HB 814

RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.

LAB, JUD

HB814 (?)

Submit Testimony

Measure Title:	RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.
Report Title:	Only Privacy; Employees; Students
Description:	Adopts uniform laws on protecting the online accounts of employees and students from employers and educational institutions, respectively.
Companion:	
Package:	None
Current Referral:	LAB, JUD
Introducer(s):	LOPRESTI, QUINLAN, TODD, Gates, Holt, Nakamura

Sort by Date		Status Text
1/23/2017	H	Pending introduction.
1/25/2017	H	Pass First Reading
1/27/2017	H	Referred to LAB, JUD, referral sheet 4
2/13/2017	H	Bill scheduled to be heard by LAB on Thursday, 02-16-17 10:00AM in House conference room 309.

S = Senate | **H** = House | **D** = Data Systems | **$** = Appropriation measure | **ConAm** = Constitutional Amendment
Some of the above items require Adobe Acrobat Reader. Please visit Adobe's download page for detailed instructions.

HOUSE OF REPRESENTATIVES
TWENTY-NINTH LEGISLATURE, 2017
STATE OF HAWAII

H.B. NO. 814

A BILL FOR AN ACT

RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. The Hawaii Revised Statutes is amended by adding a new chapter to be appropriately designated and to read as follows:

"CHAPTER

THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

§ -1 Short title. This chapter may be cited as the uniform employee and student online privacy protection act.

§ -2 Definitions. As used in this chapter:

"Content" means information, other than login information, that is contained in a protected personal online account, accessible to the account holder, and not publicly available.

"Educational institution" means a person that provides students at the postsecondary level an organized program of study or training which is academic, technical, trade-oriented, or preparatory for gaining employment and for which the person gives academic credit. The term includes:

(1) A public or private institution; and

(2) An agent or designee of the educational institution.

"Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

"Employee" means an individual who provides services or labor to an employer in exchange for salary, wages, or the equivalent or, for an unpaid intern, academic credit or occupational experience. The term includes:

(1) A prospective employee who:

(A) Has expressed to the employer an interest in being an employee; or

(B) Has applied to or is applying for employment by, or is being recruited for employment by, the employer; and

(2) An independent contractor.

"Employer" means a person that provides salary, wages, or the equivalent to an employee in exchange for services or labor or engages the services or labor of an unpaid intern. The term includes an agent or designee of the employer.

"Login information" means a user name and password, password, or other means or credentials of authentication required to access or control:

(1) A protected personal online account; or

(2) An electronic device, which the employee's employer or the student's educational institution has not supplied or paid for in full, that itself provides access to or control over the account.

"Login requirement" means a requirement that login information be provided before an online account or electronic device can be accessed or controlled.

"Online" means accessible by means of a computer network or the Internet.

"Person" means an individual, estate, business or nonprofit entity, public corporation, government or governmental subdivision, agency, or instrumentality, or other legal entity.

"Protected personal online account" means an employee's or student's online account that is protected by a login requirement. The term does not include an online account or the part of an online account:

(1) That is publicly available; or

(2) That the employer or educational institution has notified the employee or student might be subject to a request for login information or content, and that:

(A) The employer or educational institution supplies or pays for in full; or

(B) The employee or student creates, maintains, or uses primarily on behalf of or under the direction of the employer or educational institution in connection with the employee's employment or the student's education.

"Publicly available" means available to the general public.

"Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

"State" means a state of the United States, the District of Columbia, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States.

"Student" means an individual who participates in an educational institution's organized program of study or training. The term includes:

(1) A prospective student who expresses to the institution an interest in being admitted to, applies for admission to, or is being recruited for admission by, the educational institution; and

(2) A parent or legal guardian of a student under the age of majority.

§ -3 **Protection Of employee online account.** (a) Subject to the exceptions in subsection (b), an employer may not:

(1) Require, coerce, or request an employee to:

(A) Disclose the login information for a protected personal online account;

(B) Disclose the content of the account, except that an employer may request an employee to add the employer to, or not remove the employer from, the set of persons to which the employee grants access to the content;

(C) Alter the settings of the online account in a manner that makes the login information for, or content of the account more accessible to others; or

(D) Access the account in the presence of the employer in a manner that enables the employer to observe the login information for or content of the account; or

(2) Take, or threaten to take, adverse action against an employee for failure to comply with:

(A) An employer requirement, coercive action, or request that violates paragraph (1); or

(B) An employer request under paragraph (1)(B) to add the employer to, or not remove the employer from, the set of persons to which the employee grants access to the content of a protected personal online account.

