D R A F T

FOR DISCUSSION ONLY

EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAW

Style Committee Review Draft

The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the Drafting Committee. They do not necessarily reflect the views of the Conference and its Commissioners and the Drafting Committee and its Members and Reporter. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

April 13, 2016

EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

The Committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this Act consists of the following individuals:

SAMUEL A. THUMMA, Arizona Court of Appeals, State Courts Bldg., 1501 W. Washington St., Phoenix, AZ 85007, *Chair*

JERRY L. BASSETT, Legislative Reference Service, 613 Alabama State House, 11 S. Union St., Montgomery, AL 36130

DIANE F. BOYER-VINE, Office of Legislative Counsel, State Capitol, Room 3021, Sacramento, CA 95814-4996

STEPHEN Y. CHOW, 125 Summer St., Boston, MA 02110-1624

BRIAN K. FLOWERS, 441 4th St. NW, Suite 830 South, Washington, DC 20001

WILLIAM H. HENNING, Texas A & M School of Law, 1515 Commerce St., Fort Worth, TX 76102

LISA R. JACOBS, One Liberty Place, 1650 Market St., Suite 4900, Philadelphia, PA 19103-7300

PETER F. LANGROCK, P.O. Drawer 351, 111 S. Pleasant St., Middlebury, VT 05753-1479

JAMES G. MANN, House Republican Legal Staff, Main Capitol Bldg., Room B-6, P.O. Box 202228, Harrisburg, PA 17120

ANN R. ROBINSON, 45 Memorial Cir., Augusta, ME 04330

STEVE WILBORN, 3428 Lyon Dr., Lexington, KY 40513

DENNIS D. HIRSCH, Capital University Law School, 303 E. Broad St., Columbus, OH 43215, *Reporter*

UNIFORM LAW CONFERENCE of CANADA

CLARK DALTON, 9909 – 110th St., Suite 203, Edmonton, AB T5K 2E5, *ULCC Liaison*

EX OFFICIO

RICHARD T. CASSIDY, 100 Main St., P.O. Box 1124, Burlington, VT 05402, *President*

JOHN T. MCGARVEY, 601 W. Main St., Louisville, KY 40202, *Division Chair*

AMERICAN BAR ASSOCIATION ADVISORS

FRANK H. LANGROCK, P.O. Drawer 351, 111 S. Pleasant St., Middlebury, VT 05753-1479, *ABA Advisor*

PETER J. GILLESPIE, 1000 Marquette Bldg., 140 South Dearborn St., Chicago, IL 60603, *ABA Section Advisor*

HEATHER A. MORGAN, 515 S. Flower St., Suite 2500, Los Angeles, CA 90071-2228, *ABA Section Advisor*

EXECUTIVE DIRECTOR

LIZA KARSAI, 111 N. Wabash Ave., Suite 1010, Chicago, IL 60602, *Executive Director*

Copies of this act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
111 N. Wabash Ave., Suite 1010
Chicago, Illinois 60602
312/450-6600
www.uniformlaws.org

EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

TABLE OF CONTENTS

EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

SECTION 1. SHORT TITLE. This [act] may be cited as the Employee and Student Online Privacy Protection Act.

SECTION 2. DEFINITIONS. In this [act]:

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

(2) "Educational institution" means a person that provides students at the postsecondary [or secondary] level an organized course of study or training that is academic, technical, trade-oriented, or preparatory for gaining employment. The term includes a public or private educational institution but not a home school. The term includes an agent or designee of the educational institution.

Comment [CM1]: As previously discussed, this draft's limitation to protecting students only after high school, or even with potentially including high school, is far too narrow, and draws a line where privacy rights begin at an age that is inappropriately late. For example, this proposal will fail to protect students in junior high school who are researching or discussing issues like their sexual orientation or reproductive choices and will subject them to unchecked government monitoring and oversight.

(3) "Educational institution policy" means a policy that an educational institution establishes for its institution, that is in writing or in a record, that students have reasonable notice of, and that was not created for the purpose of gaining access to a protected personal online account.

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

(5) "Employee" means an individual who provides services or labor to an employer in exchange for compensation. The term includes a prospective employee.

(6) "Employer" means a person that provides compensation to one or more employees in exchange for services or labor. The term includes an agent or designee of the employer.

(7) "Employer policy" means a policy that an employer establishes for its workplace, that

is in writing or in a record, that employees have reasonable notice of, and that was not created for the purpose of gaining access to a protected personal online account.

(8) “Login information” means a user name and password, password, or other means or credentials of authentication required to access or control

(A) a protected personal online account; or

(B) an electronic device that the employer or educational institution has not supplied or paid for and that itself provides access to or control over a protected personal online account.

(9) “Login requirement” means a requirement that login information be provided before an online account or an electronic device can be accessed or controlled.

(10) “Online” means accessed by means of a computer network or the Internet.

(11) “Person” means an individual, estate, business or nonprofit entity, public corporation, government or governmental subdivision, agency or instrumentality, or other legal entity.

