

Regular Session, 2014

HOUSE BILL NO. 340

BY REPRESENTATIVE JAMES

PRIVACY/COMPUTERS: Creates the Personal Online Account Privacy Protection Act

1 AN ACT

2 To enact Chapter 28 of Title 51 of the Louisiana Revised Statutes of 1950, to be comprised
3 of R.S. 51:1951 through 1955, relative to Internet privacy; to prohibit employers and
4 educational institutions from requesting or requiring certain individuals to disclose
5 information that allows access to or observation of personal online accounts; to
6 prohibit employers and educational institutions from taking certain actions for failure
7 to disclose information that allows access to personal online accounts; to provide for
8 certain individuals to self-disclose information that allows access to or observation
9 of personal online accounts; to limit liability for failure to search or monitor the
10 activity of an individual's personal online account; to provide for exceptions; and to
11 provide for related matters.

12 Be it enacted by the Legislature of Louisiana:

13 Section 1. Chapter 28 of Title 51 of the Louisiana Revised Statutes of 1950,
14 comprised of R.S. 51:1951 through 1955, is hereby enacted to read as follows:

15 CHAPTER 28. PERSONAL ONLINE ACCOUNT PRIVACY PROTECTION ACT

16 §1951. Title

17 This Chapter shall be known and may be cited as the "Personal Online
18 Account Privacy Protection Act".

19 §1952. Definitions

20 As used in this Chapter, the terms defined in this Section have the meanings
21 herein given to them, except where the context expressly indicates otherwise:

1 (1) "Educational institution" means a public or private educational institution
2 or a separate school or department of a public or private educational institution and
3 includes but is not limited to the following:

4 (a) A university, college, or junior college.

5 (b) An academy.

6 (c) An elementary or secondary school.

7 (d) An extension course.

8 (e) A kindergarten.

9 (f) A nursery school.

10 (g) A school system, school district, or intermediate school district.

11 (h) A business, nursing, professional, secretarial, technical, or vocational
12 school.

13 (i) A public or private educational testing service or administrator.

14 (j) An agent of an educational institution.

15 (2) "Employer" means a person, including a unit of state or local
16 government, engaged in a business, industry, profession, trade, or other enterprise
17 in this state and includes an agent, representative, or designee of the employer.

18 (3) "Personal online account" means an online account that the employee,
19 applicant for employment, student, or prospective student uses exclusively for
20 personal communications unrelated to any business purpose of the employer or
21 educational institution. A personal online account does not extend to any account
22 or profile created, serviced, maintained, used, or accessed by a current employee,
23 applicant for employment, student, or prospective student for either business
24 purposes of the employer or educational institution or to engage in business-related
25 communications.

26 (4) "Electronic communications device" means any device that uses
27 electronic signals to create, transmit, and receive information, including a computer,
28 telephone, personal digital assistant, or other similar device.

1 §1953. Employers; prohibited activities; exceptions

2 A. An employer shall not do any of the following:

3 (1) Request or require an employee or applicant for employment to disclose
4 any username, password, or other authentication information that allows access to
5 the employee's or applicant's personal online account.

6 (2) Discharge, discipline, fail to hire, or otherwise penalize or threaten to
7 penalize an employee or applicant for employment for failure to disclose any
8 information specified in this Subsection.

9 B. An employer shall not be prohibited from doing any of the following:

10 (1) Requesting or requiring an employee or applicant for employment to
11 disclose any username, password, or other authentication information to the
12 employer to gain access to or operate any of the following:

13 (a) An electronic communications device paid for or supplied in whole or in
14 part by the employer.

15 (b) An account or service provided by the employer, obtained by virtue of
16 the employee's or applicant's relationship with the employer, or used for the
17 employer's business purposes.

18 (2) Disciplining or discharging an employee for transferring the employer's
19 proprietary or confidential information or financial data to an employee's personal
20 online account without the employer's authorization.

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

23 (a) If there is specific information about activity on the employee's personal
24 online account, for the purpose of ensuring compliance with applicable laws,
25 regulatory requirements, or prohibitions against work-related employee misconduct.

26 (b) If the employer has specific information about an unauthorized transfer
27 of the employer's proprietary information, confidential information, or financial data
28 to an employee's or applicant's personal online account.

1 (4) Conducting an investigation or requiring an employee or applicant to
2 cooperate in an investigation as specified in this Subsection, including requiring the
3 employee or applicant to share the content that has been reported in order to make
4 a factual determination, without obtaining the username and password to the
5 employee's or applicant's personal online account.

6 (5) Restricting or prohibiting an employee's or applicant's access to certain
7 websites while using an electronic communications device paid for or supplied in
8 whole or in part by the employer or while using an employer's network or resources,
9 in accordance with state and federal law.

