



STATE OF HAWAII
DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAII 96804

Date: 02/26/2019
Time: 02:05 PM
Location: 325
Committee: House Judiciary

Department: Education

Person Testifying: Dr. Christina M. Kishimoto, Superintendent of Education

Title of Bill: HB 0006, HD2 RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.

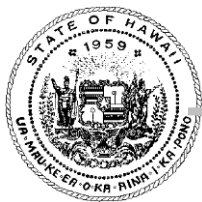
Purpose of Bill: Establishes The Uniform Employee and Student Online Privacy Protection Act that adopts uniform laws on protecting the online accounts of employees, prospective employees, unpaid interns, applicants, students, and prospective students from employers and educational institutions. (HB6 HD2)

Department's Position:

The Department of Education (Department) supports HB6, HD2 which is in line with protecting employee and student online accounts, while ensuring that employers and educational institutions are able to address non-compliance with laws and regulations that directly impact the employer or educational institution.

Thank you for the opportunity to provide testimony on this measure.

The Hawaii State Department of Education seeks to advance the goals of the Strategic Plan which is focused on student success, staff success, and successful systems of support. This is achieved through targeted work around three impact strategies: school design, student voice, and teacher collaboration. Detailed information is available at www.hawaiipublicschools.org.



HAWAII CIVIL RIGHTS COMMISSION

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

February 26, 2019
Rm. 325, 2:05 p.m.

To: The Honorable Chris Lee, Chair
The Honorable Joy A. San Buenaventura, Vice Chair
Members of the House Committee on Judiciary

From: Linda Hamilton Krieger, Chair
and Commissioners of the Hawai'i Civil Rights Commission

Re: H.B. No. 6, H.D.2

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

H.B. No. 6, H.D.2, if enacted, will add a new chapter to the Hawai'i 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 H.B. No. 6, H.D.2, with a request for an amendment to add a new subsection in the new HRS § ___-3, expressly providing that nothing in subsection ___-3(a) 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 H.B. No. 6, H.D.2, with the requested amendment 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 H.B. NO. 6, H.D. 2
RELATING TO THE UNIFORM EMPLOYEE AND
STUDENT ONLINE PRIVACY PROTECTION ACT.**

BEFORE THE HOUSE COMMITTEE ON JUDICIARY

DATE: Tuesday, February 26, 2019, at 2:05 p.m.
Conference Room 325, State Capitol

PERSON TESTIFYING: KEN TAKAYAMA or PETER HAMASAKI,
Commission to Promote Uniform Legislation

Chair Lee and Members of the House Committee on Judiciary:

My name is Peter Hamasaki, and I am a member of the State of Hawai'i Commission to Promote Uniform Legislation. Thank you for this opportunity to testify in strong support of House Bill No. 6, H.D. 2, which enacts the Uniform Employee and Student Online Privacy Protection Act (UESOPPA).

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

This act, which was developed by the Uniform Law Commission (ULC) 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. In such event, the student or employee will provide the access, either by printing out the relevant content or by otherwise showing the content to the requesting employer or school. In either case, the individual is involved in providing the requested content and can limit the content to that relevant to the request.

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

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

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

In conclusion, we urge your support for House Bill No. 6, H.D. 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.

Thank you very much for this opportunity to testify.



UNIVERSITY OF HAWAII SYSTEM

Legislative Testimony

Testimony Presented Before the
House Committee on Judiciary
Tuesday, February 26, 2019 at 2:05 p.m.

By

Donald O. Straney, Vice President for Academic Planning and Policy
Garret Yoshimi, Vice President for Information Technology/Chief Information Officer
Carrie Okinaga, Vice President for Legal Affairs and University General Counsel
University of Hawai'i System

HB 6 HD2 – RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

Chair Lee, Vice Chair San Buenaventura and members of the committee:

Thank you for the opportunity to present testimony regarding HB 6 HD2 – Relating to the Uniform Employee and Student Online Privacy Protection Act.

The University of Hawai'i supports the intent of the bill and appreciates the changes made to HB 6 to ensure that it does not adversely impact University of Hawai'i accounts and resources that are necessary for the efficient operation of University business. With the revised definition of the term "protected personal online account" as set forth in HB 6 HD2, the University is in full support of this measure.

Thank you for the opportunity to provide testimony.

HB-6-HD-2

Submitted on: 2/22/2019 6:12:12 PM

Testimony for JUD on 2/26/2019 2:05:00 PM

Submitted By	Organization	Testifier Position	Present at Hearing
Michael Golojuch Jr	LGBT Caucus of the Democratic Party of Hawaii	Support	Yes

Comments:

Aloha Representatives,

The LGBT Caucus of the Democratic Party of Hawaii supports the passage of HB 6 HD 2.

