SB 429, SD2

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

LAB, JUD

SB429 SD2 (?)

Submit Testimony

Measure Title:	RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.
Report Title:	Online Privacy; Employees; Applicants; Students; Prospective Students
Description:	Adopts uniform laws on protecting the online accounts of employees, applicants, students, and prospective students from employers and educational institutions, respectively. Takes effect 1/7/2059. (SD2)
Companion:	HB814
Package:	None
Current Referral:	LAB, JUD
Introducer(s):	KEITH-AGARAN, K. RHOADS, Gabbard, K. Kahele, Kidani, Kim, Wakai

Sort by Date		Status Text
1/20/2017	S	Introduced.
1/23/2017	S	Passed First Reading.
1/23/2017	S	Referred to HRE/JDL, CPH.
1/27/2017	S	Re-Referred to JDL/HRE, CPH/WAM.
1/30/2017	S	The committee(s) on JDL/HRE has scheduled a public hearing on 02-02-17 1:15PM in conference room 224.
2/2/2017	S	The committee(s) on JDL recommend(s) that the measure be PASSED, WITH AMENDMENTS. The votes in JDL were as follows: 4 Aye(s): Senator(s) Keith-Agaran, K. Rhoads, Gabbard, Kim; Aye(s) with reservations: none ; 0 No(es): none; and 1 Excused: Senator(s) L. Thielen.
2/2/2017	S	The committee(s) on HRE recommend(s) that the measure be PASSED, WITH AMENDMENTS. The votes in HRE were as follows: 5 Aye(s): Senator(s) K. Kahele, Kidani, Espero, Keith-Agaran, Taniguchi; Aye(s) with reservations: none ; 0 No(es): none; and 0 Excused: none.

2/9/2017	S	Reported from JDL/HRE (Stand. Com. Rep. No. 99) with recommendation of passage on Second Reading, as amended (SD 1) and referral to CPH/WAM.
2/9/2017	S	Report adopted; Passed Second Reading, as amended (SD 1) and referred to CPH/WAM.
2/17/2017	S	The committee(s) on CPH/WAM will hold a public decision making on 02-28-17 9:30AM in conference room 211.
2/28/2017	S	The committee(s) on WAM recommend(s) that the measure be PASSED, WITH AMENDMENTS. The votes in WAM were as follows: 9 Aye(s): Senator(s) Tokuda, Dela Cruz, English, Galuteria, Harimoto, K. Kahele, Riviere, Shimabukuro, Taniguchi; Aye(s) with reservations: none ; 0 No(es): none; and 2 Excused: Senator(s) Inouye, Wakai.
2/28/2017	S	The committee(s) on CPH recommend(s) that the measure be PASSED, WITH AMENDMENTS. The votes in CPH were as follows: 6 Aye(s): Senator(s) Baker, Nishihara, S. Chang, Espero, Ihara, Kidani; Aye(s) with reservations: none ; 0 No(es): none; and 1 Excused: Senator(s) Ruderman.
3/3/2017	S	Reported from CPH/WAM (Stand. Com. Rep. No. 824) with recommendation of passage on Third Reading, as amended (SD 2).
3/3/2017	S	48 Hrs. Notice 03-07-17.
3/7/2017	S	Report adopted; Passed Third Reading, as amended (SD 2). Ayes, 25; Aye(s) with reservations: none . Noes, 0 (none). Excused, 0 (none). Transmitted to House.
3/7/2017	H	Received from Senate (Sen. Com. No. 163) in amended form (SD 2).
3/9/2017	H	Pass First Reading
3/9/2017	H	Referred to LAB, JUD, referral sheet 27
3/17/2017	H	Bill scheduled to be heard by LAB on Tuesday, 03-21-17 10:00AM in House conference room 309.

THE SENATE
TWENTY-NINTH LEGISLATURE, 2017
STATE OF HAWAII

S.B. NO. 429 S.D. 2

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:

"Applicant" means an applicant for employment.

