



**ASSEMBLY SUBSTITUTE AMENDMENT 1,
TO ASSEMBLY BILL 218**

August 19, 2013 - Offered by Representatives SARGENT and BIES.

1 **AN ACT** *to amend* 111.322 (2m) (a) and 111.322 (2m) (b); and *to create* 106.54
2 (10), 111.91 (2) (im) and 995.55 of the statutes; **relating to:** employer access to,
3 and observation of, the personal Internet accounts of employees and applicants
4 for employment; educational institution access to, and observation of, the
5 personal Internet accounts of students and prospective students; landlord
6 access to, and observation of, the personal Internet accounts of tenants and
7 prospective tenants; and providing a penalty.

Analysis by the Legislative Reference Bureau

Current law does not regulate employer access to, or observation of, the personal Internet accounts of employees and applicants for employment; educational institution access to, or observation of, the personal Internet accounts of students and prospective students; or landlord access to, or observation of, the personal Internet accounts of tenants and prospective tenants.

This substitute amendment prohibits an employer, educational institution, or landlord from:

1. Requesting or requiring an employee, applicant for employment, student, prospective student, tenant, or prospective tenant to disclose a user name and

password or any other security information (access information) that protects access to an Internet-based account that is created and used exclusively for purposes of personal communications (personal Internet account) of the employee, applicant, student, prospective student, tenant, or prospective tenant or to otherwise grant access to or allow observation of that account.

2. Discharging, expelling, suspending, disciplining, or otherwise penalizing or discriminating against an employee, student, tenant, or prospective tenant for exercising the right under the substitute amendment to refuse to disclose that access information or to otherwise grant that access or allow that observation, opposing such a practice, filing a complaint or attempting to enforce that right, or testifying or assisting in any action or proceeding to enforce that right.

3. Refusing to hire an applicant for employment or to admit a prospective student because the applicant or prospective student refused to disclose that access information or to otherwise grant that access or allow that observation.

The substitute amendment, however, permits an employer, educational institution, or landlord to view, access, or use information about an employee, applicant for employment, student, prospective student, tenant, or prospective tenant that can be obtained without access information or that is available from the public domain.

The substitute amendment also permits an employer or educational institution to request or require an employee or student to disclose access information to the employer or educational institution in order for the employer or educational institution to gain access to or operate an electronic communications device supplied or paid for in whole or in part by the employer or educational institution or in order for the employer or educational institution to gain access to an account or service provided by the employer or educational institution, obtained by virtue of the employment relationship or admission to the educational institution, or used for business or educational purposes.

The substitute amendment, in addition, permits an employer to do any of the following:

1. Discharge or discipline an employee for transferring the employer's proprietary or confidential information or financial data to the employee's personal Internet account without the employer's authorization.

2. Conduct an investigation or require an employee to cooperate in an investigation of any alleged unauthorized transfer of the employer's proprietary or confidential information or financial data to the employee's personal Internet account or of any other alleged employment-related misconduct, violation of the law, or violation of the employer's work rules as specified in an employee handbook, provided that in conducting or requiring cooperation in such an investigation the employer may require the employee to grant access or allow observation of the employee's personal Internet account, but may not require the employee to disclose access information for that account.

3. Restrict or prohibit an employee's access to certain Internet sites while using an electronic communications device supplied or paid for in whole or in part by the

employer (employer-provided electronic communications device) or while using the employer's network or other resources.

4. Comply with a duty to screen applicants for employment prior to hiring or a duty to monitor or retain employee communications that is established under state or federal law, rules, or regulations or the rules of a self-regulatory organization, as defined under the federal Securities Exchange Act of 1934 (self-regulatory organization).

5. Requesting or requiring an employee to disclose the employee's personal electronic mail address.

In addition, with respect to an employer, the substitute amendment provides: 1) that the prohibition created under the substitute amendment does not apply to a personal Internet account or an electronic communications device of an employee engaged in providing financial services who uses the account or device to conduct the business of an employer that is subject to the content, supervision, and retention requirements imposed by federal securities laws and regulations or by the rules of a self-regulatory organization; and 2) that an employer that inadvertently obtains access information for an employee's personal Internet account through the use of an electronic device or program that monitors the employer's network or through an employer-provided electronic communications device is not liable under the substitute amendment for possessing that access information so long as the employer does not use that access information to access the employee's personal Internet account.

Finally, the substitute amendment provides that an employer, educational institution, or landlord does not have a duty to search or monitor the activity of any personal Internet account and is not liable for any failure to request or require access to or observation of a personal Internet account of an employee, applicant for employment, student, prospective student, tenant, or prospective tenant.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

1 **SECTION 1.** 106.54 (10) of the statutes is created to read:

2 106.54 (10) (a) The division shall receive complaints under s. 995.55 (6) (b) and
3 shall process the complaints in the same manner as employment discrimination
4 complaints are processed under s. 111.39.

5 (b) The division shall receive complaints under s. 995.55 (6) (c) and shall
6 process the complaints in the same manner as housing discrimination complaints
7 are processed under s. 106.50.

1 **SECTION 2.** 111.322 (2m) (a) of the statutes is amended to read:

2 111.322 **(2m)** (a) The individual files a complaint or attempts to enforce any
3 right under s. 103.02, 103.10, 103.13, 103.28, 103.32, 103.34, 103.455, 103.50,
4 104.12, ~~106.04~~, 109.03, 109.07, 109.075, ~~or 146.997, or 995.55~~, or ss. 101.58 to
5 101.599 or 103.64 to 103.82.

6 **SECTION 3.** 111.322 (2m) (b) of the statutes is amended to read:

7 111.322 **(2m)** (b) The individual testifies or assists in any action or proceeding
8 held under or to enforce any right under s. 103.02, 103.10, 103.13, 103.28, 103.32,
9 103.34, 103.455, 103.50, 104.12, ~~106.04~~, 109.03, 109.07, 109.075, ~~or 146.997, or~~
10 995.55, or ss. 101.58 to 101.599 or 103.64 to 103.82.

11 **SECTION 4.** 111.91 (2) (im) of the statutes is created to read:

12 111.91 **(2)** (im) Employer access to the social networking Internet site of an
13 employee that provides fewer rights and remedies to employees than are provided
14 under s. 995.55.

15 **SECTION 5.** 995.55 of the statutes is created to read:

16 **995.55 Internet privacy protection. (1) DEFINITIONS.** In this section:

17 (a) “Access information” means a user name and password or any other security
18 information that protects access to a personal Internet account.

19 (b) “Educational institution” means an institution of higher education, as
20 defined in s. 108.02 (18); a technical college established under s. 38.02; a school, as
21 defined in s. 38.50 (11) (a) 2.; a public school, as described in s. 115.01 (1); a charter
22 school, as defined in s. 115.001 (1); a private school, as defined in s. 115.001 (3r); or
23 a private educational testing service or administrator.

24 (c) “Employer” means any person engaging in any activity, enterprise, or
25 business employing at least one individual. “Employer” includes the state, its

1 political subdivisions, and any office, department, independent agency, authority,
2 institution, association, society, or other body in state or local government created or
3 authorized to be created by the constitution or any law, including the legislature and
4 the courts.

5 (d) "Personal Internet account" means an Internet-based account that is
6 created and used by an individual exclusively for purposes of personal
7 communications.

8 **(2) RESTRICTIONS ON EMPLOYER ACCESS TO PERSONAL INTERNET ACCOUNTS.** (a)
9 Except as provided in pars. (b), (c), and (d), no employer may do any of the following:

10 1. Request or require an employee or applicant for employment to disclose
11 access information for the personal Internet account of the employee or applicant or
12 to otherwise grant access to or allow observation of that account.

13 2. Discharge or otherwise discriminate against an employee for exercising the
14 right under subd. 1. to refuse to disclose access information for, grant access to, or
15 allow observation of the employee's personal Internet account, opposing a practice
16 prohibited under subd. 1., filing a complaint or attempting to enforce any right under
17 subd. 1., or testifying or assisting in any action or proceeding to enforce any right
18 under subd. 1.

