STATE OF NEW YORK

7521

2017-2018 Regular Sessions

IN ASSEMBLY

April 28, 2017

Introduced by M. of A. SEAWRIGHT -- read once and referred to the Committee on Governmental Operations

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:

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

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

ARTICLE 10-A

OFFICE OF ONLINE PRIVACY PROTECTION AND INTERNET SAFETY

Section 205. Office of online privacy protection and internet safety; created.
205-a. Administration.
205-b. Online privacy protection and internet safety advisory committee.
205-c. Responsibilities.
205-d. Construction.
205-e. Report.

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

§ 205-a. Administration. The office shall be headed by a commissioner 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

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

§ 205-b. Online privacy protection and internet safety advisory committee. There is hereby created the online privacy protection and internet safety advisory committee, which shall consist of the following ex-officio members or their designees: the secretary of state, the attorney general, the commissioner of the division of homeland security and emergency services, the commissioner of the office of online privacy protection and internet safety, and the director of the office of information technology services. In addition, there shall be appointed by the governor by and with the advice and consent of the senate, five persons who have been employed at the level of executive officer in companies in the information technology industry for a period of five years or more, or employed at a senior management level in the areas of privacy compliance and internet security for a period of five years or more, or as a privacy compliance officer or other high level position requiring expertise in the field of privacy and information technology for such period. The governor shall designate the chair of the advisory committee.

Each appointed member of the committee shall be appointed for terms of three years. Any member may be reappointed for two additional terms. The advisory committee shall meet no less than three times each year, or more if its business requires. The advisory committee shall advise the commissioner on matters relating to online privacy and internet safety concerns. Members of the advisory committee shall receive no compensation but shall be entitled to actual and necessary traveling and other expenses while engaged in the performance of such member's duties hereunder.

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

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

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

3. To make recommendations concerning surveys and reports; and

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

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

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

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

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

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

4. Model policies: develop and disseminate model online privacy policies;

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

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

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

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

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

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

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

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

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

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

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

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

ARTICLE 39-H

THE NEW YORK STATE ONLINE ACCOUNTS AND SOCIAL MEDIA PRIVACY ACT

Section 900. Short title.

901. Definitions.
902. Purpose.
903. Requests for disclosure by employers.
904. Requests for disclosure by an educational institution.
905. Prohibited and permitted activities by landlord.
906. Construction.
907. Remedies.

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

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

2. "Educational institution" means a college, university, academy, school district and city school district or other entity offering secondary education, program offering career education or higher education, as such terms are defined in section two of the education law, and any other institution of higher education, technical college, school, public school, charter school, private school, and any private educational testing service or administrator.

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

4. "Personal internet account" means an online account that is used by an employee or an applicant for employment exclusively for personal communications unrelated to any business purpose of the employer, but does not include an account created, maintained, used, or accessed by an employee or applicant for employment for business related communications or for a business purpose of the employer. As used herein, "personal internet account" also means and includes social media accounts and website or online services, as defined in this section, used by an employee or an applicant for employment exclusively for personal communications unrelated to any business purpose of the employer but not created, maintained, used, or accessed by an employee or applicant for employment for business related communications or for a business purpose of the employer.

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

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

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

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

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

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

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

(d) take adverse action, including fail to hire, or otherwise penalize an employee or applicant for employment for failure to disclose information or failure to take actions specified in this subdivision.

2. The foregoing provisions of this section to the contrary notwithstanding, nothing contained herein shall prohibit an employer from doing any of the following:

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

(b) disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal internet account without the employer's authorization;

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

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

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

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

the course of a law enforcement employment application or law enforcement officer conduct investigation performed by a law enforcement agency.

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

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

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

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

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

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

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

2. The foregoing provisions of this section to the contrary notwithstanding, nothing contained herein shall prohibit an educational institution from requesting or requiring a student to disclose access information to the educational institution in order for the institution to gain access to or operate an electronic communications device supplied or paid for in whole or in part by the institution or in order for the educational institution to gain access to an account or service provided by the institution, or obtained by virtue of the student's admission to or enrollment in the educational institution; or from viewing, accessing, or using information about a student or prospective student that can be obtained without accessing information or that is available in the public domain. In addition:

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

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

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

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

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

(b) request or require a tenant or prospective tenant to add the landlord to the tenant or prospective tenant's list of contacts associated with a personal internet account;

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

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

2. The foregoing provisions of this section to the contrary notwithstanding, nothing contained herein shall prohibit a landlord from viewing, accessing, or using information about a tenant or prospective tenant that can be obtained without accessing information or that is available in the public domain.

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

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

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

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

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

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

3. It is unlawful for any person, by means of a web page, electronic message, **social media,** or other use of the internet to solicit, request or collect identifying information by deceptively representing himself or herself, either directly or by implication, to be a business or a governmental entity and doing so without the authority or approval of such business or such governmental entity**, or by deceptively representing himself or herself to be another person without the authority or approval of such other person, and doing so with the intent to obtain financial information or information that would allow such individual to obtain financial information from one or more other persons or businesses**.

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

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

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

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

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

§ 899-bb. Data breach group. 1. The data breach group is hereby created, to consist of the attorney general, the secretary of state, the commissioner of the division of homeland security and emergency services, the chief information officer of the office of information technology services, the superintendent of the division of state police, and the commissioner of the office of online privacy and internet safety, or their designees. Its purposes shall be: to receive, evaluate, and act on any report of a breach of the security of the system made pursuant to section eight hundred ninety-nine-aa of this article, or to section two hundred eight of the state technology law; to establish priorities and responsibilities pursuant to law among its members so as to promote efficiency in responses to violations of internet privacy and avoid duplication, overlap, and unnecessary paperwork, including multiple filings by for-profit and not-for-profit businesses and entities, and other governmental entities; to establish where appropriate simplified reporting forms and procedures in accordance with law, and a single reporting intake system; to maintain database records and reports concerning security breaches; to establish cooperative working relationships with federal, state, and local police and investigators; and to insure appropriate and timely public notification of security breaches that includes information sufficient for individuals to take appropriate steps to protect themselves.

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

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

§ 13. Any other provision of any other law to the contrary notwithstanding, the director of the division of the budget, the office of state comptroller, and the commissioner of the department of civil service shall develop a plan providing for the orderly transition of such employees and functions as shall be necessary and appropriate to the operations and functioning of the office of online privacy protection and internet safety created by this act. Such plan shall be completed and submitted to the legislature not later than 180 days after this act shall have become law, but in no case later than February first of the succeeding calendar year, at which time such agencies and agencies affected by the plan shall begin implementation of the plan. Any other provision of any other law to the contrary notwithstanding, and in accordance with section 4 of the state finance law, the comptroller is hereby authorized and directed to transfer, at the request of the director of the budget and pursuant to such plan, such funds as shall be necessary and appropriate for the creation and operation of the office of online privacy and internet safety, but in no case shall such transfers total more than 10 million dollars within the fiscal year in which the office shall have been created.

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

§ 15. This act shall take effect on the first of January next succeeding the date on which it shall have become a law.