"Educational institution" means:

(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;

(2) School employees and agents acting under the authority or on behalf of an educational institution; and

(3) Any state or local educational agency authorized to direct or control an entity described in paragraph (1) of this definition.

"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 other remuneration or compensation.

"Employer" means a person that provides salary, wages, or the equivalent to an employee in exchange for services or labor. The term includes an agent or designee of the employer acting under the authority or on behalf of an employer.

"Personal online account" means any online account maintained by an employee or student, including social media or electronic mail accounts, that is protected by a login requirement. The term does not include an account, or the discrete portion of an account, that was:

(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 an educational institution's behest, or provided by an educational institution and intended to be used solely or primarily on behalf of or under the direction of the educational institution.

"Prospective student" means an applicant for admission to an educational institution.

"Publicly available" means available to the general public.

"Specifically identified content" means 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.

"Student" means any full-time or part-time student, participant, or trainee who is enrolled in a class or any other organized course of study at an educational institution.

§ -3 Protection of employee or applicant online account. (a) Subject to the exceptions in subsection (b), an employer shall not:

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

(A) 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;

(B) Disclose the non-public content of a personal online account;

(C) Provide password or authentication information to a personal technological device for the purpose of gaining access to a personal online account, or turn over an unlocked personal technological device for the purpose of gaining access to a personal online account;

(D) Alter the settings of the personal online account in a manner that makes the content of the personal online account more accessible to others; or

(E) Access the personal online account in the presence of the employer in a manner that enables the employer to observe the content of the account;

(2) Require or coerce an employee or applicant to add anyone, including the employer, to the employee's or applicant's list of contacts associated with a personal online account;

(3) Take, or threaten to take, adverse action against an employee or applicant for failure to comply with an employer requirement, coercive action, or request that violates paragraph (1); or

(4) Fail or refuse to admit any applicant as a result of the applicant's refusal to disclose any information or take any action specified in paragraph (1).

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

(1) Accessing information about an employee or applicant 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 Exchange Act of 1934 (15 U.S.C. 78c(a)(26));

(3) 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, requiring or requesting an employee or applicant to provide specifically identified content that has been reported to the employer for the purpose of:

(A) Enabling the employer to comply with legal and regulatory obligations;

(B) 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's or applicant's personal online account;

(C) Investigating an allegation, based on the receipt of information regarding specifically identified content, of unlawful harassment or threats of violence in the workplace; or

(D) Protecting against a threat to safety, employer information technology, communications technology systems, or employer property;

(4) Prohibiting an employee or applicant from using a personal online account for business purposes; or

(5) Prohibiting an employee or applicant from accessing or operating a personal online account during business hours or while on business property.

(c) An employer that accesses employee or applicant 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) Shall not alter the content unless necessary to achieve the specified purpose.

(d) An employer that inadvertently receives the user name and password, password, or other means of authentication that provides access to an employee's or applicant's 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) Is not liable for having the information;

(2) Shall not use the information to access the personal online account of the employee or applicant or share the information with any other person or entity;

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

(4) Unless otherwise provided in paragraph (5), shall dispose of the information as soon as, as securely as, and to the extent reasonably practicable; and

(5) Shall, if the employer retains the information for use in connection with the pursuit of a specific criminal complaint or civil action, or the investigation

thereof, 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.

(e) Nothing in this chapter shall diminish the authority and obligation of an employer to investigate complaints, allegations, or the occurrence of sexual, racial, or other prohibited harassment under chapter 378.

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

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

(A) 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;

(B) Disclose the non-public content of a personal online account;

(C) Provide password or authentication information to a personal technological device for the purpose

of gaining access to a personal online account, or turn over an unlocked personal technological device for the purpose of gaining access to a personal online account;

(D) Alter the settings of the personal online account in a manner that makes the content of the personal online account more accessible to others; or

(E) Access the personal online account in the presence of the educational institution employee or educational institution volunteer, including a coach, teacher, or school administrator, in a manner that enables the educational institution employee or educational institution volunteer to observe the content of the account;

(2) 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 the student's or prospective student's list of contacts associated with a personal online account;

(3) Take, or threaten to take, adverse action against a student or prospective student, including discharge, discipline, prohibition from participation in curricular or extracurricular activities, for failure to comply with an educational institution requirement, coercive action, or request that violates paragraph (1);

(4) Fail or refuse to admit any prospective student as a result of the prospective student's refusal to disclose any information or take any action specified in paragraph (1).

