SENATE DOCKET, NO. 1856 FILED ON: 2/18/2021

SENATE . . . . . No. 50

The Commonwealth of Massachusetts

PRESENTED BY:

Barry R. Finegold

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act relative to data security and privacy.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
Barry R. Finegold	*Second Essex and Middlesex*	
Linda Dean Campbell	*15th Essex*	*2/26/2021*

SENATE DOCKET, NO. 1856 FILED ON: 2/18/2021

SENATE . . . . . No. 50

By Mr. Finegold, a petition (accompanied by bill, Senate, No. 50) of Barry R. Finegold and Linda Dean Campbell for legislation relative to data security and privacy. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Second General Court
(2021-2022)

An Act relative to data security and privacy.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. Section 1 of Chapter 93H of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by inserting the following definitions:-

"Brokered personal information," one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties: (i) name; (ii) address; (iii) date of birth; (iv) place of birth; (v) mother's maiden name; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; (vii) name or address of a member of the consumer's immediate family or household; (viii) Social Security number or other government-issued identification number; or (ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty. "Brokered

personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public, provided that such information is related to a consumer’s business or profession.

"Business," a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this commonwealth, any other state or commonwealth, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but does not include the commonwealth, an agency of the commonwealth, any political subdivision of the commonwealth, or a vendor acting solely on behalf of, and at the direction of, the commonwealth.

"Consumer," an individual residing in this commonwealth.

“Data broker,” a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. Examples of a direct relationship with a business include if the consumer is a past or present: (i) customer, client, subscriber, user, or registered user of the business's goods or services; (ii) employee, contractor, or agent of the business; (iii) investor in the business; or (iv) donor to the business. The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, shall not qualify the business as a data broker: (i) developing or maintaining third-party e-commerce or application platforms; (ii)

providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier; (iii) providing publicly available information related to a consumer's business or profession; or (iv) providing publicly available information via real-time or near-real-time alert services for health or safety purposes. The phrase "sells or licenses" does not include: (i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or (ii) a sale or license of data that is merely incidental to the business

"Data broker security breach," an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person. "Data broker security breach" shall not include good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure. In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data broker may consider the following factors, among others:

(i) indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information;

(ii) indications that the brokered personal information has been downloaded or copied;

(iii) indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) that the brokered personal information has been made public.

"License," a grant of access to, or distribution of, data by one person to another in exchange for consideration. A use of data for the sole benefit of the data provider, where the data provider maintains control over the use of the data, is not a license.

"Login credentials," a consumer's user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account.

SECTION 2. Section 1 of Chapter 93H of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by inserting after the first three times the phrase “personal information” appears the following:- or login credentials

SECTION 3. Section 1 of Chapter 93H of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by inserting after the first use of the phrase “unauthorized disclosure” the following:-

In determining whether personal information or login credentials have been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:

(i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;

(ii) indications that the information has been downloaded or copied;

(iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) that the information has been made public.

SECTION 4. Section 1 of Chapter 93H of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by adding after the phrase “state-issued identification number” the following:- or individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction

SECTION 5. Section 1 of Chapter 93H of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by adding, after the phrase “access to a resident’s financial account;” the following:

(d) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; or

(e) genetic information;

SECTION 6. Chapter 93H of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by inserting, after Section 6, the following new section:-

Section 7.

(a) Annually, on or before January 31 following a year in which a person meets the definition of data broker as provided in Section 1 of this chapter, a data broker shall:

(1) register with the state secretary;

(2) pay a registration fee of $100.00; and

(3) provide the following information:

(A) the name and primary physical, e-mail, and Internet addresses of the data broker;

(B) if the data broker permits a consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data:

(i) the method for requesting an opt-out;

(ii) if the opt-out applies to only certain activities or sales, which ones; and

(iii) whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(C) a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;

(D) a statement whether the data broker implements a purchaser credentialing process;

(E) the number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(F) where the data broker has actual knowledge that it possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors; and

(G) any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register pursuant to subsection (a) of this section is liable to the commonwealth for:

(1) a civil penalty of $50.00 for each day, not to exceed a total of $10,000.00 for each year, it fails to register pursuant to this section;

(2) an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) other penalties imposed by law.

(c) The attorney general may maintain an action in the Civil Division of the Superior Court to collect the penalties imposed in this section and to seek appropriate injunctive relief.

SECTION 7. Chapter 93H of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by inserting, after Section 6, the following new section:-

Section 8.

a) A person shall not acquire brokered personal information through fraudulent means.

A person shall not acquire or use brokered personal information for the purpose of: (i) stalking or harassing another person; (ii) committing a fraud, including identity theft, financial fraud, or email fraud; or (iii) engaging in unlawful discrimination, including employment discrimination and housing discrimination.

(b) A person who violates a provision of this section shall have committed an unfair and deceptive act in commerce in violation of section 2 of Chapter 93A of the General Laws. The attorney general has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under Chapter 93A.

SECTION 8. On or before March 1, 2022, the attorney general and state secretary shall submit a preliminary report concerning the implementation of this act to the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity.

On or before March 1, 2023, the attorney general and state secretary shall update its preliminary report and provide additional information concerning the implementation of this act to the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity.

SECTION 10. On or before January 1, 2022, the attorney general shall:

(1) review and consider the necessity of additional legislative and regulatory approaches to protecting the data security and privacy of Massachusetts residents, including: a) whether to expand or reduce the scope of regulation to businesses with direct relationships to consumers; b) what additional resources or policies might be needed to support the attorney general's Data Privacy and Security Division.

(2) report its findings and recommendations to the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity.