

STATE OF NEW YORK

3657

2017-2018 Regular Sessions

IN SENATE

January 25, 2017

Introduced by Sen. GOLDEN -- read twice and ordered printed, and when printed to be committed to the Committee on Finance

AN ACT to amend the executive law and the general business law, in relation to the New York state online privacy act

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

1 Section 1. Short title. This act may be known and cited as the "New
2 York state online privacy act".

3 § 2. The executive law is amended by adding a new article 10-A to read
4 as follows:

ARTICLE 10-A

OFFICE OF ONLINE PRIVACY PROTECTION AND INTERNET SAFETY

5
6
7 Section 205. Office of online privacy protection and internet safety;
8 created.

9 205-a. Administration.

10 205-b. Online privacy protection and internet safety advisory
11 committee.

12 205-c. Responsibilities.

13 205-d. Construction.

14 205-e. Report.

15 § 205. Office of online privacy protection and internet safety;
16 created. The office of online privacy protection and internet safety is
17 hereby created in the executive department. Its purposes shall be to
18 promote and protect the online privacy and internet safety of personal
19 information of individuals and private businesses by receiving, address-
20 ing, referring, and mediating complaints; developing education and
21 outreach programs, and disseminating model privacy policies; and by
22 coordinating the activities of state agencies performing online privacy
23 protection and internet safety functions.

24 § 205-a. Administration. The office shall be headed by a commissioner
25 of online privacy protection and internet safety who shall be appointed

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

LBD04247-01-7

1 by the governor by and with the advice and consent of the senate. The
2 commissioner shall possess such rights, powers and duties in connection
3 with privacy protection and internet safety as are expressed or reason-
4 ably implied by this article or other applicable laws of this state
5 relating to online privacy and internet safety. The commissioner shall
6 consult with the online privacy protection and internet safety advisory
7 committee in developing policies and programs, and shall coordinate
8 responsibilities concerning security breaches with the data breach
9 group.

10 § 205-b. Online privacy protection and internet safety advisory
11 committee. There is hereby created the online privacy protection and
12 internet safety advisory committee, which shall consist of the following
13 ex-officio members or their designees: the secretary of state, the
14 attorney general, the commissioner of the division of homeland security
15 and emergency services, the commissioner of the office of online privacy
16 protection and internet safety, and the director of the office of infor-
17 mation technology services. In addition, there shall be appointed by the
18 governor by and with the advice and consent of the senate, five persons
19 who have been employed at the level of executive officer in companies in
20 the information technology industry for a period of five years or more,
21 or employed at a senior management level in the areas of privacy compli-
22 ance and internet security for a period of five years or more, or as a
23 privacy compliance officer or other high level position requiring exper-
24 tise in the field of privacy and information technology for such period.
25 The governor shall designate the chair of the advisory committee.

26 Each appointed member of the committee shall be appointed for terms of
27 three years. Any member may be reappointed for two additional terms. The
28 advisory committee shall meet no less than three times each year, or
29 more if its business requires. The advisory committee shall advise the
30 commissioner on matters relating to online privacy and internet safety
31 concerns. Members of the advisory committee shall receive no compen-
32 sation but shall be entitled to actual and necessary traveling and other
33 expenses while engaged in the performance of such member's duties here-
34 under.

35 The committee shall have the following functions, powers and duties:

36 1. To review and comment in the manner and form it deems appropriate
37 on proposed rules, regulations, guidelines, and programs of the office;

38 2. To provide guidance and support to the office in development of
39 policies, programs, and recommendations;

40 3. To make recommendations concerning surveys and reports; and

41 4. To perform such other acts as assigned by the chair of the commit-
42 tee which are necessary or appropriate to carry out the functions of the
43 committee and support the operations of the office.

44 § 205-c. Responsibilities. The office of online privacy protection and
45 internet safety shall:

46 1. Receive complaints: Receive complaints concerning violations of
47 articles thirty-nine-H and thirty-nine-F of the general business law,
48 relating to confidentiality and privacy of e-mail and social media and
49 to data security breaches, and violations of other online privacy-relat-
50 ed laws, attempt to mediate such complaints where appropriate, and refer
51 complaints to the appropriate governmental agency authorized to take
52 appropriate action on such complaints;

53 2. Information and referral: Provide information to individuals and
54 entities about obtaining, using, disclosing, or disposing of online
55 personally identifiable information in a lawful manner, and other such
56 online privacy issues as posting of privacy policies, compliance with

1 federal and state laws and guidelines concerning personal information of
2 minors, and others;

3 3. Education and outreach: Develop and coordinate public and private
4 informational and educational programs and materials to foster and
5 improve public understanding concerning online privacy and internet
6 safety, including programs targeted to minors in consultation with the
7 education department;

8 4. Model policies: develop and disseminate model online privacy poli-
9 cies;

10 5. Training: Assist as requested in the training of local, state, and
11 federal law enforcement agencies and others regarding the prevention of
12 identity theft and other online privacy-related crimes;

13 6. Coordinate security breach procedures: Coordinate effective
14 responses to online security breaches with the data breach group;

15 7. Research: Conduct investigations, research, studies and analyses of
16 matters affecting the online privacy and internet safety; and

17 8. Advise: Advise and make recommendations to the governor concerning
18 online privacy and internet safety.

19 § 205-d. Construction. The authority of the office of online privacy
20 protection and internet safety to adopt regulations under this article
21 shall be limited exclusively to those regulations necessary to implement
22 subdivisions one through six of section two hundred five-c of this arti-
23 cle. Nothing contained herein shall be deemed to apply to the legisla-
24 ture or the judiciary, or except as specifically otherwise provided in
25 law, to a state agency as such term is defined by section one hundred
26 one of the state technology law.

27 § 205-e. Report. The office shall report annually not later than the
28 thirtieth of January each year to the governor, the temporary president
29 of the senate, the speaker of the assembly, the minority leaders of the
30 senate and assembly, and the public beginning in the first calendar year
31 after the effective date of this section concerning: the number of
32 complaints received and the resolutions thereof by category or class of
33 complaint, the numbers of closed cases, and any recommendations concern-
34 ing improvements in online privacy laws and procedures and internet
35 safety.

36 § 3. Section 399-ddd of the general business law, as added by chapter
37 372 of the laws of 2012, is renumbered section 399-dddd.

38 § 4. Subdivision 1 of section 399-dddd, as added by chapter 372 of the
39 laws of 2012 and such section as renumbered by section three of this
40 act, is amended to read as follows:

41 1. As used in this section, "social security account number" shall
42 include the number issued by the federal social security administration
43 and any number derived from such number, or any part of such number.
44 Such term shall not include any number that has been encrypted.

45 § 5. Paragraph (a) of subdivision 1 of section 399-ddd of the general
46 business law, as amended by chapter 371 of the laws of 2012, is amended
47 to read as follows:

48 (a) As used in this section "social security account number" shall
49 include the number issued by the federal social security administration
50 and any number derived from such number, or any part of such number.
51 Such term shall not include any number that has been encrypted.

52 § 6. The general business law is amended by adding a new article 39-H
53 to read as follows:

54 ARTICLE 39-H

55 THE NEW YORK STATE ONLINE ACCOUNTS AND SOCIAL MEDIA PRIVACY ACT
56 Section 900. Short title.

1 901. Definitions.

2 902. Purpose.

3 903. Requests for disclosure by employers.

4 904. Requests for disclosure by an educational institution.

5 905. Prohibited and permitted activities by landlord.

6 906. Construction.

7 907. Remedies.

8 § 900. Short title. This article shall be known and may be cited as
9 the "online media privacy act".

10 § 901. Definitions. As used in this article: 1. "Adverse action"
11 means to discharge, threaten, or otherwise discriminate against an
12 employee in any manner that affects the employee's employment, including
13 compensation, terms, conditions, location, rights, immunities,
14 promotions, or privileges.

15 2. "Educational institution" means a college, university, academy,
16 school district and city school district or other entity offering
17 secondary education, program offering career education or higher educa-
18 tion, as such terms are defined in section two of the education law, and
19 any other institution of higher education, technical college, school,
20 public school, charter school, private school, and any private educa-
21 tional testing service or administrator.

22 3. "Employer" means a person, including the state or a political
23 subdivision of the state, that has one or more workers employed in the
24 same business or business activity, or in or about the same establish-
25 ment, with the right to control and direct the work provided by such
26 workers.

27 4. "Personal internet account" means an online account that is used by
28 an employee or an applicant for employment exclusively for personal
29 communications unrelated to any business purpose of the employer, but
30 does not include an account created, maintained, used, or accessed by an
31 employee or applicant for employment for business related communications
32 or for a business purpose of the employer. As used herein, "personal
33 internet account" also means and includes social media accounts and
34 website or online services, as defined in this section, used by an
35 employee or an applicant for employment exclusively for personal commu-
36 nications unrelated to any business purpose of the employer but not
37 created, maintained, used, or accessed by an employee or applicant for
38 employment for business related communications or for a business purpose
39 of the employer.

40 5. "Social media" means an internet-based service that allows individ-
41 uals to engage in activities which include but are not limited to the
42 following: construct a public or semi-public profile within a bounded
43 system, created by the service; create a list of other users with whom
44 they share a connection within the system; and view and navigate their
45 list of connections and those made by others within the system. Social
46 media includes Facebook, e-mail, and Twitter accounts, and other similar
47 services, and websites and online services which include the activities
48 described in this subdivision, and the digital media contained in those
49 sites, including photos, videos, texts and e-mail messages.

50 6. "Website or online service" means and includes a website, online
51 service, online application, mobile application, electronic service or
52 account, that contains electronic content, including but not limited to
53 videos, still photographs, blogs, video blogs, podcasts, instant and
54 text messages, e-mail, online services or accounts, or website profiles
55 or locations.

1 § 902. Purpose. The purpose of this article is to protect the privacy
2 of online users against inappropriate intrusion.

3 § 903. Requests for disclosure by employers. 1. Except as otherwise
4 provided herein, an employer may not seek disclosure of information
5 related to a personal internet account in any of the following ways. An
6 employer may not:

7 (a) request or require an employee or an applicant for employment to
8 disclose a username and password, or a password, that allows access to
9 the employee's or applicant's personal internet account;

10 (b) request or require an employee or applicant for employment to add
11 the employer or an employment agency to the employee's or applicant's
12 list of contacts associated with a personal internet account;

13 (c) request or require an employee or an applicant for employment to
14 access a personal internet account in the presence of the employer in a
15 manner that enables the employer to observe the contents of the employ-
16 ee's or applicant's personal internet account; or

17 (d) take adverse action, including fail to hire, or otherwise penalize
18 an employee or applicant for employment for failure to disclose informa-
19 tion or failure to take actions specified in this subdivision.

20 2. The foregoing provisions of this section to the contrary notwith-
21 standing, nothing contained herein shall prohibit an employer from doing
22 any of the following:

23 (a) requesting or requiring an employee to disclose a username or
24 password required solely for the purpose of gaining access to an elec-
25 tronic communications device supplied by or paid for in whole or in part
26 by the employer; or an account or service provided by the employer,
27 obtained by virtue of the employee's employment relationship with the
28 employer, or used for the employer's business purposes;

29 (b) disciplining or discharging an employee for transferring the
30 employer's proprietary or confidential information or financial data to
31 an employee's personal internet account without the employer's authori-
32 zation;

33 (c) conducting an investigation or requiring an employee to cooperate
34 in an investigation if there is specific information about activity on
35 the employee's personal internet account, for the purpose of ensuring
36 compliance with applicable laws, regulatory requirements, or prohibi-
37 tions against work-related employee misconduct; or if the employer has
38 specific information about an unauthorized transfer of the employer's
39 proprietary information, confidential information, or financial data to
40 an employee's personal internet account. In such cases an employer may
41 require an employee to share the content that has been reported in order
42 to make a factual determination;

43 (d) restricting or prohibiting an employee's access to certain
44 websites while using an electronic communications device supplied by, or
45 paid for in whole or in part by, the employer or while using an employ-
46 er's network or resources, to the extent permissible under applicable
47 laws; or

48 (e) monitoring, reviewing, accessing, or blocking electronic data
49 stored on an electronic communications device supplied by, or paid for
50 in whole or in part by, the employer, or stored on an employer's
51 network, to the extent permissible under applicable laws.