(b) Nothing in subsection (a) shall prevent an employer from:

(1) Accessing information about an employee that is publicly available;

(2) Complying with a federal or state law, court order, or rule of a self-regulatory organization established by federal or state statute, including a self-regulatory organization as defined in section 3(a)(26) of the

Securities and Exchange Act of 1934, 15 U.S.C. §78c(a)(26); or

(3) Requiring or requesting, based on specific facts about the employee's protected personal online account, access to the content of, but not the login information for, the account in order to:

(A) Ensure compliance, or investigate non-compliance, with:

(i) Federal or state law; or

(ii) An employer prohibition against work-related employee misconduct of which the employee has reasonable notice, which is in a record, and that was not created primarily to gain access to a protected personal online account; or

(B) Protect against:

(i) A threat to safety;

(ii) A threat to employer information technology or communications technology systems or to employer property; or

(iii) Disclosure of information in which the employer has a proprietary interest or information the employer has a legal obligation to keep confidential.

(c) An employer that accesses employee content for a purpose specified in subsection (b)(3):

(1) Shall attempt reasonably to limit its access to content that is relevant to the specified purpose;

(2) Shall use the content only for the specified purpose; and

(3) May not alter the content unless necessary to achieve the specified purpose.

(d) An employer that acquires the login information for an employee's protected personal online account by means of otherwise lawful technology that monitors the employer's network, or employer-provided devices, for a network security, data confidentiality, or system maintenance purpose:

(1) May not use the login information to access or enable another person to access the account;

(2) Shall make a reasonable effort to keep the login information secure;

(3) Unless otherwise provided in paragraph (4), shall dispose of the login information as soon as, as securely as, and to the extent reasonably practicable; and

(4) Shall, if the employer retains the login information for use in an ongoing investigation of an actual or suspected breach of computer, network, or data security, make a reasonable effort to keep the login information secure and dispose of it as soon as, as securely as, and to the extent reasonably practicable after completing the investigation.

§ -4 Protection of student online account. (a) Subject to the exceptions in subsection (b), an educational institution may not:

(1) Require, coerce, or request a student to:

(A) Disclose the login information for a protected personal online account;

(B) Disclose the content of the account, except that an educational institution may request a student to add the educational institution to, or not remove the educational institution from, the set

of persons to which the student grants access to the content;

(C) Alter the settings of the account in a manner that makes the login information for or content of the account more accessible to others; or

(D) Access the account in the presence of the educational institution in a manner that enables the educational institution to observe the login information for or content of the account; or

(2) Take, or threaten to take, adverse action against a student for failure to comply with:

(A) An educational institution requirement, coercive action, or request, that violates paragraph (1); or

(B) An educational institution request under paragraph (1)(B) to add the educational institution to, or not remove the educational institution from, the set of persons to which the student grants access to the content of a protected personal online account.

(b) Nothing in subsection (a) shall prevent an educational institution from:

(1) Accessing information about a student that is publicly available;

(2) Complying with a federal or state law, court order, or rule of a self-regulatory organization established by federal or state statute; or

(3) Requiring or requesting, based upon specific facts about the student's protected personal online account, access to the content of, but not the login information for, the account in order to:

(A) Ensure compliance, or investigate non-compliance, with:

(i) Federal or state law; or

(ii) An educational institution prohibition against education-related student misconduct of which the student has reasonable notice, which is in a record, and that was not created primarily to gain access to a protected personal online account; or

(B) Protect against:

(i) A threat to safety;

(ii) A threat to educational institution information technology or communications technology systems or to educational institution property; or

(iii) Disclosure of information in which the educational institution has a proprietary interest or information the educational institution has a legal obligation to keep confidential.