(12) “Protected personal online account” means an individual’s online account that is protected by a login requirement. The term does not include:

(A) an online account that is, or those portions of an online account that are, publicly available; or,

(B) an online account that an employer or educational institution notifies the employee or student might be subject to a request for login information or content, and that

(1) the employer or educational institution supplies or pays for in full; or

(2) an employee or student creates, maintains, or uses primarily on behalf of or under the direction of an employer or educational institution in connection with that

employee's employment or that student's education;

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

(14) "Student" means an individual who participates in an educational institution's organized course of study. The term includes:

(A) a prospective student; and

(B) a parent or legal guardian of a student under the age of [majority].

SECTION 3. PROTECTION OF EMPLOYEE ONLINE ACCOUNTS

(a) Except as otherwise provided in subsection (b):

(1) An employer may not:

(A) require, coerce, or request an employee to:

(1) disclose the login information for any protected personal online account;

(2) disclose the content of any protected personal online account;

(3) alter the settings of the employee's protected personal online account in a manner that makes the login information for or content of that account more accessible to others; or

(4) access the employee's protected personal online account in the presence of the employer in a manner that enables the employer to observe the login information for or content of that account; or

(B) require or coerce an employee to add the employer to, or refrain from removing the employer from, the list of contacts who have access to the employee's protected personal online account.

(2) An employer may not take or threaten to take an adverse action against an employee for noncompliance with conduct that violates paragraph (1).

(b) Subsection (a) does not apply to employer action that is necessary to:

(1) comply with federal or state law or a court order, the rules of a self-regulatory organization defined in Section 3(a)(26) of the Securities and Exchange Act of 1934, 15 USC 78c(a)(26), or the rules of another self-regulatory organization established by federal or state statute that requires an employer to inspect or monitor an employee's protected personal online account;

(2) investigate, based on specific information about an employee's protected personal online account, whether the employee has used, is using or will use the account to violate federal or state law or an employer policy, so long as:

(A) the employer reasonably suspects that the employee has used, is using or will use the account to violate the law or employer policy; and

(B) the employer accesses only ~~accounts or~~ content that it reasonably believes to be relevant to the investigation;

(3) take adverse action against the employee for violating federal or state law or an employer policy; or

(4) protect against:

(A) a credible threat to health or safety; or

(B) a credible threat to employer information or communications technology systems or to property; or

(C) disclosure of information in which the employer has a proprietary interest or that the employer has a legal obligation to keep confidential.

Comment [CM2]: As previously discussed, including this phrase unnecessary exposes an entire account to employer review when the employer is only investigating a specific act. False allegations of misconduct will be able to be used to justify broad violations of employee privacy.

(c) Subsection (b) does not permit an employer to:

(1) use its access to, or the content of, an employee's protected personal online account obtained pursuant to subsection (b) for a purpose unrelated to a purpose specified in subsection (b);

(2) alter the settings or content of an employee's protected personal online account, unless:

(A) the employer has a proprietary interest in the settings or content;

(B) federal or state law or court order requires or authorizes the employer to alter the settings or content; or

(C) to do so is necessary to protect against a credible threat to health or safety; or

(3) require, coerce, or request an employee to provide login information unless there is no less intrusive means of accomplishing the purpose specified in subsection (b).

(d) An employer that receives the login information for or content of an employee's protected personal online account by means of lawful network- or device-monitoring technology that the employer uses for system maintenance, network security or data confidentiality purposes, or that inadvertently receives login information by any other means not in violation this [act]:

(1) does not, solely by acquiring that information, violate this section; and

(2) unless otherwise authorized by Subsection (b),

(A) may not use the login information to access or alter an employee's protected personal online account;

(B) may not record or share the login information; and

(C) shall, as soon as and to the extent practicable, dispose of the login information;

(D) may not take or threaten to take an adverse employment-related action against the employee based on the content received by means of the monitoring technology;

(E) may not record or share that content; and

(F) shall, as soon as and to the extent practicable, dispose of that content.

Provided that, with respect to subsections 3(d)(1)(C) and (F), the information reasonably necessary to an ongoing investigation of an actual or suspected breach of computer, network, or data security, may be retained temporarily and used only for the purpose of such investigation, in which case the employer shall take reasonable steps to secure the information and shall dispose of it as soon as practicable after completing that investigation.

Comment [CM3]: Change section as agreed upon in email from Dennis Hirsh to Jim Halpert dated May 26, 2016 with the subject "RE: Hawaii"

SECTION 4. PROTECTION OF STUDENT ONLINE ACCOUNTS

(a) Except as otherwise provided in subsection (b):

(1) An educational institution may not:

(A) require, coerce, or request a student to:

(1) disclose the login information for a protected personal online account;

(2) disclose the content of a protected personal online account;

(3) alter the settings of the student's protected personal online account in a manner that makes the login information for or content of that account more accessible to others; or

(4) access a protected personal online 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 that account; or

(B) require or coerce a student to add the educational institution to, or refrain from removing the employer from, the list of contacts who have access to the student's protected personal online account.

(2) An educational institution may not take or threaten to take an adverse action against a student for noncompliance with conduct that violates paragraph (1).