52 3. Nothing contained herein shall be deemed to prohibit or restrict an
53 employer from complying with a duty to screen employees or applicants
54 before hiring or to monitor or retain employee communications estab-
55 lished under federal law, by a self-regulatory organization under the
56 Securities and Exchange Act of 1934, 15 U.S.C. Sec. 78c(a)(26), or in

1 the course of a law enforcement employment application or law enforce-
2 ment officer conduct investigation performed by a law enforcement agen-
3 cy.

4 4. Nothing contained herein shall be deemed to prohibit or restrict an
5 employer from viewing, accessing, or using information about an employee
6 or applicant that can be obtained without accessing the personal infor-
7 mation account described in subdivision one of this section or that is
8 otherwise available in the public domain.

9 5. Waiver of any provision of subdivision one of this section with
10 respect to access by an employer to the personal internet account of an
11 employee is hereby declared to be contrary to public policy and void and
12 unenforceable, and nothing contained herein shall be deemed to allow an
13 employer to require a violation of such subdivision as a condition of
14 employment or in a contract or oral agreement with an employee or appli-
15 cant for employment.

16 § 904. Requests for disclosure by an educational institution. 1.
17 Except as otherwise provided herein, an educational institution may not
18 seek disclosure of information related to a personal internet account of
19 a student or prospective student in any of the following ways. An educa-
20 tional institution may not:

21 (a) request or require a student or prospective student to disclose a
22 username and password, or a password that allows access to the student's
23 or prospective student's personal internet account;

24 (b) request or require a student or prospective student to add the
25 educational institution to the student's or prospective student's list
26 of contacts associated with a personal internet account;

27 (c) request or require a student or prospective student to access a
28 personal internet account in the presence of the educational institution
29 in a manner that enables the educational institution to observe the
30 contents of the student or prospective student's personal internet
31 account; or

32 (d) expel, suspend, discipline, or otherwise penalize a student or
33 prospective student for failure to disclose information or take actions
34 prohibited in this subdivision.

35 2. The foregoing provisions of this section to the contrary notwith-
36 standing, nothing contained herein shall prohibit an educational insti-
37 tution from requesting or requiring a student to disclose access infor-
38 mation to the educational institution in order for the institution to
39 gain access to or operate an electronic communications device supplied
40 or paid for in whole or in part by the institution or in order for the
41 educational institution to gain access to an account or service provided
42 by the institution, or obtained by virtue of the student's admission to
43 or enrollment in the educational institution; or from viewing, access-
44 ing, or using information about a student or prospective student that
45 can be obtained without accessing information or that is available in
46 the public domain. In addition:

47 (a) Nothing contained in this section shall be deemed to affect the
48 rights and obligations of an educational institution to protect against
49 and investigate alleged student misconduct or violations of applicable
50 laws and regulations.

51 (b) Nothing contained in this section shall be deemed to prohibit such
52 institution from taking any adverse action against a student, prospec-
53 tive student, or student group for any lawful reason.

54 (c) Nothing contained in this section shall be deemed to prohibit a
55 student from voluntarily consenting to such disclosure.

1 § 905. Prohibited and permitted activities by landlord. 1. A landlord
2 may not request disclosure of information related to the personal inter-
3 net account of a tenant or prospective tenant in any of the following
4 ways. A landlord may not:

5 (a) request or require a tenant or prospective tenant to disclose a
6 username and password, or a password that allows access to the tenant or
7 prospective tenant's personal internet account;

8 (b) request or require a tenant or prospective tenant to add the land-
9 lord to the tenant or prospective tenant's list of contacts associated
10 with a personal internet account;

11 (c) request or require a tenant or prospective tenant to access a
12 personal internet account in the presence of the landlord in a manner
13 that enables the landlord to observe the contents of the tenant or
14 prospective tenant's personal internet account; or

15 (d) discriminate against or otherwise penalize a tenant or prospective
16 tenant for failure to disclose information or take actions specified in
17 this subdivision.

18 2. The foregoing provisions of this section to the contrary notwith-
19 standing, nothing contained herein shall prohibit a landlord from view-
20 ing, accessing, or using information about a tenant or prospective
21 tenant that can be obtained without accessing information or that is
22 available in the public domain.