(c) An educational institution that accesses student content for a purpose specified in subsection (b)(3):

(1) Shall attempt reasonably to limit its access to content that is relevant to the specified purpose;

(2) Shall use the content only for the specified purpose; and

(3) May not alter the content unless necessary to achieve the specified purpose.

(d) An educational institution that acquires the login information for a student's protected personal online account by means of otherwise lawful technology that monitors the

educational institution's network, or educational institution-provided devices, for a network security, data confidentiality, or system maintenance purpose:

(1) May not use the login information to access or enable another person to access the account;

(2) Shall make a reasonable effort to keep the login information secure;

(3) Unless otherwise provided in paragraph (4), shall dispose of the login information as soon as, as securely as, and to the extent reasonably practicable; and

(4) If the educational institution retains the login information for use in an ongoing investigation of an actual or suspected breach of computer, network, or data security, shall make a reasonable effort to keep the login information secure and dispose of it as soon as, as securely as, and to the extent reasonably practicable after completing the investigation.

§ -5 Civil action. (a) The attorney general may bring a civil action against an employer or educational institution

for a violation of this chapter. A prevailing attorney general may obtain:

(1) Injunctive and other equitable relief; and

(2) A civil penalty of up to $1,000 for each violation, but not exceeding $100,000 for all violations caused by the same event.

(b) An employee or student may bring a civil action against the individual's employer or educational institution for a violation of this chapter. A prevailing employee or student may obtain:

(1) Injunctive and other equitable relief;

(2) Actual damages; and

(3) Costs and reasonable attorney's fees.

(c) An action under subsection (a) shall not preclude an action under subsection (b), and an action under subsection (b) shall not preclude an action under subsection (a).

(d) This chapter shall not affect a right or remedy available under law other than this chapter.

§ -6 Uniformity of application and construction. In applying and construing this chapter, consideration shall be

given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

§ -7 **Relation to Electronic Signatures In Global And National Commerce Act.** This chapter modifies, limits, or supersedes the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001 et seq., but does not modify, limit, or supersede section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

§ -8 **Relation to other state laws.** If any provision in this chapter conflicts with a provision in any other chapter, the provision in this chapter shall control.

§ -9 **Severability.** If any provision of this chapter or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this chapter which can be given effect without the invalid provision or application, and to this end the provisions of this chapter are severable."

SECTION 2. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 3. This Act shall take effect upon its approval.

INTRODUCED BY:

JAN 2 3 2017

H.B. NO. 814

Report Title:
Only Privacy; Employees; Students

Description:
Adopts uniform laws on protecting the online accounts of employees and students from employers and educational institutions, respectively.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.

TESTIMONY OF
THE DEPARTMENT OF THE ATTORNEY GENERAL
TWENTY-NINTH LEGISLATURE, 2017

ON THE FOLLOWING MEASURE:
H.B. NO. 814, RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.

BEFORE THE:
HOUSE COMMITTEE ON LABOR & PUBLIC EMPLOYMENT

DATE: Thursday, February 16, 2017 **TIME:** 10:00 a.m.

LOCATION: State Capitol, Room 309

TESTIFIER(S): Douglas S. Chin, Attorney General, or
Doris Dvonch, Deputy Attorney General

Chair Johanson and Members of the Committee:

The Department of the Attorney General recognizes this is a uniform law and supports it, but provides these comments.

The purpose of this bill is to prohibit employers and educational institutions from requiring, coercing, or requesting an employee or student to provide access to his or her personal online accounts.

Section -5 of the new chapter added to the Hawaii Revised Statutes by section 1 of the bill on page 13, line 19, to page 14, line 18, permits the Attorney General, an employee, or a student to bring a civil action against an employer or educational institution for a violation of this bill's protections. Section -5(c) also permits the Attorney General and the employee or student to pursue parallel civil actions against an employer or educational institution.

It is unclear in which forum the Attorney General may bring a civil action against an employer or educational institution. We recommend the Attorney General be able to bring a civil action in district court against an employer or educational institution. As such, the following wording may be added to the current wording on page 13, line 19 to page 14, line 1:

> (a) The attorney general may bring a civil action in district court against an employer or educational institution for a violation of this chapter.

