

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2013

H

1

HOUSE BILL 846

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

Sponsors: Representatives D. Hall and Saine (Primary Sponsors).

For a complete list of Sponsors, refer to the North Carolina General Assembly Web Site.

Referred to: Judiciary Subcommittee A.

April 11, 2013

1 A BILL TO BE ENTITLED
2 AN ACT TO ENACT THE JOB AND EDUCATION PRIVACY ACT TO PREVENT
3 EMPLOYERS AND COLLEGES FROM REQUIRING INDIVIDUALS TO DISCLOSE
4 ACCESS INFORMATION FOR SOCIAL MEDIA AND PERSONAL ELECTRONIC
5 MAIL ACCOUNTS.

6 The General Assembly of North Carolina enacts:

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

8 **"Chapter 99F.**

9 **"Job and Education Privacy Act.**

10 **"§ 99F-1. Title.**

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

12 **"§ 99F-2. Definitions.**

13 The following definitions apply in this Article:

- 14 (1) Academic institution. – A public or private institution of higher education or
15 institution of postsecondary education. The term includes an agent,
16 representative, or designee of the academic institution.
- 17 (2) Access information. – A user name, a password, log-in information, or any
18 other security information that protects access to a personal electronic
19 account.
- 20 (3) Applicant. – A prospective student applying for admission into an academic
21 institution or a prospective employee applying for employment with an
22 employer.
- 23 (4) Electronic communication device. – A cell telephone, personal digital
24 assistant, electronic device with mobile data access, laptop computer, pager,
25 broadband personal communication device whether mobile or desktop,
26 two-way messaging device, electronic game, or portable computing device.
- 27 (5) Employer. – This State; a political subdivision of this State; or a person
28 engaged in a business, an industry, a profession, a trade, or other enterprise
29 in the State. The term includes any agent, representative, or designee of the
30 employer.
- 31 (6) Personal electronic account. – An account created via an electronic medium
32 or service that allows users to create, share, or view user-generated content,
33 including uploading or downloading videos or still photographs, blogs, video
34 blogs, podcasts, messages, electronic mail, Internet Web site profiles or
35 locations, or any other electronic information. The term does not include an



* H 8 4 6 - V - 1 *

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

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

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

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

13 **"§ 99F-3. Academic institutions; prohibited act.**

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

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

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

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

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

30 **"§ 99F-4. Academic institutions; wrongful dismissal or refusal to admit.**

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

34 (b) It is unlawful for an academic institution to fail or refuse to admit any applicant as a
35 result of the applicant's refusal to disclose any information specified in G.S. 99F-2.

36 **"§ 99F-5. Employers; prohibited acts.**

37 (a) An employer shall not require or request that an employee or applicant grant access
38 to, allow observation of, or disclose information that allows access to or observation of, the
39 employee's or applicant's personal electronic account.

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

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

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

49 (e) An employer is prohibited from accessing an employee's or applicant's social
50 networking site profile or account indirectly through any other person who is a social
51 networking contact of the employee or applicant.

1 **"§ 99F-6. Employers; wrongful discharge or refusal to hire.**

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

5 (b) It is unlawful for an employer to fail or refuse to hire any applicant as a result of the
6 applicant's refusal to disclose any information specified in G.S. 99F-4.

7 **"§ 99F-7. Nonretaliation.**

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

10 **"§ 99F-8. Exceptions.**

11 This Chapter does not:

- 12 (1) Preclude access to publically accessible communications appearing on a
13 social networking site.
- 14 (2) Apply to investigations conducted by an academic institution's public safety
15 department or police agency having a reasonable articulable suspicion of
16 criminal activity or to an investigation, inquiry, or determination conducted
17 pursuant to an academic institution's threat assessment policy or protocol.
- 18 (3) Prohibit employers in the financial services industry, who are subject to the
19 laws and regulations of State or federal financial regulators, from conducting
20 internal investigations into employee wrongdoing or complying with the
21 supervision requirements of those regulators.
- 22 (4) Prohibit an employer from requiring that an employee disclose any user
23 name, password, or other means for accessing (i) nonpersonal accounts or
24 (ii) services that provide access to the employer's internal computer or
25 information systems.
- 26 (5) Limit the right of an employer to create, maintain, and enforce lawful
27 workplace policies governing the use of the electronic equipment of the
28 employer, including policies concerning Internet use, social networking Web
29 site use, and electronic mail use involving the equipment."

30 **SECTION 2.** This act is effective when it becomes law.