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

(1) Accessing information about a student or prospective 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, including a self-regulatory organization as defined in section 3(a)(26) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(26));

(3) 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, requiring or requesting a student or prospective student to provide specifically identified content that has been reported to the educational institution for the purpose of:

(A) Enabling the educational institution to comply with legal and regulatory obligations;

(B) Investigating an allegation, based on the receipt of information regarding specifically identified content, of the unauthorized transfer of an educational institution's proprietary or confidential information or financial data to a student's or prospective student's personal online account;

(C) Investigating an allegation, based on the receipt of information regarding specifically identified content, of noncompliance with 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 personal online account; or

(D) Protecting against a threat to safety, educational institution information technology, communications technology systems, or educational institution property;

(4) Prohibiting a student or prospective student from using a personal online account for educational institution purposes; or

(5) Prohibiting a student or prospective student from accessing or operating a personal online account during school hours or while on school property.

(c) An educational institution that accesses student or prospective 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) Shall not alter the content unless necessary to achieve the specified purpose.

(d) An educational institution that inadvertently receives the user name and password, password, or other means of authentication that provides access to a student's or prospective student's 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) Is not liable for having the information;

(2) Shall not use the information to access the personal online account of the student or prospective student or share the information with any other person or entity;

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

(4) Unless otherwise provided in paragraph (5), shall dispose of the information as soon as, as securely as, and to the extent reasonably practicable; and

(5) Shall, if the educational institution retains the information for use in connection with the pursuit of a specific criminal complaint or civil action, or the investigation thereof, make a reasonable effort to keep the information secure and dispose of it as soon as, as securely as, and to the extent reasonably practicable after completing the investigation.

§ -5 **Enforcement.** (a) The attorney general may bring a civil action in district court 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, applicant, student, or prospective student may bring a civil action in district court against the individual's employer or educational institution for a violation of this chapter. A prevailing employee, applicant, student, or prospective student may obtain:

(1) Injunctive and other equitable relief;

(2) Actual damages; and

(3) Costs and reasonable attorney's fees.

(c) An 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, 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 shall prevail except where the agreement, memorandum, or practice does not conflict with this chapter.

(d) 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).

(e) 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, and supersedes the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.), but does not modify, limit, or supersede section 101(c) of that act (15 U.S.C. 7001(c)), or authorize electronic delivery of any of the notices described in Section 103(b) of that act (15 U.S.C. 7003(b)).

§ -8 **Relation to other state laws.** Unless otherwise provided in this chapter, 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 on January 7, 2059.

S.B. NO. 429 S.D. 2

Report Title:
Online Privacy; Employees; Applicants; Students; Prospective Students

Description:
Adopts uniform laws on protecting the online accounts of employees, applicants, students, and prospective students from employers and educational institutions, respectively. Takes effect 1/7/2059. (SD2)

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

HAWAIʻI CIVIL RIGHTS COMMISSION

830 PUNCHBOWL STREET, ROOM 411 HONOLULU, HI 96813 · PHONE: 586-8636 FAX: 586-8655 TDD: 568-8692

March 21, 2017
Rm. 309, 10:00 a.m.

To: The Honorable Aaron Johanson, Chair
Members of the House Committee on Labor and Public Employment

From: Linda Hamilton Krieger, Chair
and Commissioners of the Hawaiʻi Civil Rights Commission

Re: S.B. No. 429, S.D.2

The Hawaiʻi Civil Rights Commission (HCRC) has enforcement jurisdiction over Hawaiʻi's laws prohibiting discrimination in employment, housing, public accommodations, and access to state and state funded services. The HCRC carries out the Hawaiʻi constitutional mandate that no person shall be discriminated against in the exercise of their civil rights. Art. I, Sec. 5.