It is also unclear what constitutes a "violation" on page 13, line 19, to page 14, line 1, and what constitutes "the same event" on page 14, lines 4 to 6. For example, if an employer requests an employee to disclose login information three times on separate days and threatens to take adverse action against that employee for failing to disclose login information two times, it is unclear if there would be five, separate violations necessitating five, separate civil penalties.

We respectfully request the Committee to consider our concerns.

UNIVERSITY OF HAWAIʻI SYSTEM
Legislative Testimony

Testimony Presented Before the
House Committee on Labor and Public Employment
February 16, 2017 at 10:00 a.m.
by
Risa E. Dickson
Vice President for Academic Planning and Policy
University of Hawaiʻi System

HB 814 – RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

Chair Johanson, Vice Chair Holt, and members of the committee:

The University of Hawaiʻi (UH) takes no position on HB 814 that proposes to adopt uniform laws on protecting the online accounts of employees and students from employers and educational institutions. UH, however, would like to note an issue of concern.

Section 2, Definitions, of SB 429, outlines a "protected personal online account" and exclusions (page 3, lines 17-21 through page 4, lines 1-10). UH understands by this language that UH accounts and resources are exempted.

Thank you for the opportunity to provide this testimony.

TESTIMONY OF THE
COMMISSION TO PROMOTE UNIFORM LEGISLATION

ON H.B. NO. 814

RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.

BEFORE THE HOUSE COMMITTEE ON LABOR & PUBLIC EMPLOYMENT

DATE: Thursday, February 16, 2017, at 10:00 a.m.
Conference Room 309, State Capitol

PERSON(S) TESTIFYING: PETER HAMASAKI
Commission to Promote Uniform Legislation

Chair Johanson and Members of the House Committee on Labor & Public Employment:

My name is Peter Hamasaki, and I am a member of the State of Hawai'i Commission to Promote Uniform Legislation. Thank you for this opportunity to testify in strong support of House Bill No. 814, which enacts the Uniform Employee and Student Online Privacy Protection Act (UESOPPA).

Ordinarily, individuals decide for themselves who will have access to information that is not otherwise publically available in their social media profiles and other online accounts. Employers and educational institutions, however, may have the power to coerce access to non-public information of students' and employees' personal online accounts. In recent years, there have been a number of reported incidents in which employers and schools have demanded, and received, such access.

This act, which was developed by the Uniform Law Commission (ULC), prevents employers and public and private post-secondary educational institutions from coercing access to such information from employees and students who will normally have less than equal bargaining power. Adoption of this uniform act will establish a set of rules that will help employers, educational institutions, employees, students, technology service providers, practitioners, judges, and others to effectively apply, comply with, or enforce the law in a more consistent manner.

UESOPPA broadly protects all online accounts protected by a login requirement. This includes not just social media networking accounts, but also email, trading, banking, credit card, and other online accounts.

Stated simply, UESOPPA does *four* things to protect information in these types of online accounts.

FIRST, this act prohibits employers and schools from requiring, coercing, or requesting an employee or student to:

(1) Disclose login information for a protected account;

(2) Disclose non-publically available content of a protected account;

(3) Alter the settings of the protected account to make the login information or non-publically available content more accessible to others;

(4) Access the protected account in a way that allows another to observe the login information for, or non-publically available content of, the account; or

(5) Take or threaten to take adverse action against the employee or student for failing to comply with conduct that violates these prohibitions.

SECOND, recognizing that there are some instances where employers and schools have a strong and justifiable interest in having the act's prohibitions lifted, the act contains a number of important, narrowly-tailored exceptions. For example, an employer may need to access content in an employee's account in order to comply with a court order. This act would not prohibit this. The act contains other exceptions to its protections as well.

THIRD, if information is obtained for one of the purposes specified under one of the act's authorized exceptions, the act provides certain limits on how the information can be used.

FOURTH, the act provides for how login information, if lawfully obtained, can be used.

For violations, UESOPPA authorizes the state attorney general to bring a civil action for injunctive and other equitable relief and to obtain a civil penalty for each violation, with a cap for violations caused by the same action. An employee or student may also bring a civil action to obtain injunctive and other equitable relief, actual damages, and an award of costs and reasonable attorney's fees.