19 3. Refuse to hire an applicant for employment because the applicant refused
20 to disclose access information for, grant access to, or allow observation of the
21 applicant's personal Internet account.

22 (b) Paragraph (a) does not prohibit an employer from doing any of the following:

23 1. Requesting or requiring an employee to disclose access information to the
24 employer in order for the employer to gain access to or operate an electronic
25 communications device supplied or paid for in whole or in part by the employer or in

1 order for the employer to gain access to an account or service provided by the
2 employer, obtained by virtue of the employee’s employment relationship with the
3 employer, or used for the employer’s business purposes.

4 2. Discharging or disciplining an employee for transferring the employer’s
5 proprietary or confidential information or financial data to the employee’s personal
6 Internet account without the employer’s authorization.

7 3. Subject to this subdivision, conducting an investigation or requiring an
8 employee to cooperate in an investigation of any alleged unauthorized transfer of the
9 employer’s proprietary or confidential information or financial data to the
10 employee’s personal Internet account, if the employer has reasonable cause to
11 believe that such a transfer has occurred, or of any other alleged
12 employment-related misconduct, violation of the law, or violation of the employer’s
13 work rules as specified in an employee handbook, if the employer has reasonable
14 cause to believe that activity on the employee’s personal Internet account relating
15 to that misconduct or violation has occurred. In conducting an investigation or
16 requiring an employee to cooperate in an investigation under this subdivision, an
17 employer may require an employee to grant access to or allow observation of the
18 employee’s personal Internet account, but may not require the employee to disclose
19 access information for that account.

20 4. Restricting or prohibiting an employee’s access to certain Internet sites while
21 using an electronic communications device supplied or paid for in whole or in part
22 by the employer or while using the employer’s network or other resources.

23 5. Complying with a duty to screen applicants for employment prior to hiring
24 or a duty to monitor or retain employee communications that is established under

1 state or federal laws, rules, or regulations or the rules of a self-regulatory
2 organization, as defined in 15 USC 78c (a) (26).

3 6. Viewing, accessing, or using information about an employee or applicant for
4 employment that can be obtained without access information or that is available in
5 the public domain.

6 7. Requesting or requiring an employee to disclose the employee's personal
7 electronic mail address.

8 (c) Paragraph (a) does not apply to a personal Internet account or an electronic
9 communications device of an employee engaged in providing financial services who
10 uses the account or device to conduct the business of an employer that is subject to
11 the content, supervision, and retention requirements imposed by federal securities
12 laws and regulations or by the rules of a self-regulatory organization, as defined in
13 15 USC 78c (a) (26).

14 (d) An employer that inadvertently obtains access information for an
15 employee's personal Internet account through the use of an electronic device or
16 program that monitors the employer's network or through an electronic
17 communications device supplied or paid for in whole or in part by the employer is not
18 liable under par. (a) for possessing that access information so long as the employer
19 does not use that access information to access the employee's personal Internet
20 account.

21 **(3) RESTRICTIONS ON EDUCATIONAL INSTITUTION ACCESS TO PERSONAL INTERNET**
22 **ACCOUNTS.** (a) Except as provided in par. (b), no educational institution may do any
23 of the following:

1 1. Request or require a student or prospective student to disclose access
2 information for the personal Internet account of the student or prospective student
3 or to otherwise grant access to or allow observation of that account.

4 2. Expel, suspend, discipline, or otherwise penalize any student for exercising
5 the right under subd. 1. to refuse to disclose access information for, grant access to,
6 or allow observation of the student's personal Internet account, opposing a practice
7 prohibited under subd. 1., filing a complaint or attempting to enforce any right under
8 subd. 1., or testifying or assisting in any action or proceeding to enforce any right
9 under subd. 1.