S.B. No. 429, S.D.2, if enacted, will add a new chapter to the Hawaiʻi Revised Statutes, prohibiting employers and educational institutions from requiring or requesting employees and potential employees and students to grant access to personal account login information or content.

The HCRC supports the intent of S.B. No. 429, S.D.2, which includes an amendment adding a new subsection (e) in the new HRS § ___-3, expressly providing that nothing in the new section shall diminish the authority and obligation of an employer to investigate complaints, allegations, or the occurrence of sexual, racial, or other prohibited harassment under chapter 378, part I.

Current state and federal fair employment law, HRS Chapter 378, Part I, and Title VII of the Civil Rights Act of 1964, require employers, once on notice of discriminatory harassment in the workplace, to promptly investigate and take effective corrective action. Failure to investigate and take effective corrective action is a violation of law. An employer investigation of sexual, racial, or other prohibited discrimination could involve allegations of harassment via social media.

The HCRC supports the intent of S.B. No. 429, S.D.2, as amended by the Senate to expressly confirm that the newly created protections do not diminish the authority and obligation of an employer to investigate and take prompt corrective action when on notice of discriminatory harassment in the workplace.

TESTIMONY OF THE
COMMISSION TO PROMOTE UNIFORM LEGISLATION

ON S.B. NO. 429, S.D.2

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

BEFORE THE HOUSE COMMITTEE ON LABOR & PUBLIC EMPLOYMENT

DATE: Tuesday, March 21, 2017 at 10:00 a.m.
Conference Room 309, State Capitol

PERSON TESTIFYING: KEN TAKAYAMA and KEVIN SUMIDA
Commission to Promote Uniform Legislation

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

My name is Ken Takayama, 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 with amendments** of Senate Bill No. 429, Senate Draft 2, which we ask this Committee to amend to reflect language closer to the Uniform Employee and Student Online Privacy Protection Act (UESOPPA).

(1) We specifically support amending Senate Bill No. 429, S.D.2 to conform to **HOUSE BILL NO. 814, H.D.2**, which the House of Representatives approved on March 7, 2017. H.B. No. 814, H.D.2 would enact UESOPPA with certain amendments as proposed by the University of Hawaii, and represents a **balanced** approach to the privacy of employee and student online accounts. In addition, with respect to students, UESOPPA is limited to post-secondary education, whereas Senate Bill No. 429, S.D.2, would include primary and secondary schools.

(2) If the Committee feels that the foregoing is too broad, we ask that sections -3(b)(3) and -4(b)(3) of the chapter created by S.B. No.429, S.D.2, be amended to reflect the wording of those same provisions in H.B. 814, H.D.2.

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. At present, however, employers and educational institutions, 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.

UESOPPA, which was developed by the Uniform Law Commission (ULC) with input from employers, educational institutions, internet and other technology companies and privacy organizations, prevents employers and public and private 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.

As introduced, S.B. No. 429 would have enacted UESOPPA. However, the S.B. No. 429, S.D.2 draft replaced much of the UESOPPA contents with those of a different proposal from the American Civil Liberties Union (ACLU). We are particularly concerned about the changes made to sections -3(b)(3) and -4(b)(3). Each allows the employer or educational institution, under certain circumstances, to gain access to an employee's or student's account or information therein—but not the login information. However, compared to the provisions of S.B. No. 429, S.D.2, H.B. No. 814, H.D.2 is more helpful to employers and educational institutions because it gives them the ability to investigate where they have specific facts pointing to a problem. Specifically, UESOPPA is more helpful in the following two ways:

First, unlike UESOPPA, S.B. No. 429, S.D.2 would not lift prohibitions on employers to request access to content upon receiving facts about a violation of any prohibition against work-related misconduct (of which the employee has had notice). Rather, it lists particular types of misconduct that could justify making such requests. If the employer has reason to believe that the employee engaged in some type of work related misconduct not on the list enumerated in S.B. No. 429, S.D.2, the prohibition would remain in place and the employer could not request access to content. That is a major difference from H.B. No. 814, H.D.2. The Uniform Law Commission drafting

committee discussed this and determined that, as drafters, they could not anticipate all the types of work-related misconduct in which employees might engage, and therefore decided against having a specific list of items that justified lifting the prohibition against requests for content.