In conclusion, we urge your support for House Bill No. 814 to adopt the Uniform Employee and Student Online Privacy Protection Act . Doing so will bolster individual choice by enabling employees and students to make decisions to maintain the privacy of their personal online accounts.

Thank you very much for this opportunity to testify.

Committee:	Committee on Labor & Public Employment
Hearing Date/Time:	Thursday, February 16, 2017, 10:00 a.m.
Place:	Conference Room 309
Re:	*Testimony of the ACLU of Hawaii **with Comments** Regarding H.B. 814, Relating to the Uniform Employee and Student Online Privacy Protection Act*

Dear Chair Johanson, Vice Chair Holt, and Committee Members:

The American Civil Liberties Union of Hawaii ("ACLU of Hawaii") writes with comments regarding H.B. 814, which adopts uniform laws on protecting online accounts for students and employees, and urges the Committee to amend this bill by inserting the language of the more comprehensive Personal Online Account Privacy Act ("POAPA"), attached.

While we support the intent of the measure, the ACLU of Hawaii has concerns with the Uniform Law Commission's Employee and Student Online Privacy Protection Act ("ULC bill"), and strongly prefers the alternative and more comprehensive reform measure, POAPA. POAPA covers more Hawaii students, creates stronger safeguards against abuse, and adds protections for Hawaii tenants.

The ULC bill does not cover most students. H.B. 814 defines educational institution as "a person that provides students at the postsecondary level an organized program of study or training which is academic, technical, trade-oriented, or preparatory for gaining employment and for which the person gives academic credit." The term "postsecondary" refers only to the college level or above. This means that the majority of Hawaii students are left unprotected by this bill. POAPA, on the other hand, guarantees privacy in personal online accounts for all students, and not just those at the postsecondary level.

Unlike POAPA, the ULC bill leaves dangerous loopholes by allowing employers and educational institutions to view employees' and students' personal online account content based solely on a general allegation of misconduct. POAPA's protections are much stronger, requiring allegations of misconduct to point to specific content, and *only* allowing employers/educational institutions/landlords to access content that has been specifically identified.

Finally, housing has become an increasingly concerning area of online privacy, with more and more stories emerging of landlords demanding access to tenants' social media accounts. While POAPA protects tenants against unwarranted invasions of privacy from their landlords, the ULC bill simply fails to address this issue.

For these reasons, the ACLU of Hawaii respectfully requests the Committee to amend H.B. 814 by inserting the language of the Personal Online Account Privacy Act, attached.

Thank you for the opportunity to testify.

Sincerely,

Mandy Finlay
Advocacy Coordinator
ACLU of Hawaii

The mission of the ACLU of Hawaii is to protect the fundamental freedoms enshrined in the U.S. and State Constitutions. The ACLU of Hawaii fulfills this through legislative, litigation, and public education programs statewide. The ACLU of Hawaii is a non-partisan and private non-profit organization that provides its services at no cost to the public and does not accept government funds. The ACLU of Hawaii has been serving Hawaii for 50 years.

American Civil Liberties Union of Hawai'i
P.O. Box 3410
Honolulu, Hawai'i 96801
T: 808.522-5900
F: 808.522-5909
E: office@acluhawaii.org
www.acluhawaii.org

Personal Online Account Privacy Act

Section 1. Definitions – As used in this Act,

(A) "Applicant" shall mean an Applicant for employment.

(B) "Employee" shall mean an individual who provides services or labor to an Employer in return for wages or other remuneration or compensation.

(C) "Employer" shall mean a person who is acting directly as an Employer, or acting under the authority or on behalf of an Employer, in relation to an Employee.

(D) "Educational Institution" shall mean:

(1) A private or public school, institution, or school district, or any subdivision thereof, that offers participants, Students, or trainees an organized course of study or training that is academic, trade-oriented, or preparatory for gainful employment, as well as school Employees and agents acting under the authority or on behalf of an Educational Institution; or

(2) A state or local educational agency authorized to direct or control an entity in Section 1(D)(1).