23 § 906. Construction. Nothing contained in this article shall be deemed
24 to create a duty for an employer, educational institution, or landlord
25 to search or monitor the activity of a personal internet account or to
26 create a liability for an employer, educational institution, or landlord
27 for any failure to request or require that an employee, applicant for
28 employment, student, prospective student, tenant, or prospective tenant
29 grant access to, allow observation of, or disclose information that
30 allows access to or observation of a personal internet account of the
31 employee, applicant for employment, student, prospective student,
32 tenant, or prospective tenant.

33 § 907. Remedies. 1. The attorney general may bring a civil cause of
34 action against an employer, educational institution, or landlord in a
35 court of competent jurisdiction on behalf of a citizen aggrieved by a
36 violation of this article.

37 2. Any employer, educational institution, or landlord who violates any
38 provision of this article shall be subject to a civil penalty not to
39 exceed five hundred dollars for each such violation.

40 § 7. Subdivision 2 of section 390-b of the general business law is
41 amended by adding a new paragraph (e) to read as follows:

42 (e) The term "social media" means an internet-based service that
43 allows individuals to engage in activities which include but are not
44 limited to the following: construct a public or semi-public profile
45 within a bounded system, created by the service; create a list of other
46 users with whom they share a connection within the system; and view and
47 navigate their list of connections and those made by others within the
48 system. Social media includes Facebook, e-mail, and Twitter accounts,
49 and other similar services, and websites and online services which
50 include the activities described in this paragraph, and the digital
51 media contained in those sites, including photos, videos, texts and
52 e-mail messages.

53 § 8. Subdivision 3 of section 390-b of the general business law, as
54 amended by chapter 414 of the laws of 2006, is amended to read as
55 follows:

1 3. It is unlawful for any person, by means of a web page, electronic
2 message, social media, or other use of the internet to solicit, request
3 or collect identifying information by deceptively representing himself
4 or herself, either directly or by implication, to be a business or a
5 governmental entity and doing so without the authority or approval of
6 such business or such governmental entity, or by deceptively represent-
7 ing himself or herself to be another person without the authority or
8 approval of such other person, and doing so with the intent to obtain
9 financial information or information that would allow such individual to
10 obtain financial information from one or more other persons or busi-
11 nesses.

12 § 9. Subdivision 1 of section 899-aa of the general business law is
13 amended by adding a new paragraph (e) to read as follows:

14 (e) "Data breach group" means the entity created by section eight
15 hundred ninety-nine-bb of this article.

16 § 10. Paragraph (a) of subdivision 8 of section 899-aa of the general
17 business law, as amended by section 6 of part N of chapter 55 of the
18 laws of 2013, is amended to read as follows:

19 (a) In the event that any New York residents are to be notified, the
20 person or business shall notify the [~~state attorney general, the depart-~~
21 ~~ment of state and the division of state police~~] office of online privacy
22 protection and internet security, which shall immediately notify the
23 data breach group as to the timing, content and distribution of the
24 notices and approximate number of affected persons. Such notice shall be
25 made without delaying notice to affected New York residents.

26 § 11. The general business law is amended by adding a new section
27 899-bb to read as follows:

28 § 899-bb. Data breach group. 1. The data breach group is hereby
29 created, to consist of the attorney general, the secretary of state, the
30 commissioner of the division of homeland security and emergency
31 services, the chief information officer of the office of information
32 technology services, the superintendent of the division of state police,
33 and the commissioner of the office of online privacy and internet safe-
34 ty, or their designees. Its purposes shall be: to receive, evaluate, and
35 act on any report of a breach of the security of the system made pursu-
36 ant to section eight hundred ninety-nine-aa of this article, or to
37 section two hundred eight of the state technology law; to establish
38 priorities and responsibilities pursuant to law among its members so as
39 to promote efficiency in responses to violations of internet privacy and
40 avoid duplication, overlap, and unnecessary paperwork, including multi-
41 ple filings by for-profit and not-for-profit businesses and entities,
42 and other governmental entities; to establish where appropriate simpli-
43 fied reporting forms and procedures in accordance with law, and a single
44 reporting intake system; to maintain database records and reports
45 concerning security breaches; to establish cooperative working relation-
46 ships with federal, state, and local police and investigators; and to
47 insure appropriate and timely public notification of security breaches
48 that includes information sufficient for individuals to take appropriate
49 steps to protect themselves.

