ACT 39 H.B. NO. 125

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 legislature considers this Act to be of statewide concern.

SECTION 2. The Hawaii Revised Statutes is amended by adding a new chapter to be appropriately designated and to read as follows:

"**CHAPTER**
UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

§ -1 Short title. This chapter shall be known and may be cited as the Uniform Employee and Student Online Privacy Protection Act.

§ -2 Definitions. As used in this chapter:

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

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

(1) A public or private institution; and

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

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

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

(1) A prospective employee who has:

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

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

(2) An independent contractor.

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

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

(1) A protected personal online account; or

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

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

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

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

"Protected personal online account" means any online account maintained by an employee or a student, including social media or electronic mail accounts, that is protected by a login requirement. "Protected personal online account" 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.

"Publicly available" means available to the general public.

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

"Specifically identified content" means data or information stored in a protected personal online account that is identified with sufficient particularity to distinguish the discrete individual pieces of content being sought from a substantial percentage of other data or information stored in the account with which it may share similar characteristics. The identification may be based on identification or verification by an individual creator, poster, sender, viewer or recipient of characteristics of that content that in the aggregate allow the employee or student requested to provide access to that content to distinguish that content with reasonable certainty from any other data or information stored in the account with which it may share similar characteristics.

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

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

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

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

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

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

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

(B) Disclose the content of the account, except that, without coercion and pursuant to a clear statement that acceptance is voluntary and not required, an employer may request an employee to add the employer to, or to not remove the employer from, the set of persons to which the employee grants access to the content;

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

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

(E) Turn over to the employer an unlocked personal technological device for purposes of gaining access to a protected personal online account; or

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

(A) Requirement, coercive action, or request that violates paragraph (1); or

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

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

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

(2) Complying with a federal or state law, court order, or rule of a self-regulatory organization established by federal or state statute, including a self-regulatory organization as defined in section 3(a)(26) of the Securities Exchange Act of 1934, title 15 United States Code section 78c(a)(26);

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

(4) Without requesting or requiring an employee to provide login information for or other means of authentication that provides access to the employee's protected personal online account, requesting or requiring an employee to share specifically identified content for the purpose of:

(A) Enabling an employer to comply with its own legal and regulatory obligations;

(B) Investigating an allegation, based on specific facts regarding specifically identified content, of:

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

(ii) The disclosure of information in which the employer has a proprietary interest or information the employer has a legal obligation to keep confidential; and

(C) Investigating threats to safety, including:

(i) Unlawful harassment or threats of violence in the workplace;

(ii) Threats to employer information technology or communications technology systems; or

(iii) Threats to employer property.

(c) An employer with whom content is shared by an employee for a purpose specified in subsection (b)(4) shall:

(1) Not access or view unshared content;

(2) Use the shared content only for the specified purpose; and

(3) Not alter the shared content.

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

(1) Shall not be held liable for violation of this chapter on the sole basis of having the login information;

(2) Shall not use the login information to access or enable another person to access the account;

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

(4) Shall not share the login information with any other person; and
(5) Shall dispose of the login information as soon as, as securely as, and to the extent reasonably practicable; provided that if the employer is retaining the login information for use in:
(A) An ongoing investigation of an actual or suspected breach of computer, network, or data security; or
(B) A specific criminal complaint or civil action, or the investigation thereof,
the employer shall make a reasonable effort to keep the login information secure and dispose of it as soon as, as securely as, and to the extent reasonably practicable after completion of the investigation, complaint, or action.

(e) Nothing in subsection (a) shall be construed to diminish the authority or obligation of an employer to investigate complaints, allegations, or the occurrence of prohibited discriminatory practices, including harassment, based on race, sex, or other characteristics protected under part I of chapter 378.

§ -4 Protection of student online account. (a) Subject to the exceptions in subsection (b), an educational institution shall not:
(1) Require, coerce, or request a student to:
(A) Disclose the login information for a protected personal online account;
(B) Disclose the content of the account, except that, without coercion and pursuant to a clear statement that acceptance is voluntary and not required, an educational institution may request a student to add the educational institution to, or to not remove the educational institution from, the set of persons to which the student grants access to the content;
(C) Alter the settings of the account in a manner that makes the login information for or content of the account more accessible to others;
(D) Access the account in the presence of the educational institution in a manner that enables the educational institution to observe the login information for or content of the account; or
(E) Turn over to the educational institution an unlocked personal technological device for purposes of gaining access to a personal online account; or
(2) Take, or threaten to take, adverse action against a student for failure to comply with an educational institution's:
(A) Requirement, coercive action, or request that violates paragraph (1); or
(B) Request under paragraph (1)(B) to add the educational institution to, or to not remove the educational institution from, the set of persons to which the student grants access to the content of a protected personal online account.

(b) Nothing in subsection (a) shall prevent an educational institution from:
(1) Accessing information about a student that is publicly available;
(2) Complying with a federal or state law, court order, or rule of a self-regulatory organization established by federal or state statute; or
(3) Without requesting or requiring a student to provide login information for or other means of authentication that provides access to the student's protected personal online account, requesting or requiring a student to share specifically identified content for the purpose of:

(A) Enabling an educational institution to comply with its own legal and regulatory obligations;

(B) Investigating an allegation, based on specific facts regarding specifically identified content, of:

(i) Noncompliance with an educational institution's prohibitions against education-related student misconduct of which the student has reasonable notice, is in a record, and was not created primarily to gain access to a protected personal online account; or

(ii) The disclosure of any interest or information the educational institution has a legal obligation to keep confidential; and

(C) Investigating threats to safety, including:

(i) Unlawful harassment or threats of violence at the educational institution;

(ii) Threats to the educational institution's information technology or communications technology systems; or

(iii) Threats to the educational institution's property.

(c) An educational institution with whom content is shared by a student for a purpose specified in subsection (b)(3) shall:

(1) Not access or view unshared content;

(2) Use the shared content only for the specified purpose; and

(3) Not alter the shared content.

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

(1) Shall not be held liable for violation of this chapter on the sole basis of having the login information;

(2) Shall not use the login information to access or enable another person to access the account;

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

(4) Shall not share the login information with any other person; and

(5) Shall dispose of the login information as soon as, as securely as, and to the extent reasonably practicable; provided that if the educational institution is retaining the login information for use in:

(A) An ongoing investigation of an actual or suspected breach of computer, network, or data security; or

(B) A specific criminal complaint or civil action, or the investigation thereof,

the educational institution shall make a reasonable effort to keep the login information secure and dispose of it as soon as, as securely as, and to the extent reasonably practicable after completion of the investigation, complaint, or action.

§ -5 Civil action. (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 or student may bring a civil action against the employee's employer or student's educational institution for a violation of this chapter. A prevailing employee or student may obtain:

(1) Injunctive and other equitable relief;

(2) Actual and general damages; and

(3) Costs and reasonable attorney's fees.

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

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

§ -6 Relation to Electronic Signatures in Global and National Commerce Act. This chapter modifies, limits, or supersedes the Electronic Signatures in Global and National Commerce Act, title 15 United States Code section 7001 et seq., but does not modify, limit, or supersede section 101(c) of that Act, title 15 United States Code section 7001(c), or authorize electronic delivery of any of the notices described in section 103(b) of that Act, title 15 United States Code section 7003(b).

§ -7 Relation to other state laws. In case of any conflict between any provision of this chapter and a provision of any other chapter, this chapter shall control.

§ -8 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 3. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 4. This Act shall take effect upon its approval.

(Approved June 7, 2021.)