(E) "Personal Online Account" means any online account maintained by an Employee, Student, or Tenant, including but not limited to a social media or email account, that is protected by a login requirement. "Personal Online Account" does not include an account, or a discrete portion of an account, that was either (1) opened at an Employer's behest, or provided by an Employer and intended to be used solely or primarily on behalf of or under the direction of the Employer, or (2) opened at a school's behest, or provided by a school and intended to be used solely or primarily on behalf of or under the direction of the school.

(F) "Prospective Student" shall mean an Applicant for admission to an Educational Institution.

(G) "Prospective Tenant" shall mean a person who inquires about or applies to rent real property from a Landlord for residential purposes.

(H) "Landlord" shall mean the owner or lawful possessor of real property who, in an exchange for rent, Leases it to another person or persons for residential purposes.

(I) "Lease" shall mean a legally binding agreement between a Landlord and a residential Tenant or Tenants for the rental of real property.

(J) "Specifically Identified Content" shall mean data or information on a Personal Online Account that is identified with sufficient particularity to:

(1) Demonstrate prior knowledge of the content's details; and

(2) Distinguish the content from other data or information on the account with which it may share similar characteristics.

(K) "Student" shall mean any full-time or part-time Student, participant, or trainee that is enrolled in a class or any other organized course of study at an Educational Institution.

(L) "Tenant" shall mean a person who Leases real property from a Landlord, in exchange for rent, for residential purposes.

Section 2. Employers – An Employer shall not:

(A) Require, request, or coerce an Employee or Applicant to:

(1) Disclose the user name and password, password, or any other means of authentication, or to provide access through the user name or password, to a Personal Online Account;

(2) Disclose the non-public contents of a Personal Online Account;

(3) Provide password or authentication information to a personal technological device for purposes of gaining access to a Personal Online Account, or to turn over an unlocked personal technological device for purposes of gaining access to a personal online account;

(4) Access a Personal Online Account in the presence of the Employer in a manner that enables the Employer to observe the contents of such account; or

(5) Change the settings that affect a third party's ability to view the contents of a Personal Online Account;

(B) Require or coerce an Employee or Applicant to add anyone, including the Employer, to their list of contacts associated with a Personal Online Account;

(C) Take any action or threaten to take any action to discharge, discipline, or otherwise penalize an Employee in response to an Employee's refusal to disclose any information specified in Section 2(A)(1)-(3) or refusal to take any action specified in Section 2(A)(4)-(5) or (B); or

(D) Fail or refuse to hire any Applicant as a result of an Applicant's refusal to disclose any information specified in Section 2(A)(1)-(3) or refusal to take any action specified in Section 2(A)(4)-(5) or (B).

Section 3. Educational Institutions – An Educational Institution shall not:

(A) Require, request, or coerce a Student or Prospective Student to:

(1) Disclose the user name and password, password, or any other means of authentication, or provide access through the user name or password, to a Personal Online Account;

(2) Disclose the non-public contents of a Personal Online Account;

(3) Provide password or authentication information to a personal technological device for purposes of gaining access to a Personal Online Account, or to turn over an unlocked personal technological device for purposes of gaining access to a personal online account;

(4) Access a Personal Online Account in the presence of an Educational Institution Employee or Educational Institution volunteer, including, but not limited to, a coach, teacher, or school administer, in a manner that enables the Educational Institution Employee or Educational Institution volunteer to observe the contents of such account; or

(5) Change the settings that affect a third party's ability to view the contents of a Personal Online Account;

(B) Require or coerce a Student or Prospective Student to add anyone, including a coach, teacher, school administrator, or other Educational Institution Employee or Educational Institution volunteer, to their list of contacts associated with a Personal Online Account;

(C) Take any action or threaten to take any action to discharge, discipline, prohibit from participating in curricular or extracurricular activities, or otherwise penalize a Student in response to a Student's refusal to disclose any information specified in Section 3(A)(1)-(3) or refusal to take any action specified in Section 3(A)(4)-(5) or (B); or

(D) Fail or refuse to admit any Prospective Student as a result of the Prospective Student's refusal to disclose any information specified in Section 3(A)(1)-(3) or refusal to take any action specified in Section 3(A)(4)-(5) or (B).