By comparison, S.B. No. 429, S.D.2 takes the opposite approach. It lists the violations that would allow requests for content, without accounting for what may happen in the future. As a result, we believe this list will become incomplete. An employee will engage in some other serious form of misconduct and, under the terms of S.B. No. 429, S.D.2, the employer will not be able to make the request for content information. In this way, S.B. No. 429, S.D.2 is narrower, less practical, and thus less helpful to employers than H.B. No. 814, H.D.2.

Second, rather than granting access to the employer (or educational institution), Sections -3(b)(3)(C) and -4(b)(3)(C).of S.B. No. 429, S.D.2 require the employee (or student) to pull out the alleged content for examination by the employer (or educational institution). However, this does not address the employer's (and institution's) concern that they are in fact getting access to all relevant content. As currently written, S.B. No. 429, S.D.2 requires an employer (or institution) to trust that the employee is complying in a good faith and honest manner. Unfortunately, in some instances, this may not be the case.

In addition, with respect to students, UESOPPA (H.B. No. 814, H.D.2) is limited to post-secondary education, whereas S.B. No. 429, S. D. 2, would include primary and secondary schools. Because primary and secondary school students are minors, the considerations that affect the need for protection and supervision of students differ from those of college or university students in many respects. This is amply reflected in the many judicial decisions which recognize that constitutional privacy considerations differ when applied to primary or secondary students. Because of these differing considerations, we believe that H. B. No. 814, H. D. 2, which is limited to employees and post-secondary students, is preferable and that the policy applied at the elementary through high school level should be handled separately, with appropriate input from the Department of Education and other stakeholders.

In the bigger picture, as provided in H.B. No. 814, H.D.2, stated simply, UESOPPA does four things to protect information in these types of online accounts.

FIRST, this act prohibits employers and schools from requiring, or coercing, 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 limited number of important but narrowly-tailored exceptions. The act does not prevent access to information that is publicly available or that is required to comply with federal or state law, a court order, or the rule of a self-regulatory organization established by federal or state statute. Additionally, only if the employer or school has **specific facts** about the protected account, the employer or school may seek access to content (but not login information) for the limited purposes of compliance with law, investigation of employee or student misconduct or a threat to the safety of persons or technology networks, or protection of confidential or proprietary information.

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 S. B. No. 429, S.D. 2, to adopt the Uniform Employee and Student Online Privacy Protection Act in the form passed earlier by the House of Representatives as H.B. No. 814, H.D.2—or by at least reinstating the specific language used by H.B. No. 814, H.D.2 in sections -3(b)(3) and -4(b)(3) Doing so will bolster individual choice by enabling employees and students to make decisions to maintain the privacy of their personal online accounts, while maintaining the ability of employers and educational institutions to take action in a timely manner in serious cases.

Thank you very much for this opportunity to testify.

Written Only

Date: 03/21/2017
Time: 10:00 AM
Location: 309
Committee: House Labor & Public Employment

Department: Education

Title of Bill: SB 0429, SD2 RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.

Purpose of Bill: Adopts uniform laws on protecting the online accounts of employees, applicants, students, and prospective students from employers and educational institutions, respectively. Takes effect 1/7/2059. (SD2)

Department's Position:
The Hawaii Department of Education (Department) supports the intent of S.B. 0429 SD2, which it believes is in line with protecting employees' and students' online accounts.

The Department is concerned that the language throughout the bill assumes that personal online accounts can be accessed and used in the workplace. The bill does not address access to school accounts.

Thank you for the opportunity to provide testimony for S.B. 0429 SD2.