10 C. If through the use of an electronic device or program that monitors an
11 employer's network or the use of an employer-provided device, an employer
12 inadvertently receives an employee's or applicant's username, password, or other
13 authentication information, the employer shall not be liable for having the
14 information, but may not use the information to access the employee's or applicant's
15 personal online account.

16 D. An employer shall not be prohibited or restricted from complying with
17 a duty to screen employees or applicants prior to hiring or to monitor or retain
18 employee communications that are established pursuant to state or federal law, rules
19 or regulations, case law, or rules of self-regulatory organizations.

20 E. An employer shall not be prohibited or restricted from viewing, accessing,
21 or utilizing information about an employee or applicant that can be obtained without
22 the information specified in Paragraph (A)(1) of this Section or that is available in
23 the public domain.

24 F. An employer shall not be prohibited or restricted from requiring an
25 employee to provide a personal e-mail address in order to facilitate communication
26 with the employee in the event the employer's e-mail system fails.

27 G. Nothing in this Section shall be construed to prohibit or restrict an
28 employee or applicant for employment from self-disclosing any username, password,

1 or other authentication information to the employer that allows access to the
2 employee's or applicant's personal online account.

3 §1954. Educational institutions; prohibited activities; exceptions

4 A. An educational institution shall not do any of the following:

5 (1) Request or require a student or prospective student to disclose any
6 username, password, or other authentication information that allows access to the
7 student's or prospective student's personal online account.

8 (2) Expel, discipline, fail to admit, or otherwise penalize or threaten to
9 penalize a student or prospective student for failure to disclose any information
10 specified in this Subsection.

11 B. An educational institution shall not be prohibited from requesting or
12 requiring a student or prospective student to disclose any username, password, or
13 other authentication information to the educational institution to gain access to or
14 operate any of the following:

15 (1) An electronic communications device paid for or supplied in whole or
16 in part by the educational institution, except where the device has been provided to
17 the student or prospective student with the intent to permanently transfer ownership
18 of the device to the student or prospective student.

19 (2) An account or service provided by the educational institution that is
20 either obtained by virtue of the student's or prospective student's admission to the
21 educational institution or used by the student or prospective student for educational
22 purposes.

23 C. An educational institution shall not be prohibited from doing any of the
24 following:

25 (1) Viewing, accessing, or utilizing information about a student or
26 prospective student that can be obtained without the information specified in
27 Paragraph (A)(1) of this Section or that is available in the public domain.

28 (2) Restricting or prohibiting a student's or prospective student's access to
29 certain websites while using an electronic communications device paid for or

1 supplied in whole or in part by the educational institution or while using an
 2 educational institution's network or resources, in accordance with state and federal
 3 law, except where the device has been provided to the student or prospective student
 4 with the intent to permanently transfer the ownership of the device to the student or
 5 prospective student.

6 D. Nothing in this Section shall be construed to prohibit or restrict a student
 7 or prospective student from self-disclosing any username, password, or other
 8 authentication information to the educational institution that allows access to the
 9 student's or prospective student's personal online account.

10 §1955. No duty to monitor; liability

11 A. This Chapter shall not create a duty for an employer or educational
 12 institution to search or monitor the activity of an individual's personal online
 13 account.

14 B. An employer or educational institution shall not be liable under this
 15 Chapter for failure to request or require an employee, a student, an applicant for
 16 employment, or a prospective student to disclose information that allows access to
 17 the employee's, student's, applicant's, or prospective student's personal online
 18 account.

DIGEST

The digest printed below was prepared by House Legislative Services. It constitutes no part of the legislative instrument. The keyword, one-liner, abstract, and digest do not constitute part of the law or proof or indicia of legislative intent. [R.S. 1:13(B) and 24:177(E)]

James

HB No. 340

Abstract: Creates the Personal Online Account Privacy Protection Act.

Proposed law shall be known and may be cited as the "Personal Online Account Privacy Protection Act".

Proposed law defines "educational institution" as a public or private educational institution or a separate school or department of a public or private educational institution and includes but is not limited to the following:

- (1) A university, college, or junior college.
- (2) An academy.

- (3) An elementary or secondary school.
- (4) An extension course.
- (5) A kindergarten.
- (6) A nursery school.
- (7) A school system, school district, or intermediate school district.
- (8) A business, nursing, professional, secretarial, technical, or vocational school.
- (9) A public educational testing service or administrator.
- (10) An agent of an educational institution.

Proposed law defines "employer" as a person, including a unit of state or local government, engaged in a business, industry, profession, trade, or other enterprise in this state and includes an agent, representative, or designee of the employer.

Proposed law defines "personal online account" as an online account that is used by an employee, applicant, student, or prospective student exclusively for personal communications unrelated to any business purpose of the employer or educational institution.