Section 4. Landlords – A Landlord shall not:

(A) Require, request, or coerce a Tenant or Prospective Tenant to:

(1) Disclose the user name and password, password, or any other means of authentication, or to provide access through the user name or password, to a Personal Online Account;

(2) Disclose the non-public contents of a Personal Online Account;

(3) Provide password or authentication information to a personal technological device for purposes of gaining access to a Personal Online Account, or to turn over an unlocked personal technological device for purposes of gaining access to a personal online account;

(4) Access a Personal Online Account in the presence of the Employer in a manner that enables the Employer to observe the contents of such account; or

(5) Change the settings that affect a third party's ability to view the contents of a Personal Online Account;

(B) Require or coerce a Tenant or Prospective Tenant to add anyone, including the Employer, to their list of contacts associated with a Personal Online Account;

(C) Take any action or threaten to take any action to evict or otherwise penalize a Tenant in response to Tenant's refusal to disclose any information specified in Section 4(A)(1)-(3) or refusal to take any action specified in Section 4(A)(4)-(5) or (B);

(D) Fail or refuse to rent real property to, or otherwise penalize any Prospective Tenant as a result of a Prospective Tenant's refusal to disclose any information specified in Section 4(A)(1)-(3) or refusal to take any action specified in Section 4(A)(4)-(5) or (B); or

(E) Include any provisions in a new or renewal Lease, executed after the date this Act takes effect, that conflict with Section 4 of this Act. Any such conflicting Lease provisions shall be deemed void and legally unenforceable.

Section 5. Limitations – Nothing in this Act shall prevent an Employer, Educational Institution, or Landlord from:

(A) Accessing information about an Applicant, Employee, Student, Prospective Student, Tenant, or Prospective Tenant that is publicly available;

(B) Complying with state and federal laws, rules, and regulations, and the rules of self-regulatory organizations as defined in section 3(a)(26) of the Securities and Exchange Act of 1934, 15 USC 78c(a)(26), or another statute governing self-regulatory organizations;

(C) For an Employer, without requesting or requiring an Employee or Applicant to provide a user name and password, password, or other means of authentication that provides access to a Personal Online Account, requesting or requiring an Employee or Applicant to share Specifically Identified Content that has been reported to the Employer for the purpose of:

(1) Enabling an Employer to comply with its own legal and regulatory obligations;

(2) Investigating an allegation, based on the receipt of information regarding Specifically Identified Content, of the unauthorized transfer of an Employer's proprietary or confidential information or financial data to an Employee or Applicant's Personal Online Account; or

(3) Investigating an allegation, based on the receipt of information regarding Specifically Identified Content, of unlawful harassment or threats of violence in the workplace;

(D) For an Educational Institution, without requesting or requiring a Student or Prospective Student to provide a user name and password, password, or other means of authentication that provides access to a Personal Online Account, requesting or requiring a Student or Prospective Student to share Specifically Identified Content that has been reported to the Educational Institution for the purpose of:

(1) Complying with its own legal obligations, subject to all legal and constitutional protections that are applicable to the Student or Prospective Student;

(E) For a Landlord, without requesting or requiring Tenant or Prospective Tenant to provide a user name and password, password, or other means of authentication that provides access to a Personal Online Account, requesting or requiring a Tenant or Prospective Tenant to share Specifically Identified Content that has been reported to the Landlord for the purpose of:

(1) Enabling a Landlord to comply with its own legal and regulatory obligations; or

(2) Investigating an allegation, based on the receipt of information regarding Specifically Identified Content, of a Lease violation by the Tenant where such a violation presents an imminent threat of harm to the health or safety of another Tenant or occupant of the real property or of damage to the real property;

(F) Prohibiting an Employee, Applicant, Student, or Prospective Student from using a Personal Online Account for business or Educational Institution purposes; or

(G) Prohibiting an Employee, Applicant, Student, or Prospective Student from accessing or operating a Personal Online Account during business or school hours or while on business or school property.

