

GENERAL ASSEMBLY OF NORTH CAROLINA  
SESSION 2013

H

2

HOUSE BILL 846  
Committee Substitute Favorable 5/15/13

Short Title: Job and Education Privacy Act.

(Public)

Sponsors:

Referred to:

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. Job and Education Privacy Act.**

9 **§ 99F-1. Title.**

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

11 **§ 99F-2. Definitions.**

12 The following definitions apply in this Article:

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



- 1           (7) Publicly accessible communication. – Information that may be obtained  
2 without required access information or that is available in the public domain.  
3           (8) Social networking site. – An Internet-based, personalized, privacy-protected  
4 Web site or application whether free or commercial that allows users to  
5 construct a private or semiprivate profile site within a bounded system,  
6 create a list of other system users who are granted reciprocal access to the  
7 individual's profile site, send and receive e-mail, and share personal content,  
8 communications, and contacts.  
9           (9) Student. – A person which at all relevant times is admitted into the academic  
10 institution.

11 **"§ 99F-3. Academic institutions; prohibited act.**

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

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

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

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

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

28 **"§ 99F-4. Academic institutions; wrongful dismissal or refusal to admit.**

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

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

34 **"§ 99F-5. Employers; prohibited acts.**

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

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

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

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

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

50 **"§ 99F-6. Employers; wrongful discharge or refusal to hire.**

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

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

6     "**§ 99F-7. Nonretaliation.**

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

9     "**§ 99F-8. Exceptions.**

10       This Chapter does not:

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

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