50 2. The data breach group shall be chaired by the commissioner of the
51 division of homeland security and emergency services with administrative
52 services provided by the office of online privacy and internet safety.
53 The data breach group shall meet on a monthly basis, or more often if
54 their work requires, provided that attendance at such meetings may be by
55 telephonic or video conference, as the group shall decide.

§ 12. The general business law is amended by adding a new article 39-I to read as follows:

ARTICLE 39-I
REQUIREMENTS FOR USE AND DESTRUCTION OF ONLINE PERSONAL AND
PRIVATE INFORMATION

Section 910. Short title.

911. Definitions.

912. Purpose.

913. Application.

914. Liability for failure to comply.

§ 910. Short title. This article shall be known and may be cited as the "New York state online privacy act".

§ 911. Definitions. As used in this article, the following terms shall have the following meanings: 1. "Personal information" and "private information" shall have the same meanings as in paragraphs (a) and (b) of subdivision one of section eight hundred ninety-nine-aa of this chapter.

2. "Destruction of information" means actions taken by the provider of a personal internet account to render the personal information and private information of a user unreadable and incapable of reconstruction.

3. "Privacy policy" means a policy concerning the privacy of personally identifiable information collected by an operator through its website or online service that meets the Fair Information Practice Principles guidelines established by the Federal Trade Commission, or any successor thereto in the form of guidelines or law.

4. "Personal internet account" has the same meaning as such term is defined in subdivision four of section nine hundred one of this chapter.

§ 912. Purpose. The purpose of this article is to safeguard the personal and private information of users of the internet by requiring that operators of services offering personal internet accounts establish privacy policies that meet federal standards, disclose such policies to users of their services, and disclose their processes for destruction of information.

§ 913. Application. 1. The provider of a service which offers personal internet accounts shall promulgate, post, and implement a privacy policy as defined herein.

2. A provider of a service which offers a personal internet account shall provide for destruction of information of a user who cancels such account and shall notify users about its policy and processes regarding such destruction.

§ 914. Liability for failure to comply. A provider of a service which offers a personal internet account which is negligent in failing to comply with any requirement imposed pursuant to this article for posting of a privacy policy or destruction of information is liable to that user in an amount equal to the sum of any actual damages sustained as a result of such failure, and in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court; provided however that solely with respect to an alleged failure to post a privacy policy, or to post timely or to post all the information required, or to post accurate information, an operator may assert as a complete defense in any action in law or equity that it thereafter provided such information to all affected users within thirty days of the date that operator knew of such failure. The rights and remedies

1 available under this section are cumulative to each other and to any
2 other rights and remedies available under law.

3 § 13. Any other provision of any other law to the contrary notwith-
4 standing, the director of the division of the budget, the office of
5 state comptroller, and the commissioner of the department of civil
6 service shall develop a plan providing for the orderly transition of
7 such employees and functions as shall be necessary and appropriate to
8 the operations and functioning of the office of online privacy
9 protection and internet safety created by this act. Such plan shall be
10 completed and submitted to the legislature not later than 180 days after
11 this act shall have become law, but in no case later than February first
12 of the succeeding calendar year, at which time such agencies and agen-
13 cies affected by the plan shall begin implementation of the plan. Any
14 other provision of any other law to the contrary notwithstanding, and in
15 accordance with section 4 of the state finance law, the comptroller is
16 hereby authorized and directed to transfer, at the request of the direc-
17 tor of the budget and pursuant to such plan, such funds as shall be
18 necessary and appropriate for the creation and operation of the office
19 of online privacy and internet safety, but in no case shall such trans-
20 fers total more than 10 million dollars within the fiscal year in which
21 the office shall have been created.

22 § 14. Severability. If any clause, sentence, paragraph, subdivision,
23 section or part of this act shall be adjudged by a court of competent
24 jurisdiction to be invalid, such judgment shall not affect, impair or
25 invalidate the remainder thereof, but shall be confined in its operation
26 to the clause, sentence, paragraph, subdivision, section or part of this
27 act directly involved in the controversy in which such judgment shall
28 have been rendered.

29 § 15. This act shall take effect on the first of January next succeed-
30 ing the date on which it shall have become a law.