Section 6. Inadvertent receipt of password –

(A) If an Employer, Educational Institution, or Landlord inadvertently receives the user name and password, password, or other means of authentication that provides access to a Personal Online Account of an Employee, Applicant, Student, Prospective Student, Tenant, or Prospective Tenant through the use of an otherwise lawful technology that monitors the Employer's, Educational Institution's, or Landlord's network or Employer-provided, Educational Institution-provided, or Landlord-provided devices for network security or data confidentiality purposes, the Employer, Educational Institution, or Landlord:

(1) Is not liable for having the information;

(2) May not use the information to access the Personal Online Account of the Employee, Applicant, Student, Prospective Student, Tenant, or Prospective Tenant;

(3) May not share the information with any other person or entity; and

(4) Must delete the information as soon as is reasonably practicable, unless the information is being retained by the Employer, Educational Institution, or Landlord in connection with the pursuit of a specific criminal complaint or civil action, or the investigation thereof.

Section 7. Enforcement –

(A) Any Employer, Educational Institution, or Landlord, including its Employee or agents, who violates this Act shall be subject to legal action for damages and/or equitable relief, to be brought by any person claiming a violation of this Act has injured his or her person or reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured on account of violation of the provisions of this Act, and reasonable attorneys' fees and other costs of litigation.

(B) Any Employee or agent of an Educational Institution who violates this Act may be subject to disciplinary proceedings and punishment. For Educational Institution Employees who are represented under the terms of a collective bargaining agreement, this Act prevails except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

Section 8. Admissibility – Except as proof of a violation of this Act, no data obtained, accessed, used, copied, disclosed, or retained in violation of this Act, nor any evidence derived therefrom, shall be admissible in any criminal, civil, administrative, or other proceeding.

Section 9. Severability – The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person, entity, or circumstance, is held invalid, the remainder of this Act, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 10. Effective Date – This Act shall take effect upon passage.

HB 814

Late Testimony

LATE

LATE

LATE

February 16, 2017

To: House Committee on Labor and Public Employment
Rep. Aaron Ling Johanson, Chair
Rep. Daniel Holt, Vice Chair

Re: **Support** for HB814 Relating to the Uniform Employee and Student Online Privacy Protection Act

Thank you for the opportunity to provide testimony. The Graduate Student Organization of the University of Hawaii supports HB814, Relating to the Uniform Employee and Student Online Privacy Protection Act.

HB814 will provide needed and reasonable protections for the online privacy of graduate students, guard them from retaliation by educational institutions for failure to comply with an unlawful demand for access, and provides mechanisms for obtaining injunctive or other equitable relief and civil penalties for violations of protected personal online accounts. The Graduate Student Organization of the University of Hawaii urges the passage of HB814.

Thank you for the opportunity to testify,

LATE

LATE

LATE

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, February 16, 2017 7:48 AM
To: LABtestimony
Cc: jbickel15@yahoo.com
Subject: Submitted testimony for HB814 on Feb 16, 2017 10:00AM

HB814
Submitted on: 2/16/2017
Testimony for LAB on Feb 16, 2017 10:00AM in Conference Room 309

Submitted By	Organization	Testifier Position	Present at Hearing
John Bickel	Individual	Support	No

Comments: I support this bill as it would enhance social media privacy. As an individual, I have been confronted by my boss about a comment on Facebook about being sad at work. I was told I was not allowed to post that because it made my employer look bad. I would hope this bill would ameliorate that kind of employer power over my personal life.

Please note that testimony submitted less than 24 hours prior to the hearing, improperly identified, or directed to the incorrect office, may not be posted online or distributed to the committee prior to the convening of the public hearing.

Do not reply to this email. This inbox is not monitored. For assistance please email webmaster@capitol.hawaii.gov

LATE LATE LATE

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, February 16, 2017 9:30 AM
To: LABtestimony
Cc: 808nateyuen@gmail.com
Subject: Submitted testimony for HB814 on Feb 16, 2017 10:00AM

HB814
Submitted on: 2/16/2017
Testimony for LAB on Feb 16, 2017 10:00AM in Conference Room 309

Submitted By	Organization	Testifier Position	Present at Hearing
Nathan Yuen	Individual	Support	No

Comments: I support HB814. It is important to protect the privacy of students and employees. Please support HB 814.

Please note that testimony submitted less than 24 hours prior to the hearing, improperly identified, or directed to the incorrect office, may not be posted online or distributed to the committee prior to the convening of the public hearing.

Do not reply to this email. This inbox is not monitored. For assistance please email webmaster@capitol.hawaii.gov