heading of article 39-F of the general business law, as amended by chapter 117 of the laws of 2019, is amended to read as follows:

[~~NOTIFICATION OF UNAUTHORIZED~~] ACQUISITION **AND USE** OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS

§ 4. The general business law is amended by adding a new section 899-cc to read as follows:

§ 899-cc. Disclosure of a customer's personal information to a third party. 1. (a) A business that retains a customer's personal information shall make available to the customer free of charge access to, or copies of, all of the customer's personal information retained by the business.

(b) A business that discloses a customer's personal information to a third party shall make the following information available to the customer free of charge:

(1) All categories of the customer's personal information that were disclosed, including the categories set forth in paragraph (b) of subdivision four of this section.

(2) The names and contact information of all of the third parties that received the customer's personal information from the business, including the third party's designated request address or addresses if available.

2. A business required to comply with subdivision one of this section shall make the required information available by one or more of the following means:

(a) By providing a designated request address and, upon receipt of a request under this section to the designated request address, providing the customer within thirty days with the required information for all disclosures occurring in the prior twelve months, provided that:

(1) if the business has an online privacy policy, that policy includes a description of a customer's rights pursuant to this section accompanied by one or more designated request addresses; provided that a business with multiple online privacy policies must include this information in the policy of each product or service that collects personal information that may be disclosed to a third party;

(2) the business ensures that all persons responsible for handling customer inquiries about the business' privacy practices or the business' compliance with this section are informed of all designated request addresses; and

(3) the business provides information pertaining to the specific customer if that information is reasonably available to the business, and provides information in standardized format if information pertaining to the specific customer is not reasonably available.

(b) For information required to be provided by paragraph (b) of subdivision one of this section, by providing the customer with notice including the required information prior to or immediately following a disclosure.

(c) By providing the customer the disclosure required by Section 6803 of Title 15 of the United States Code, but only if the disclosure also complies with this section.

3. (a) A business is not obligated to provide more than one notice under paragraph (b) of subdivision two of this section to the same customer in a twelve-month period about the disclosure of the same personal information to the same third party and is not obligated under paragraph (a) of subdivision two of this section to respond to a request by the same customer more than once within a given twelve-month period.

(b) A business is not obligated to provide information to the customer pursuant to subdivision one of this section if the business cannot reasonably verify that the individual making the request is the customer.

4. For purposes of this section, the following terms have the following meanings:

(a) "Business" means any person, proprietorship, firm, partnership, association, cooperative, nonprofit organization or corporation organized or existing under the laws of this state or any other state, and doing business in this state, exclusive of public corporations as defined pursuant to article two-A of the general construction law.

(b) "Categories of personal information" includes, but is not limited to, the following:

(1) Identity information including, but not limited to, real name, alias, nickname, and user name.

(2) Address information, including, but not limited to, postal address or e-mail.

(3) Telephone number.

(4) Account name.

(5) Social security number or other government-issued identification number, including, but not limited to, social security number, driver's license number, identification card number, and passport number.

(6) Birthdate or age.

(7) Physical characteristic information, including, but not limited to, height and weight.

(8) Sexual information, including, but not limited to, sexual orientation, sex, gender status, gender identity, and gender expression.

(9) Race or ethnicity.

(10) Religious affiliation or activity.

(11) Political affiliation or activity.

(12) Professional or employment-related information.

(13) Educational information.

(14) Medical information, including, but not limited to, medical conditions or drugs, therapies, mental health, or medical products or equipment used.

(15) Financial information, including, but not limited to, credit, debit, or account numbers, account balances, payment history, or information related to assets, liabilities, or general creditworthiness.

(16) Commercial information, including, but not limited to, records of property, products or services provided, obtained, or considered, or other purchasing or consumer histories or tendencies.

(17) Location information.

(18) Internet or mobile activity information, including, but not limited to, Internet protocol addresses or information concerning the access or use of any Internet or mobile-based site or service.

(19) Content, including text, photographs, audio or video recordings, or other material generated by or provided by the customer.

(20) Any of the above categories of information as they pertain to the children of the customer.

(c) (1) "Customer" means an individual who is a resident of New York state who provides personal information to a business, with or without an exchange of consideration, in the course of purchasing, viewing, accessing, renting, leasing, or otherwise using real or personal property, or any interest therein, or obtaining a product or service from the business including advertising or any other content.

(2) An individual is also the customer of a business if that business obtained the personal information of that individual from any other business.

(d) "Designated request address" means a mailing address, e-mail address, web page, toll-free telephone number, or other applicable contact information, whereby customers may request or obtain the information required to be provided under subdivision one of this section.

(e) (1) "Disclose" means to disclose, release, share, transfer, disseminate, make available, or otherwise communicate orally, in writing, or by electronic or any other means to any third party as defined in this section.

(2) "Disclose" does not include:

(A) Disclosure of personal information by a business to a third party pursuant to a written contract authorizing the third party to utilize the personal information to perform services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, or similar services, but only if (I) the contract prohibits the third party from using the personal information for any reason other than performing the specified service or services on behalf of the business and from disclosing any such personal information to additional third parties and (II) the business effectively enforces these prohibitions.

(B) Disclosure of personal information by a business to a third party based on a good-faith belief that disclosure is required to comply with applicable law, regulation, legal process, or court order.

(C) Disclosure of personal information by a business to a third party that is reasonably necessary to address fraud, security, or technical issues; to protect the disclosing business' rights or property; or to protect customers or the public from illegal activities as required or permitted by law.

(D) Disclosure of personal information by a business to a third party that is otherwise lawfully available to the general public, provided that the business did not direct the third party to the personal information.

(f) "Personal information" means:

(1) Any information that identifies or references a particular individual or electronic device, including, but not limited to, a real name, alias, postal address, telephone number, electronic mail address, Internet protocol address, account name, social security number, driver's license number, passport number, or any other identifier intended or able to be uniquely associated with a particular individual or device.

(2) Any information that relates to or describes an individual if such information is disclosed in connection with any identifying or referencing information as defined in subparagraph one of this paragraph.

(g) (1) "Retains" means to store or otherwise hold information, whether the information is collected or obtained directly from the subject of the information or from any third party.

(2) "Retains" does not include information that is stored or otherwise held solely for one or more of the following purposes, so long as the information is deleted as soon as it is no longer needed for those purposes:

(A) To perform a service or complete a transaction initiated by or on behalf of the customer, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, or similar services.

(B) To address fraud, security, or technical issues; to protect the disclosing business' rights or property; or to protect customers or the public from illegal activities as required or permitted by law.

(C) To comply with applicable law or regulation or with a court order or other legal process where the business has a good-faith belief that the law, regulation, court order, or legal process requires the information to be stored or held.

(h) "Third party" or "third parties" means one or more of the following:

(1) A business that is a separate legal entity from the business that has disclosed personal information.

(2) A business that does not share common ownership or common corporate control with the business that has disclosed personal information.

(3) A business that does not share a brand name or common branding with the business that has disclosed personal information such that the affiliate relationship is clear to the customer.

5. The provisions of this section are severable. If any provision of this section or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

6. A violation of this section constitutes an injury to a customer. A civil action to recover penalties may be brought by a customer, the attorney general, a district attorney, a city attorney, or a city prosecutor, in a court of competent jurisdiction.

§ 5. This act shall take effect immediately.