Tammy Cota, Executive Director
1 Blanchard Ct., Suite 101
Montpelier, VT 05602
802-279-3534
www.theinternetcoalition.com
tammy@theinternetcoalition.com

March 20, 2017

Honorable Aaron Ling Johnson, Chair of Senate Labor and Public Employment Committee
Hawaii State Capitol
415 South Beretania Street, Room 309
Honolulu, HI 96813

Re: **Hawaii SB 429,** Uniform Employee and Student Online Privacy Protection Act

Dear Senator Johnson:

I am the executive director of the Internet Coalition (IC), a national trade association that represents members in state public policy discussions. The IC also serves as an informational resource, striving to protect and foster the Internet economy and the benefits it provides consumers.

I wish to express support for the proposed substitute model langauge being offered by the American Civil Liberties Union (ACLU), relating to password protection. The language the ACLU is proposing would define the rules governing employer, educational institutions, and landlords' access to employee, student, and tenants' personal online accounts. It represents a model social media privacy law, which IC members and other associations worked together to help write.

The ACLU language would prohibit employers, educational institutions, or landlords from *compelling* the individuals covered by the bill from adding them to a social media contact list, but would allow *requests* to do so. This is a valuable change in light of the way businesses communicate with employees, customers, and the general public today. Many businesses post updates and offers or specials on social media, for example, and it is reasonable that the employer would invite employees to add the employer to their list of contacts.

Second, employers, educational institutions, and landlords must be able to ensure compliance with all applicable laws and regulatory requirements, in addition to prohibitions against work-related employee misconduct. The bill, as amended, would allow for that. It would allow employers to request that an employee share specific content regarding a personal account for these limited purposes.

The ACLU model bill strikes an appropriate balance of protecting employee, student, and tenant privacy while leaving room for employer practices to protect employers' networks, systems, and proprietary information. It addresses a real – and not simply theoretical – harm, and it is imperative to enact these privacy protections now.

I thank you for addressing this important issue and urge you to support substituting SB 429 with the ACLU model bill.

Please feel free to contact me if you would like to discuss this issue further.

Sincerely,

Tammy Cota

Tammy Cota

cc: Senate Labor and Public Employment Committee

AMERICAN CIVIL LIBERTIES UNION of HAWAI'I

Committee:	Committee on Labor & Public Employment
Hearing Date/Time:	Tuesday, March 21, 2017, 10:00 a.m.
Place:	Room 309
Re:	*Testimony of the ACLU of Hawaii with Comments regarding S.B. 429, S.D.2, 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 S.B. 429, S.D.2, which adopts uniform laws on protecting online accounts for students and employees, and urges the Committee to amend this bill by inserting the tenant privacy protections of the more comprehensive Personal Online Account Privacy Act ("POAPA"), attached. The ACLU of Hawaii also offers an amendment regarding the definition of "specifically identified content."

While the ACLU of Hawaii strongly supports the protection of student and employee online privacy, and applauds the Legislature's efforts to do so through this measure, we would prefer that the measure also protect privacy in the area of housing. Housing has become an increasingly concerning area of online privacy, with more and more stories emerging of landlords demanding access to tenants' personal accounts. While POAPA protects tenants against unwarranted invasions of privacy from their landlords, the ULC bill, after which this measure is modeled, simply fails to address this issue.

Finally, in order to address concerns raised by the tech industry regarding the current bill language's requirement that an employer/educational institution demonstrate prior knowledge of the online account content's details prior to requesting the disclosure of content, the ACLU of Hawaii respectfully requests the Committee to amend S.B. 429, S.D.2 by amending the definition of "Specifically Identified Content" the reflect the following:

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

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

~~(2) D~~ distinguish the discrete, individual piece of content being sought from any other data or information stored in ~~on~~ the account with which it may share similar characteristics.

Thank you for this opportunity to testify.