We do support the amendments suggested by the ACLU of Hawai'i.

Mahalo for your consideration and for the opportunity to testify.

Mahalo,

Michael Golojuch, Jr.
Chair
LGBT Caucus of the Democratic Party of Hawai'i

TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS
COMMENTING ON HOUSE BILL HB 6, HD 2, RELATING TO THE UNIFORM
EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

February 26, 2019

Via e mail: capitol.hawaii.gov/submittestimony.aspx

Honorable Representative Chris Lee, Chair
Committee on Judiciary
State House of Representatives
Hawaii State Capitol, Conference Room 325
415 South Beretania Street
Honolulu, Hawaii 96813

Dear Chair Lee:

Thank you for the opportunity to submit comments on HB 6, HD 2, relating to the Uniform Employee and Student On Line Privacy Protection Act.

Our firm represents the American Council of Life Insurers (“ACLI”). ACLI advocates on behalf of 280 member companies dedicated to providing products and services that promote consumers’ financial and retirement security. 90 million American families depend on our members for life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, dental and vision and other supplemental benefits. ACLI represents member companies in state, federal and international forums for public policy that supports the industry marketplace and the families that rely on life insurers’ products for peace of mind. ACLI members represent 95 percent of industry assets in the United States. Two hundred twenty-one (221) ACLI member companies currently do business in the State of Hawaii; and they represent 95% of the life insurance premiums and 99% of the annuity considerations in this State.

Today, many individuals use social media accounts and personal devices for both business and personal purposes.

ACLI and its member companies believe that an individual’s personal information should remain private and should not be subject to inspection by an employer or prospective employer.

However, legislation which seeks to protect strictly personal social media account information must simultaneously accommodate legal and regulatory requirements imposed upon life insurers that certain communications be reviewed and retained to comply with recordkeeping requirements. In addition, the legislation must recognize that employers sometimes require access to social media accounts that are used in any part for a business purpose.

Life insurance companies have legal obligations with respect to business communications made by their insurance producers and registered representatives of their affiliated broker-dealers or registered investment advisers (RIAs). State insurance laws and regulations require insurers to supervise their captive producers' communications with the public. The National Association of Insurance Commissioners (NAIC) has issued a White Paper titled “The Use of Social Media in

Insurance.” This Paper provides an overview of insurance regulatory and compliance issues associated with the use of social media, and guidance for addressing identified regulatory and compliance issues. Insurance regulators have emphasized the requirement that “[a]n insurer’s policies, procedures and controls relative to social media communications must comport with existing regulations, which include, but are not limited to, statutes and rules related to advertising and marketing, record retention, consumer privacy and consumer complaints.” To comply with these requirements, insurers must have the ability to properly supervise their producers’ social media communications, if such content is attributable to the insurer or the insurer’s products or services.

In addition, federal and state securities laws and regulations as well as self-regulatory organization rules require broker-dealers and RIAs to comply with specific requirements related to its communications with the public in order to protect investors and consumers. For example, FINRA rules require prior review of certain advertisements and other specified communications. In addition, strict recordkeeping requirements apply to business communications of registered representatives.

Further, the Securities Exchange Commission issued National Examination Risk Alert earlier this year which details regulatory requirements related to the use of social media by RIAs and their investment advisory representatives (IARs). As part of an effective compliance program, the SEC staff stressed a firm’s obligation to maintain an effective compliance program to ensure compliance with securities laws and rules related to their use of social media. Key components of an effective compliance program includes policies and procedures which establish usage guidelines, content standards, sufficient monitoring, approval of content, training, and recordkeeping responsibilities.

In large part these regulatory notices and guidelines affirm that existing approval, supervision, and recordkeeping requirements are applicable regardless of the delivery mechanism. Supervising employers have an obligation to monitor personal social media accounts utilized for business purposes, and must have in place mechanisms to capture and store relevant communications.

Life insurers want to accommodate the use of new technologies by their representatives to the extent practical. At the same time, companies must have in place compliance procedures that ensure compliance with federal and state laws and regulations as well as FINRA rules and guidance.

It should also be noted that it is not uncommon for registered representatives, producers, and investment advisory representatives to seek and obtain approval from their employers to use personal accounts for business purposes. In fact, the trend is for employers to require the use of internal systems for all business communications regardless of the social media account and electronic device enabling the communication.

Therefore, any legislation that is designed to limit an employer’s access to social media accounts must provide exceptions that permit access to such accounts to meet legal and regulatory

requirements and contain exceptions when the accounts and devices are used for business purposes.

