

HOUSE BILL No. 5623

May 10, 2012, Introduced by Rep. Opsommer and referred to the Committee on Energy and Technology.

A bill to prohibit employers and educational institutions from requiring certain individuals to disclose information that allows access to certain personal data storage accounts; to prohibit employers and educational institutions from taking certain actions for failure to disclose information that allows access to certain personal data storage accounts; and to provide remedies.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

1 Sec. 1. This act shall be known and may be cited as the
2 "personal data storage privacy act".

3 Sec. 2. As used in this act:

4 (a) "Access information" means user name, password, login
5 information, or other security feature that regulates control or
6 access to a personal data storage account or its contents.

1 (b) "Educational institution" means a public or private
2 educational institution, a public or private educational testing
3 service or administrator, or a separate school or department of a
4 public or private educational institution, and includes an academy;
5 elementary or secondary school; extension course; kindergarten;
6 nursery school; school system; school district; intermediate school
7 district; business, nursing, professional, secretarial, technical,
8 or vocational school; and an agent of an educational institution.
9 Educational institution shall be construed broadly to include
10 public and private institutions of higher education to the greatest
11 extent consistent with constitutional limitations.

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

16 (d) "Friending" means an act by which a personal data storage
17 account user grants full or partial access to other entities by
18 adding them to a list that regulates control or access to the
19 personal data storage account.

20 (e) "Personal data storage account" means an electronic or
21 digital repository of personal data or information that can be
22 directly or remotely accessed via a computer, smart-phone,
23 telephone, or other device and includes, but is not limited to, a
24 social networking account, banking account, shopping account,
25 electronic mail account, texting account, internet access account,
26 contact list, address book, or cloud-based storage of personal
27 information.

1 (f) "Shoulder surfing" means seeing or accessing data in a
2 personal data storage account after authorization from the account
3 user but without obtaining any user name, password, login
4 information, or other security feature from the account user.

5 Sec. 3. An employer shall not do any of the following:

6 (a) Request an employee or an applicant for employment to
7 disclose access information associated with the employee's or
8 applicant's personal data storage account.

9 (b) Request an employee or applicant for employment to
10 authorize full or partial access to the employee's or applicant's
11 personal data storage account through friending or shoulder
12 surfing.

13 (c) Subject to section 7, request an employee or applicant for
14 employment to waive any right under this act or to indemnify or
15 hold the employer harmless for a violation of this act.

16 (d) Discharge, discipline, fail to hire, or otherwise
17 discriminate against an employee or applicant for employment for
18 his or her lack of a personal data storage account, failure to
19 authorize friending or shoulder surfing, or failure to disclose
20 access information for the employee's or applicant's personal data
21 storage account.

22 Sec. 4. An educational institution shall not do any of the
23 following:

24 (a) Request a student or prospective student to disclose
25 access information associated with the student's or prospective
26 student's personal data storage account.

27 (b) Request a student or prospective student to authorize full

1 or partial access to the student's or prospective student's
2 personal data storage account through friending or shoulder
3 surfing.

4 (c) Request a student or prospective student to waive any
5 right under this act or to indemnify or hold the educational
6 institution harmless for a violation of this act.

7 (d) Discharge, discipline, fail to admit, or otherwise
8 discriminate against a student or prospective student for his or
9 her lack of a personal data storage account, failure to authorize
10 friending or shoulder surfing, or failure to disclose access
11 information associated with the student's or prospective student's
12 personal data storage account.

13 Sec. 5. (1) An employer or educational institution, or an
14 agent of an employer or educational institution, that violates
15 section 3 or 4 is guilty of a misdemeanor punishable by
16 imprisonment for not more than 93 days or a fine of not more than
17 \$1,000.00, or both.

18 (2) An individual who is the subject of a violation of this
19 act may bring a civil action for a violation of section 3 or 4 and
20 may recover actual damages or \$5,000.00, whichever is greater, and
21 reasonable attorney fees and court costs. Except for good cause,
22 not later than 60 days before filing a civil action, the individual
23 shall make a written demand of the alleged violator for the greater
24 of the amount of the individual's actual damages or \$5,000.00. The
25 written demand shall include reasonable documentation of the
26 violation and, if applicable, of the actual damages. The written
27 demand and documentation shall either be served in the manner

1 provided by law for service of process in civil actions or mailed
2 by certified mail with sufficient postage affixed and addressed to
3 the alleged violator at his or her residence, principal office, or
4 place of business. An action under this subsection may be brought
5 in the circuit court for the county where the alleged violation
6 occurred or for the county where the person against whom the civil
7 complaint is filed resides or has his or her principal place of
8 business.

9 Sec. 6. This act does not prohibit an employer from making a
10 decision not to hire an applicant for employment or from
11 disciplining or terminating an employee based on information
12 ordinarily available to the public or that is obtained through an
13 otherwise authorized background check.

14 Sec. 7. This act does not prohibit a law enforcement agency
15 from doing any of the following:

16 (a) Establishing a social media policy that prohibits its
17 employees from posting information on the internet that may
18 endanger the public, endanger law enforcement officers, jeopardize
19 criminal investigations, or otherwise run counter to the law
20 enforcement agency's mission or purpose.

21 (b) Entering into an agreement with its employee bargaining
22 representative regarding the circumstances under which the employer
23 can be granted temporary shoulder-surfing access to personal social
24 media accounts as a condition of employment.