

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:	
<i>Barry R. Finegold</i>	<i>Second Essex and Middlesex</i>	
<i>Linda Dean Campbell</i>	<i>15th Essex</i>	<i>2/26/2021</i>

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:

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

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

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

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

25 "Consumer," an individual residing in this commonwealth.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

81 (iv) that the information has been made public.

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

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

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

94 (e) genetic information;

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

97 Section 7.

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

100 (1) register with the state secretary;

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

102

103 (3) provide the following information:

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

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

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

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

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

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

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

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

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

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

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

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

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

128 (3) other penalties imposed by law.

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

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

133 Section 8.

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

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

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

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

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

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

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

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