AN ACT to amend 111.322 (2m) (a) and 111.322 (2m) (b); and to create 106.54 (10), 111.91 (2) (im) and 995.55 of the statutes; relating to: employer access to, and observation of, the personal Internet accounts of employees and applicants for employment; educational institution access to, and observation of, the personal Internet accounts of students and prospective students; landlord access to, and observation of, the personal Internet accounts of tenants and 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, or 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 bill prohibits an employer, educational institution, or landlord from: 1) requesting an employee, applicant for employment, student, prospective student, tenant, or prospective tenant to grant access to, allow observation of, or disclose information that allows access to or observation of the personal Internet account of the employee, applicant, student, prospective student, tenant, or prospective tenant; and 2) discharging, expelling, suspending, disciplining, or otherwise penalizing or
SENATE BILL 223

discriminating against any person for exercising the right to refuse such a request, 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.

The bill, 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 bill 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 paid for in whole or in part by the employer or educational institution or to gain access to an account or service that is provided by the employer or educational institution, that the employee or student obtained by virtue of the employment relationship or admission to the educational institution, or that is used for business or educational purposes.

The bill, 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 or violation of the law.

3. Restrict or prohibit an employee’s access to certain Internet sites while using an electronic communications device paid for in whole or in part by the employer or while using the employer’s network or other resources.

4. Monitor, review, or access electronic data that is stored on an electronic communications device paid for in whole or in part by the employer or electronic data that is traveling through or stored on the employer’s network.

5. Comply with a duty to screen applicants for employment prior to hiring that is established under state or federal law or by a self–regulatory organization, as defined under the federal Securities and Exchange Act of 1934 (self–regulatory organization).

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

In addition, with respect to an employer, the bill provides that the prohibition created under the bill 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 a self–regulatory organization.

Finally, the bill 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 that an employer, educational institution, or landlord 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.

For purposes of the bill: 1) “access information” means a user name and password, login information, or any other security information that protects access to a personal Internet account; 2) “educational institution” means an institution of higher education, a technical college, a proprietary school, a public school, a charter school, a private school, or a private educational testing service or administrator; 3) “employer” includes the state; and 4) “personal Internet account” means an account created and used exclusively for personal purposes within a bounded system established by an Internet-based service that requires a user to input or store access information via an electronic device in order to view, create, use, or edit the user’s account information, profile, display, communications, or stored data.

For further information see the state and local fiscal estimate, which will be printed as an appendix to this bill.

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

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

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

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

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

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

SECTION 3. 111.322 (2m) (b) of the statutes is amended to read:
111.322 (2m) (b) The individual testifies or assists in any action or proceeding
held under or to enforce any right under s. 103.02, 103.10, 103.13, 103.28, 103.32,
103.34, 103.455, 103.50, 104.12, 106.04, 109.03, 109.07, 109.075, or 146.997, 995.55,
or ss. 101.58 to 101.599 or 103.64 to 103.82.

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

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

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

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

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

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

(c) “Employer” means any person engaging in any activity, enterprise, or
business employing at least one individual. “Employer” includes the state, its
political subdivisions, and any office, department, independent agency, authority,
institution, association, society, or other body in state or local government created or
authorized to be created by the constitution or any law, including the legislature and
the courts.

(d) “Personal Internet account” means an account created and used exclusively
for personal purposes within a bounded system established by an Internet–based
service that requires a user to input or store access information via an electronic
device in order to view, create, use, or edit the user’s account information, profile,
display, communications, or stored data.

(2) Restrictions on employer access to personal Internet accounts. (a) Except as provided in pars. (b) and (c), no employer may do any of the following:

1. Request an employee or applicant for employment to grant access to, allow
observation of, or disclose information that allows access to or observation of the
personal Internet account of the employee or applicant.

2. Discharge or otherwise discriminate against any person for exercising the
right to refuse a request under subd. 1., opposing a practice prohibited under subd.
1., filing a complaint or attempting to enforce any right under subd. 1., or testifying
or assisting in any action or proceeding to enforce any right under subd. 1.

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

1. Requesting or requiring an employee to disclose access information to the
employer in order for the employer to gain access to or operate an electronic
communications device paid for in whole or in part by the employer or to gain access
to an account or service that is provided by the employer, that the employee obtained
by virtue of the employee’s employment relationship with the employer, or that is
used for the employer’s business purposes.

2. Discharging or disciplining 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.

3. Conducting an investigation or requiring 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, if the employer has reasonable cause to believe that such a transfer has occurred, or of any other alleged employment-related misconduct or violation of the law, if the employer has reasonable cause to believe that activity on the employee's personal Internet account relating to that misconduct or violation of the law has occurred.

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

5. Monitoring, reviewing, or accessing electronic data that is stored on an electronic communications device paid for in whole or in part by the employer or electronic data that is traveling through or stored on the employer’s network.

6. Complying with a duty to screen applicants for employment prior to hiring that is established under state or federal law or by a self-regulatory organization, as defined in 15 USC 78c (a) (26).

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

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

(c) Paragraph (a) 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 a self-regulatory organization, as defined in 15 USC 78c (a) (26).
SENATE BILL 223

(3) Restrictions on educational institution access to personal Internet accounts. (a) Except as provided in par. (b), no educational institution may do any of the following:

1. Request a student or prospective student to grant access to, allow observation of, or disclose information that allows access to or observation of the personal Internet account of the student or prospective student.

2. Expel, suspend, discipline, or otherwise penalize any student or prospective student for exercising the right to refuse a request under subd. 1., opposing a practice prohibited under subd. 1., filing a complaint or attempting to enforce any right under subd. 1., or testifying or assisting in any action or proceeding to enforce any right under subd. 1.

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

1. Requesting or requiring a student to disclose access information to the educational institution in order for the institution to gain access to or operate an electronic communications device paid for in whole or in part by the institution or to gain access to an account or service that is provided by the institution, that the student obtained by virtue of the student’s admission to the educational institution, or that is used by the student for educational purposes.

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

(4) Restrictions on landlord access to personal Internet accounts. (a) Except as provided in par. (b), no landlord may do any of the following:
1. Request a tenant or prospective tenant to grant access to, allow observation of, or disclose information that allows access to or observation of the personal Internet account of the tenant or prospective tenant.

2. Discriminate in a manner described in s. 106.50 (2) against a tenant or prospective tenant for exercising the right to refuse a request under subd. 1., opposing a practice prohibited under subd. 1., filing a complaint or attempting to enforce any right under subd. 1., or testifying or assisting in any action or proceeding to enforce any right under subd. 1.

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

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

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

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

(b) An employee or applicant for employment who is discharged or otherwise discriminated against in violation of sub. (2) (a) 2. or a student or prospective student who is expelled, suspended, disciplined, or otherwise penalized in violation of sub.
(3) (a) 2. may file a complaint with the department, and the department shall process
the complaint in the same manner as employment discrimination complaints are
processed under s. 111.39. If the department finds that a violation of sub. (2) (a) 2.
or (3) (a) 2. has been committed, the department may order the employer or
educational institution to take such action authorized under s. 111.39 as will remedy
the violation. Section 111.322 (2m) applies to a discharge or other discriminatory act
arising in connection with any proceeding under this paragraph.

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

SECTION 6. Initial applicability.

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