ACLI submits that to enable a life insurer to more effectively monitor and supervise its captive producers' in their communications with the public as required by law but at the same time protect the legitimate privacy of its captive producers and representatives in their personal communications more clarity in the language of the bill is required.

ACLI suggests that Paragraph (b) of Section 3 of the proposed new Chapter, be amended to include a new subparagraph (3) to be inserted immediately following the provisions of existing subparagraph (2) (on page 6, at lines 16 to 21), as set forth below:

(3) Preventing an employer from implementing and enforcing a policy pertaining to the use of employer issued electronic communications device or to the use of an employee-owned electronic communications device that will be used for business purposes.

Lastly, paragraphs (b) and (c) of Section 5, of the proposed new Chapter, at page 14, lines 5 through 14 of the bill, grants an employee a private cause of action against an insurer for violation of the bill's provisions. ACLI objects to these provisions and requests that they be deleted from the bill.

Again, thank you for the opportunity to comment on HB 6, HD 2, relating to the Uniform Employee and Student On Line Privacy Protection Act.

LAW OFFICES OF
OREN T. CHIKAMOTO
A Limited Liability Law Company

Oren T. Chikamoto
1001 Bishop Street, Suite 1750
Honolulu, Hawaii 96813
Telephone: (808) 531-1500
E mail: otc@chikamotolaw.com



LATE

Committee: House Committee on Judiciary
Hearing Date/Time: Tuesday, February 26, 2019, 2:05 p.m.
Place: Conference Room 325
Re: *Testimony of the ACLU of Hawai'i with Comments on H.B. 6, H.D. 2, Relating to the Uniform Employee and Student Online Privacy Protection Act*

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

The American Civil Liberties Union of Hawai'i ("ACLU of Hawai'i") **writes with comments and concerns** regarding H.B. 6, H.D. 2, which aims to prohibit employers and educational institutions from demanding access to the personal online accounts such as Facebook, Snapchat, and email, of both current and prospective employees and students. Unfortunately, as written, this measure leaves serious loopholes for abuse.

Social media provides an important platform for free speech and open dialogue, and has become central to the way that we communicate in the 21st century. As social media use has increased, so too has the incentive for schools, employers, and landlords to monitor what students, employees, and tenants are expressing online. But access by those who have leverage over our education and livelihood inevitably leads to discrimination, self-censorship, and the chilling of the free expression of ideas.

For this reason, the ACLU of Hawai'i appreciates that the Legislature is taking steps to protect students and employees against unwarranted invasions of privacy. The Uniform Law Commission's Employee and Student Online Privacy Protection Act ("ULC bill"), however, fails to adequately protect students and employees, and does not even address online privacy for tenants. **The ACLU of Hawai'i prefers the alternative and more comprehensive reform measure, the Personal Online Account Privacy Act ("POAPA"), attached.** POAPA would create stronger safeguards against abuse, and include within its protection Hawaii's renters.

As currently written, H.B. 6, H.D. 2 leaves dangerous loopholes by allowing employers and educational institutions to view employees' and students' personal online account content based solely on a general — and potentially unsubstantiated — allegation of misconduct tenuously linked to the account. POAPA's protections are much stronger, requiring allegations of misconduct to point to specific content, and only allowing employers/educational institutions/landlords to access content that has been specifically identified. POAPA defines "specifically identified content," whereas H.B. 6, H.D. 2 provides no clarity regarding what would constitute "specific facts" about the employee's/student's protected personal online account sufficient to allow employers and schools to access the content of these accounts.

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

For these reasons, the ACLU of Hawai'i respectfully requests that the Committee amend this measure to address these concerns in the following ways:

1. Include within the protections of this bill the personal online accounts of tenants against invasions of privacy from their landlords.
2. **Page 1, line 8.** Under "Definitions," insert "'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."
3. **Page 6, line 12.** Replace § -3(b) of H.B. 6, H.D. 2 with Section 5 of POAPA.

Alternatively, if the Committee is not inclined to amend H.B. 6, H.D. 2, we ask that the Committee defer the measure.

Thank you for the opportunity to testify.

Sincerely,



Mandy Fernandes
Policy Director
ACLU of Hawai'i

The mission of the ACLU of Hawai'i is to protect the fundamental freedoms enshrined in the U.S. and State Constitutions. The ACLU of Hawai'i fulfills this through legislative, litigation, and public education programs statewide. The ACLU of Hawai'i 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 Hawai'i has been serving Hawai'i for 50 years.

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. (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. (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, or someone acting under the authority or on behalf of a Landlord, in relation to a Tenant or Prospective Tenant.
- (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 administrator, 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 5
- (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.