HOUSE BILL 846
Committee Substitute Favorable 5/15/13
Third Edition Engrossed 5/16/13

Short Title: Job and Education Privacy Act. (Public)

Sponsors:

Referred to:

April 11, 2013

A BILL TO BE ENTITLED

AN ACT TO ENACT THE JOB AND EDUCATION PRIVACY ACT TO PREVENT EMPLOYERS AND COLLEGES FROM REQUIRING INDIVIDUALS TO DISCLOSE ACCESS INFORMATION FOR SOCIAL MEDIA AND PERSONAL ELECTRONIC MAIL ACCOUNTS.

The General Assembly of North Carolina enacts:

SECTION 1. The General Statutes are amended by adding a new Chapter to read:

"**Chapter 99F. Job and Education Privacy Act.**

"**§ 99F-1. Title.**

This Chapter shall be known and may be cited as the "Job and Education Privacy Act."

"**§ 99F-2. Definitions.**

The following definitions apply in this Article:

(1) Academic institution. – A public or private institution of higher education or institution of postsecondary education. The term includes an agent, representative, or designee of the academic institution.

(2) Access information. – A user name, a password, log-in information, or any other security information that protects access to a personal electronic account.

(3) Applicant. – A prospective student applying for admission into an academic institution or a prospective employee applying for employment with an employer.

(4) Electronic communication device. – A cellular telephone, personal digital assistant, electronic device with mobile data access, laptop computer, pager, broadband personal communication device whether mobile or desktop, two-way messaging device, electronic game, or portable computing device.

(5) Employer. – This State; a political subdivision of this State; or a person engaged in a business, an industry, a profession, a trade, or other enterprise in the State. The term includes any agent, representative, or designee of the employer.

(6) Personal electronic account. – An account created via an electronic medium or service that allows users to create, share, or view user-generated content, including uploading or downloading videos or still photographs, blogs, video blogs, podcasts, messages, electronic mail, Internet Web site profiles or locations, or any other electronic information. The term does not include an

account that is opened on behalf of, or owned by, an academic institution or an employer.

(7) Publicly accessible communication. – Information that may be obtained without required access information or that is available in the public domain.

(8) Social networking site. – An Internet-based, personalized, privacy-protected Web site or application whether free or commercial that allows users to construct a private or semiprivate profile site within a bounded system, create a list of other system users who are granted reciprocal access to the individual's profile site, send and receive e-mail, and share personal content, communications, and contacts.

(9) Student. – A person which at all relevant times is admitted into the academic institution.

"**§ 99F-3. Academic institutions; prohibited act.**

(a) An academic institution shall not request or require that a student or applicant grant access to, allow observation of, or disclose information that allows access to or observation of the student's personal electronic account.

(b) An academic institution shall not require or request that a student or applicant log onto a social networking site, electronic mail account, or any other Internet site or application by way of an electronic communication device in the presence of an agent of the institution so as to provide the institution access to the student's or applicant's social networking site profile or account.

(c) No academic institution shall monitor or track a student's or applicant's personal electronic communication device by installation of software upon the device or by remotely tracking the device by using intercept technology.

(d) An academic institution shall not request or require a student or applicant to add an agent of the academic institution to his or her personal social networking site profile or account.

(e) An academic institution is prohibited from accessing a student's or applicant's social networking site profile or account indirectly through any other person who is a social networking contact of the student or applicant.

"**§ 99F-4. Academic institutions; wrongful dismissal or refusal to admit.**

(a) An academic institution may not discipline, dismiss, or otherwise penalize or threaten to discipline, dismiss, or otherwise penalize a student for refusing to disclose any information protected by G.S. 99F-3.

(b) It is unlawful for an academic institution to fail or refuse to admit any applicant as a result of the applicant's refusal to disclose any information specified in G.S. 99F-3.

"**§ 99F-5. Employers; prohibited acts.**

(a) An employer shall not require or request that an employee or applicant disclose a username and password, or a password that allows access to the employee's or applicant's personal Internet account.

(b) An employer shall not request or require that an employee or applicant log onto a social networking site, electronic mail account, or any other Internet site or application by way of an electronic communications device in the presence of the employer so as to provide the employer access to the employee's or applicant's social networking site profile or account.

(c) No employer shall monitor or track an employee's or applicant's personal electronic communication device by installation of software upon the employee's or applicant's personal device or by remotely tracking that device by using intercept technology.

(d) An employer shall not compel an employee or applicant to add the employer or its representative to his or her personal social networking site profile or account.

"**§ 99F-6. Employers; wrongful discharge or refusal to hire.**

(a) An employer may not discharge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee for the employee's refusal to disclose any information protected by G.S. 99F-5.

(b) It is unlawful for an employer to fail or refuse to hire any applicant as a result of the applicant's refusal to disclose any information specified in G.S. 99F-5.

"**§ 99F-7. Nonretaliation.**

It is unlawful to take retaliatory action against any individual for that individual's refusal to disclose information protected by this Chapter.

"**§ 99F-8. Exceptions.**

This Chapter does not:

(1) Preclude access to publicly accessible communications appearing on a social networking site.

(2) Apply to an academic institution conducting an investigation or inquiry (i) pursuant to an academic institution's threat assessment policy or protocol, (ii) having a reasonable, articulable suspicion of criminal activity, or (iii) pursuant to established complaint review procedures.

(3) Prohibit employers in the financial services industry, who are subject to the laws and regulations of State or federal financial regulators, from conducting internal investigations into employee wrongdoing or complying with the supervision requirements of those regulators.

"**§ 99F-9. Permitted actions by an employer.**

(a) This Chapter does not prohibit an employer from doing any of the following:

(1) Requesting or requiring an employee to disclose a username or password required only to gain access to either of the following:

a. An electronic communications device supplied by or paid for by the employer.

b. 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.

(2) 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.

(3) Conducting an investigation or requiring an employee to cooperate in an investigation in any of the following:

a. When 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.

b. When 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.

(4) Restricting or prohibiting an employee's access to certain Web sites 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, in accordance with State and federal law to the extent permissible under applicable laws.

(5) 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, in accordance with State and federal law to the extent permissible under applicable laws.

(b) Conducting an investigation or requiring an employee to cooperate in an investigation as specified in subdivision (3) of subsection (a) of this section includes requiring the employee to share the content that has been reported in order to make a factual determination.

(c) This Chapter does not prohibit or restrict an employer from complying with a duty to screen employees or applicants before hiring or to monitor to retain employee communications that is established under federal law, by a self-regulatory organization under the Securities and Exchange Act of 1934, 15 U.S.C. § 78c(a)(26), or in the course of a law enforcement.

"**§ 99F-10. Chapter does not create duties.**

(a) This Chapter does not create a duty for an employer to search or monitor the activity of a personal Internet account.

(b) An employer is not liable under this Chapter for failure to request or require that an employee or applicant for employment grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal Internet account.

"**§ 99F-11. Remedy.**

(a) The Attorney General may bring a civil cause of action against an employer in a court of competent jurisdiction on behalf of a citizen aggrieved by a violation of this Chapter.

(b) In an action brought under subsection (a) of this section, if the court finds a violation of this Chapter, the court shall award the State not more than five hundred dollars ($500.00) per violation."

SECTION 2. This act becomes effective October 1, 2013.