TESTIMONY OF THE
COMMISSION TO PROMOTE UNIFORM LEGISLATION

ON S.B. NO. 429, S.D.2, H.D. 1
RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.

BEFORE THE HOUSE COMMITTEE ON JUDICIARY.

DATE: Wednesday, March 29, 2017, at 2:00 p.m.
Conference Room 325, State Capitol

PERSON TESTIFYING: KEN TAKAYAMA and/or PETER J. HAMASAKI
Commission to Promote Uniform Legislation

Chair Nishimoto and Members of the House Committee on Judiciary:

On behalf of the State of Hawai'i Commission to Promote Uniform Legislation, thank you for this opportunity to submit testimony in strong **SUPPORT WITH AMENDMENTS** of Senate Bill No. 429, Senate Draft 2, House Draft 1, which enacts the Uniform Employee and Student Online Privacy Protection Act (UESOPPA). We specifically support amending Senate Bill No. 429 to conform to **HOUSE BILL NO.814, HOUSE DRAFT 2**, which would enact UESOPPA with a 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, Senate Draft 2, House Draft 1, 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 House Bill No. 814, House Draft 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.

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) with input from employers, educational institutions, internet and other technology companies and privacy organizations, 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 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 Senate Bill No. 429, Senate Draft 2, House Draft 1, with amendments to conform to House Bill 814, House Draft 2, 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 in a fair and balanced manner.

Thank you very much for this opportunity to submit testimony.

UNIVERSITY OF HAWAI'I SYSTEM
Legislative Testimony

Testimony Presented Before the
House Committee on Judiciary
March 29, 2017 at 2:00 p.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 HD1 – RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

Chair Nishimoto, Vice Chair San Buenaventura, and Members of the Committee:

Thank you for the opportunity to present testimony regarding SB 429 SD2 HD1 – 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 HD1, 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 4, and Page 9, line 4, 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 6, lines 19 to 22, 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; or

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 HD1.

(3) Page 8, lines 12 to 14, 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 HD1 replaces that with reference instead to a specific criminal complaint or civil action. Respectfully, both situations merit inclusion in the bill.

(4) Page 14, lines 10 to 12, should be revised to read:

(5) Shall, if the educational 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 HD1 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 HD1, with amendment.

HAWAIʻI CIVIL RIGHTS COMMISSION

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

March 29, 2017
Rm. 325, 2:30 p.m.

To: The Honorable Scott Nishimoto, Chair
Members of the House Committee on Judiciary

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

Re: S.B. No. 429, S.D.2, H.D.1

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, H.D.1, 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, H.D.1, 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, H.D.1, 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.

AMERICAN CIVIL LIBERTIES UNION of HAWAI'I

Committee:	Committee on Judiciary
Hearing Date/Time:	Wednesday, March 29, 2017, 2:00 p.m.
Place:	Room 325
Re:	*Testimony of the ACLU of Hawaii in Support of, with Suggest Amendments to S.B. 429, S.D.2, H.D.1, Relating to The Uniform Employee and Student Online Privacy Protection Act*

Dear Chair Nishimoto, Vice Chair San Buenaventura, and Committee Members:

The American Civil Liberties Union of Hawaii ("ACLU of Hawaii") writes in support of, with suggested amendments to S.B. 429, S.D.2, H.D.1, which adopts uniform laws on protecting online accounts for students and employees. The ACLU of Hawaii 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."

The ACLU of Hawaii supports the protection of student and employee online privacy, and strongly prefers this version to the measure as it was introduced. This version covers all students, rather than limiting privacy protections to students at the postsecondary level. The H.D. 1 also closes a dangerous loophole from the Uniform Law Commission's original language, which allowed an employer or school to access all content in an employee/student's email account based on a general allegation of misconduct related to the account. Under the current version, this process works more like legal discovery, where the employer or school may require an employee or student to disclose *only* specifically identified content tied to a specific allegation of misconduct.

While this measure provides strong privacy protections for Hawaii's employees and students, the ACLU of Hawaii 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 <u>stored in</u> ~~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
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.