Proposed law provides that a "personal online account" does not extend to any account or profile created, serviced, maintained, used, or accessed by a current or prospective employee, applicant, student, or prospective student for either business purposes of the employer or educational institution or to engage in business-related communications.

Proposed law defines "electronic communications device" as any device using electronic signals to create, transmit, and receive information, including a computer, telephone, personal digital assistant, or other similar device.

Proposed law prohibits an employer from doing any of the following:

- (1) Requesting or requiring an employee or an applicant for employment to disclose information that allows access to the employee's or applicant's personal online account.
- (2) Discharging, disciplining, failing to hire, or otherwise penalizing or threatening to penalize an employee or applicant for employment for failure to disclose information that allows access to or observation of the employee's or applicant's personal online account.

Proposed law provides that an employer is not prohibited from requesting or requiring an employee or applicant for employment to disclose access information to the employer to gain access to or operate any of the following:

- (1) An electronic communications device paid for or supplied in whole or in part by the employer.
- (2) An account or service provided by the employer, obtained by virtue of the employee's or applicant's relationship with the employer, or used for the employer's business purposes.

Proposed law provides that an employer is not prohibited from disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal online account without the employer's authorization.

Proposed law provides that an employer is not prohibited from conducting an investigation or requiring an employee or applicant to cooperate in an investigation in any of the following circumstances:

- (1) If there is specific information about activity on the employee's personal online account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct.
- (2) 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 or applicant's personal online account.

Proposed law provides that an employer is not prohibited from conducting an investigation or requiring an employee or applicant to cooperate in an investigation, including requiring the employee or applicant to share the content that has been reported in order to make a factual determination, without obtaining the username and password to the employee's or applicant's personal online account.

Proposed law provides that an employer is not prohibited from restricting or prohibiting an employee's or applicant's access to certain websites while using an electronic communications device paid for or supplied in whole or in part by the employer or while using an employer's network or resources, in accordance with state and federal law.

Proposed law provides that an employer is not liable for the inadvertent receipt of personal online account access information through the use of any electronic device or program monitoring the employer's network or employer provided device; however, the employer may not use the information to access the employee's or applicant's personal online account.

Proposed law provides that an employer is not prohibited or restricted from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under state or federal law.

Proposed law provides that an employer is not prohibited or restricted from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain.

Proposed law provides that an employer is not prohibited or restricted from requiring an employee to provide a personal e-mail address in order to facilitate communication with the employee, in the event the employer's e-mail system fails.

Proposed law provides that no provision of proposed law shall be construed to prohibit or restrict an employee or applicant for employment from self-disclosing any username, password, or other authentication information to the employer allowing access to the employee's or applicant's personal online account.

Proposed law prohibits an educational institution from doing any of the following:

- (1) Requesting or requiring a student or prospective student to disclose information that allows access to the student's or prospective student's personal online account.
- (2) Expelling, disciplining, failing to admit, or otherwise penalizing or threatening to penalize a student or prospective student for failure to disclose information that allows access to the student's or prospective student's personal online account.

Proposed law provides that an educational institution is not prohibited from requesting or requiring a student or prospective student to disclose access information to the educational institution to gain access to or operate any of the following:

- (1) An electronic communications device paid for or supplied in whole or in part by the educational institution, except where the device has been provided to the student or prospective student with the intent to permanently transfer the ownership of the device to the student or prospective student.
- (2) An account or service provided by the educational institution that is either obtained by virtue of the student's or prospective student's admission to the educational institution or used by the student or prospective student for educational purposes.

Proposed law provides that an educational institution is not prohibited from viewing, accessing, or utilizing information about a student or prospective student that can be obtained without any required access information or that is available in the public domain.

Proposed law provides that an educational institution is not prohibited from restricting or prohibiting a student's or prospective student's access to certain websites while the student or prospective student uses an electronic communications device paid for or supplied in whole or in part by the educational institution or while the student or prospective student uses an educational institution's network, unless the device has been provided with the intent to permanently transfer ownership of the device to the student or prospective student.

Proposed law provides that no provision of proposed law shall be construed to prohibit or restrict an employee or applicant for employment from self-disclosing any username, password, or other authentication information to the employer allowing access to the employee's or applicant's personal online account.

Proposed law does not create a duty for an employer or educational institution to search or monitor the activity of an individual's personal online account.

Proposed law provides that an employer or educational institution is not liable for failure to request or require an employee, a student, an applicant for employment, or a prospective student to disclose information that allows access to the employee's, applicant's, student's, or prospective student's personal online account.

(Adds R.S. 51:1951-1955)

Summary of Amendments Adopted by House

Committee Amendments Proposed by House Committee on Commerce to the original bill.

1. Added a provision to include that an employer is not prohibited or restricted from requiring an employee to provide a personal e-mail address to facilitate communication with the employee, in the event the employer's e-mail system fails.
2. Made technical change.