Mandy Finlay

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 stored in a Personal Online Account that is identified with sufficient particularity to distinguish the discrete, individual piece of content being sought from any other data or information stored in 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 account settings of a Personal Online Account so as to increase third party access to its contents;

(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 account settings of a Personal Online Account so as to increase third party access to its contents;

(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 account settings of a Personal Online Account so as to increase third party access to its contents;

(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.

SB 429, SD2

Late Testimony

UNIVERSITY OF HAWAI'I SYSTEM
Legislative Testimony

LATE

LATE

LATE

Testimony Presented Before the
House Committee on Labor and Public Employment
March 21, 2017 at 10:00 a.m.
by
Risa Dickson, Vice President for Academic Planning and Policy
Garret Yoshimi, Vice President for Information Technology
Carrie Okinaga, Vice President for Legal Affairs
University of Hawai'i System

SB 429 SD2 – RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

Chair Johanson, Vice Chair Holt, and Members of the Committee:

Thank you for the opportunity to present testimony regarding SB 429 SD2 – Relating to the Uniform Employee and Student Online Privacy Protection Act.

We support the intent of this bill in protecting employee and student privacy. That said, this uniform act was just newly approved in 2016 by the National Conference of Commissioners on Uniform State Laws, has not yet been adopted by any state to our knowledge, and needs to be amended to avoid unintended consequences. In that regard, the University recommended certain amendments to the related measure, HB 814, and these were incorporated into HB 814 HD2, which we support and believe merits consideration.

With regard to SB 429 SD2, the following amendments are requested in keeping with our prior testimony on the related measure and our concerns regarding this bill:

(1) Page 4, line 7, and Page 9, line12, should be revised to read:

(1) Require~~,~~ or coerce ~~or request~~ … :

The purpose of the bill is to prevent coercion of employees and students. As written, this bill would subject the University (and all employers and educational institutions) to penalties and civil liability for an innocent "request" for login information, no matter the intent. Therefore, if a student or employee is leaving school/work for an extended vacation or emergency medical situation, and a caring adviser or supervisor instinctively requests login information for a covered account to assist the person with monitoring email or coursework assignments, that would be expressly prohibited under this bill and would subject the University to liability and individual employees or agents of the educational institution to discipline.

(2) Page 7, lines 3 to 6, should be revised to read:

(C) Investigating an allegation, based on the receipt of information regarding specifically identified content, of work-related employee misconduct, or unlawful harassment or threats of violence in the workplace.

HB 814 HD2 provided at proposed HRS section __-3(b)(3)(A)(ii) for access to an employee's protected personal online account to ensure compliance, or to investigate non-compliance with work-related employee misconduct. A similar provision should be included in SB 429 SD2.

(3) Page 8, lines 19 to 21, should be revised to read:

(5) Shall, if the employer retains the information for use in connection with the pursuit of an ongoing investigation of actual or suspected breach of computer, network, or data security, or a specific criminal complaint or civil action …"

HB 814 HD2 provided at proposed HRS section __-3(d)(4) for limited retention of login information for investigation of computer, network or data security breaches. SB 429 SD2 replaces that with reference instead to a specific criminal complaint or civil action. Respectfully, both situations merit inclusion in the bill.

(4) Page 15, lines 1 to 3, should be revised to read:

(5) Shall, if the education institution retains the information for use in connection with the pursuit of an ongoing investigation of actual or suspected breach of computer, network, or data security, or a specific criminal complaint or civil action …"

HB 814 HD2 provided at proposed HRS section __-4(d)(4) for limited retention of login information for investigation of computer, network or data security breaches. SB 429 SD2 replaces that with reference instead to a specific criminal complaint or civil action. Respectfully, both situations merit inclusion in the bill.

(5) Effective date: Currently, there is a January 7, 2059 effective date. If enacted, the University will need time to effect policies and training to ensure compliance with this act. We would respectfully request an effective date of 2020 to afford time for necessary consultations and implementation of said policies and training.

Based on the foregoing, the University supports SB 429 SD2, with amendment.