10 3. Refuse to admit a prospective student because the prospective student
11 refused to disclose access information for, grant access to, or allow observation of the
12 prospective student's personal Internet account.

13 (b) Paragraph (a) does not prohibit an educational institution from doing any
14 of the following:

15 1. Requesting or requiring a student to disclose access information to the
16 educational institution in order for the institution to gain access to or operate an
17 electronic communications device supplied or paid for in whole or in part by the
18 institution or in order for the educational institution to gain access to an account or
19 service provided by the institution, obtained by virtue of the student's admission to
20 the educational institution, or used for educational purposes.

21 2. Viewing, accessing, or using information about a student or prospective
22 student that can be obtained without access information or that is available in the
23 public domain.

24 **(4) RESTRICTIONS ON LANDLORD ACCESS TO PERSONAL INTERNET ACCOUNTS.** (a)
25 Except as provided in par. (b), no landlord may do any of the following:

1 1. Request or require a tenant or prospective tenant to disclose access
2 information for the personal Internet account of the tenant or prospective tenant or
3 to otherwise grant access to or allow observation of that account.

4 2. Discriminate in a manner described in s. 106.50 (2) against a tenant or
5 prospective tenant for exercising the right under subd. 1. to refuse to disclose access
6 information for, grant access to, or allow observation of the personal Internet account
7 of the tenant or prospective tenant, opposing a practice prohibited under subd. 1.,
8 filing a complaint or attempting to enforce any right under subd. 1., or testifying or
9 assisting in any action or proceeding to enforce any right under subd. 1.

10 (b) Paragraph (a) does not prohibit a landlord from viewing, accessing, or using
11 information about a tenant or prospective tenant that can be obtained without access
12 information or that is available in the public domain.

13 **(5) NO DUTY TO MONITOR.** (a) Nothing in this section creates a duty for an
14 employer, educational institution, or landlord to search or monitor the activity of any
15 personal Internet account.

16 (b) An employer, educational institution, or landlord is not liable under this
17 section for any failure to request or require that an employee, applicant for
18 employment, student, prospective student, tenant, or prospective tenant grant
19 access to, allow observation of, or disclose information that allows access to or
20 observation of a personal Internet account of the employee, applicant for
21 employment, student, prospective student, tenant, or prospective tenant.

22 **(6) ENFORCEMENT.** (a) Any person who violates sub. (2) (a), (3) (a), or (4) (a) may
23 be required to forfeit not more than \$1,000.

24 (b) An employee who is discharged or otherwise discriminated against in
25 violation of sub. (2) (a) 2., an applicant for employment who is not hired in violation

1 of sub. (2) (a) 3., a student who is expelled, suspended, disciplined, or otherwise
2 penalized in violation of sub. (3) (a) 2., or a prospective student who is not admitted
3 in violation of sub. (3) (a) 3., may file a complaint with the department, and the
4 department shall process the complaint in the same manner as employment
5 discrimination complaints are processed under s. 111.39. If the department finds
6 that a violation of sub. (2) (a) 2. or 3. or (3) (a) 2. or 3. has been committed, the
7 department may order the employer or educational institution to take such action
8 authorized under s. 111.39 as will remedy the violation. Section 111.322 (2m) applies
9 to a discharge or other discriminatory act arising in connection with any proceeding
10 under this paragraph.

11 (c) A tenant or prospective tenant who is discriminated against in violation of
12 sub. (4) (a) 2. may file a complaint with the department, and the department shall
13 process the complaint in the same manner as housing discrimination complaints are
14 processed under s. 106.50. If the department finds that a violation of sub. (4) (a) 2.
15 has been committed, the department may order the landlord to take such action
16 authorized under s. 106.50 as will remedy the violation.

17 **SECTION 6. Initial applicability.**

18 (1) COLLECTIVE BARGAINING AGREEMENT. This act first applies to an employee
19 who is affected by a collective bargaining agreement that contains provisions
20 inconsistent with this act on the day on which the collective bargaining agreement
21 expires or is extended, modified, or renewed, whichever occurs first.

22 (END)