(b) Subsection (a) does not apply to educational institution action that is necessary to:

(1) comply with federal or state law or a court order, or with the rules of a self-regulatory organization established by federal or state statute that requires an educational institution to inspect or monitor a student's protected personal online account;

(2) investigate, based on specific information about a student's protected personal online account, whether the student has used, is using or will use the account to violate federal or state law or an educational institution policy, so long as:

(A) the educational institution reasonably suspects that the student has used, is using or will use the account to violate the law or educational institution policy; and

(B) the educational institution accesses only ~~accounts or~~ content that it reasonably believes to be relevant to the investigation;

(3) take adverse action against the student for violating federal or state law or an educational institution policy; or

(4) protect against:

(A) a credible threat to health or safety

(B) a credible significant threat to educational institution information or communications technology systems or to property; or

Comment [CM4]: A school official is a government actor. If a government actor is seeking to search the contents of a student's private account for evidence of a crime, a warrant must be required. In addition to the Constitutional problems with this provision, it would also allow law enforcement to evade warrant requirements by asking school officials to do searches on their behalf.

Comment [CM5]: This is too broad and undefined. The way this section is currently drafted, a school could access the entirety of a student social media account because the student is suspected of violating the dress code. This educational policy provision could only work if you said a school could only investigate a violation of school policy if it pertained to one of the items listed below in subsection (4)(A)-(C).

Comment [CM6]: Reasonable suspicion is too low a bar – should be probable cause (and should require a warrant for criminal investigations as noted above).

Comment [CM7]: As previously discussed, including this phrase unnecessary exposes an entire account to school-official review when the school is only investigating a specific act. False allegations of misconduct will be able to be used to justify broad violations of student privacy.

Comment [CM8]: This is vague, and could be read to sanction retaliation unrelated to the substance of a violation. Under what circumstances would taking adverse action against a student for a violation require access to their protected account? Would this be post-conviction, or upon mere suspicion? What "action" would be taken? If the action changes the contents of a website/account, in certain circumstances, it could constitute destruction of or tampering with evidence.

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

(c) Subsection (b) does not permit an educational institution to:

(1) use its access to, or the content of, a student's protected personal online account obtained pursuant to subsection (b) for a purpose unrelated to a purpose specified in subsection (b);

(2) alter the settings or content of a student's protected personal online account, unless:

(A) the educational institution has a proprietary interest in the settings or content;

(B) federal or state law or court order requires or authorizes the educational institution to alter the settings or content; or

(C) to do so is necessary to protect against a credible threat to health or safety; or

(3) require, coerce, or request a student to provide login information unless there is no less intrusive means of accomplishing the purpose specified in subsection (b).

(d) An educational institution that receives the login information for or content of a student's protected personal online account by means of lawful network- or device-monitoring technology that the educational institution uses for system maintenance, network security or data confidentiality purposes, or that inadvertently receives login information by any other means not in violation this [act]:

(1) does not, solely by acquiring that information, violate this section; and

(2) unless otherwise authorized by Subsection (b),

(A) may not use the login information to access or alter an student's protected personal online account;

(B) may not record or share the login information; and

(C) shall, as soon as and to the extent practicable, dispose of the login information;

(D) may not take or threaten to take an adverse education-related action against the student based on the content received by means of the monitoring technology;

(E) may not record or share that content; and

(F) shall, as soon as and to the extent practicable, dispose of that content.

Provided that, with respect to subsections 4(d)(1)(C) and (F), the information reasonably necessary to an ongoing investigation of an actual or suspected breach of computer, network, or data security, may be retained temporarily and used only for the purpose of such investigation, in which case the educational institution shall take reasonable steps to secure the information and shall dispose of it as soon as practicable after completing that investigation.

Comment [CM9]: This needs to change to mirror the changes to the employee section regarding the same.

SECTION 5. CIVIL ACTION.

(a) The [Attorney General] may bring a civil action against an employer or educational institution alleging a violation of this [act]. A prevailing [Attorney General] may obtain:

(1) injunctive and other equitable relief; and

(2) [a civil penalty of up to $[1000] per violation, though such penalty shall not exceed $[100,000] per occurrence.]

(b) An employee or student may bring a civil action against an employer or educational institution for a violation of this [act]. An action under subsection (a) does not preclude an action under this subsection.

(c) In an action under subsection (b) an employee or student may obtain:

(1) injunctive and other equitable relief;

(2) actual damages; and

(3) costs and reasonable attorneys' fees.

SECTION 6. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT. This [act] modifies, limits, or supersedes the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001 et seq., but does not modify, limit or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

[SECTION 7. SEVERABILITY. If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act] which can be given effect without the invalid provision or application, and to this end the provisions of this [act] are severable.]

Legislative Note: *Include this section only if this state lacks a general severability statute or a decision by the highest court of this state stating a general rule of severability.*

SECTION 8: UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this [act], consideration shall be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

SECTION 9. REPEALS; CONFORMING AMENDMENTS.

(a) ……

(b) ……

(c) ……

SECTION 10. EFFECTIVE DATE. This [act] takes effect . . . .