LATE

LATE

LATE

AMERICAN CIVIL LIBERTIES UNION of HAWAI'I

Committee:	Committee on Labor & Public Employment
Hearing Date/Time:	Tuesday, March 21, 2017, 10:00 a.m.
Place:	Room 309
Re:	*Testimony of the ACLU of Hawaii with Comments regarding S.B. 429, S.D.2, 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 S.B. 429, S.D.2, which adopts uniform laws on protecting online accounts for students and employees, and urges the Committee to amend this bill by inserting the tenant privacy protections of the more comprehensive Personal Online Account Privacy Act ("POAPA"), attached. The ACLU of Hawaii also offers an amendment regarding the definition of "specifically identified content."

While the ACLU of Hawaii strongly supports the protection of student and employee online privacy, and applauds the Legislature's efforts to do so through this measure, we would prefer that the measure also protect privacy in the area of housing. Housing has become an increasingly concerning area of online privacy, with more and more stories emerging of landlords demanding access to tenants' personal accounts. While POAPA protects tenants against unwarranted invasions of privacy from their landlords, the ULC bill, after which this measure is modeled, simply fails to address this issue.

Finally, in order to address concerns raised by the tech industry regarding the current bill language's requirement that an employer/educational institution demonstrate prior knowledge of the online account content's details prior to requesting the disclosure of content, the ACLU of Hawaii respectfully requests the Committee to amend S.B. 429, S.D.2 by amending the definition of "Specifically Identified Content" the reflect the following:

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

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

~~(2) D~~ distinguish the discrete, individual piece of content being sought from any other data or information stored in ~~on~~ the account with which it may share similar characteristics.

Thank you for this opportunity to testify.

Mandy Finlay

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 stored in a Personal Online Account that is identified with sufficient particularity to distinguish the discrete, individual piece of content being sought from any other data or information stored in 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 account settings of a Personal Online Account so as to increase third party access to its contents;

(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 account settings of a Personal Online Account so as to increase third party access to its contents;

(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 account settings of a Personal Online Account so as to increase third party access to its contents;

(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.

1513977-1

KOBAYASHI SUGITA & GODA, LLP
Attorneys at Law

Bert T. Kobayashi, Jr.*
Alan M. Goda*

John R. Aube*
Wendell H. Fuji*
Charles W. Gall*
Neal T. Gota
Clifford K. Higa*
Robert K. Ichikawa*
Christopher T. Kobayashi*
Jan M. L.Y. Kutsunai*

David M. Louie*
Jonathan S. Moore
Bruce A. Nakamura*
Kenneth M. Nakasone*
Gregory M. Sato*
Jesse W. Schiel*
Craig K. Shikuma*
Lex R. Smith*
Joseph A. Stewart*
David B. Tongg*

*A Law Corporation

Stephen D. Atwell
Yuko Funaki
Caycie K. Gusman
Charles D. Hunter
Nicholas R. Monlux
Aaron Mun
Gabriele V. Provenza
Nicholas P. Smith
Anthony Suetsugu
Brian D. Tongg
Maria Y.Y. Wang

Of Counsel
Kenneth Y. Sugita*
Jonathan A. Kobayashi
Burt T. Lau*
John F. Lezak*
Larry L.Myers*

March 20, 2017

COMMITTEE ON LABOR & PUBLIC EMPLOYMENT
Rep. Aaron Ling Johanson, Chair; Rep. Daniel Holt, Vice Chair

Tuesday, March 21, 2017 at 10:00 AM
Conference Room 309 State Capitol

Re: LATE TESTIMONY ON BEHALF OF FACEBOOK
RE: S.B. 429 SD2

Dear Representatives:

I write on behalf of my client, Facebook. Facebook supports the amendments and language submitted by the American Civil Liberties Union, which reflect language agreed upon between civil liberties and privacy advocates and the tech industry. This language protects personal accounts against unwarranted intrusions while also providing employers with important certainty regarding what practices are and are not permitted.

I respectfully urge you to adopt such amendments. Thank you for your consideration.

Very truly yours,

DAVID M. LOUIE
for
KOBAYASHI SUGITA & GODA, LLP