UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT\*

drafted by the

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

and by it

APPROVED AND RECOMMENDED FOR ENACTMENT

IN ALL THE STATES

at its

ANNUAL CONFERENCE

MEETING IN ITS ONE-HUNDRED-AND-TWENTY-FIFTH YEAR

STOWE, VERMONT

JULY 8 - JULY 14, 2016

*WithOUT Prefatory Note and Comments*

Copyright © 2016

By

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

\*The conference changed the designation of the Uniform Employee and Student Online Privacy Protection Act from Uniform to Model as approved by the Executive Committee on July 7, 2022.

August 24, 2022

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

 SECTION 1. SHORT TITLE**.** This [act] may be cited as the UniformEmployee 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, accessible to the account holder, and not publicly available.

(2) “Educational institution” means a person that provides students at the postsecondary level an organized program of study or training which is academic, technical, trade-oriented, or preparatory for gaining employment and for which the person gives academic credit. The term includes:

(A) a public or private institution; and

(B) an agent or designee of the educational institution.

(3) “Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(4) “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. The term includes:

(A) a prospective employee who:

 (i) has expressed to the employer an interest in being an employee; or

 (ii) has applied to or is applying for employment by, or is being recruited for employment by, the employer; and

(B) an independent contractor.

(5) “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. The term includes an agent or designee of the employer.

(6) “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, 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.

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

(8) “Online” means accessible by means of a computer network or the Internet.

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

 (10) “Protected personal online account” means an employee’s or student’s online account that is protected by a login requirement. The term does not include an online account or the part of an online account:

 (A) that is publicly available; or

 (B) that the employer or educational institution has notified the employee or student might be subject to a request for login information or content, and which:

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

 (ii) the employee or student creates, maintains, or uses primarily on behalf of or under the direction of the employer or educational institution in connection with the employee’s employment or the student’s education.

 (11) “Publicly available” means available to the general public.

(12) “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.

(13) “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.

(14) “Student” means an individual who participates in an educational institution’s organized program of study or training. The term includes:

 (A) 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

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

***Legislative Note:*** *A state should insert the appropriate age of majority in place of the bracketed material in paragraph (14)(B).*

 SECTION 3. PROTECTION OF EMPLOYEE ONLINE ACCOUNT.

 (a) Subject to the exceptions in subsection (b), an employer may 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 an employer may request an employee to add the employer to, or not remove the employer from, the set of persons to which the employee grants access to the content;

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

 (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

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

(A) an employer requirement, coercive action, or request that violates paragraph (1); or

(B) an employer request under paragraph (1)(B) to add the employer to, or 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 which 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 defined in Section 3(a)(26) of the Securities and Exchange Act of 1934, 15 U.S.C. § 78c(a)(26); or

 (3) requiring or requesting, based on specific facts about the employee’s protected personal online account, access to the content of, but not the login information for, the account in order to:

 (A) ensure compliance, or investigate non-compliance, with:

(i) federal or state law; or

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

 (B) protect against:

 (i) a threat to safety;

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

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

 (c) An employer that accesses employee content for a purpose specified in subsection (b)(3):

 (1) shall attempt reasonably to limit its access to content that is relevant to the specified purpose;

 (2) shall use the content only for the specified purpose; and

 (3) may not alter the content unless necessary to achieve the specified purpose.

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

(2) shall make a reasonable effort to keep the login information secure;

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

(4) shall, if the employer retains the login information for use in an ongoing investigation of an actual or suspected breach of computer, network, or data security, make a reasonable effort to keep the login information secure and dispose of it as soon as, as securely as, and to the extent reasonably practicable after completing the investigation.

SECTION 4. PROTECTION OF STUDENT ONLINE ACCOUNT.

 (a) Subject to the exceptions in subsection (b), an educational institution may 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 an educational institution may request a student to add the educational institution to, or 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; or

 (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

 (2) take, or threaten to take, adverse action against a student for failure to comply with:

(A) an educational institution requirement, coercive action, or request, that violates paragraph (1); or

(B) an educational institution request under paragraph (1)(B) to add the educational institution to, or 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) requiring or requesting, based on specific facts about the student’s protected personal online account, access to the content of, but not the login information for, the account in order to:

 (A) ensure compliance, or investigate non-compliance, with:

(i) federal or state law; or

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

 (B) protect against:

 (i) a threat to safety;

 (ii) a threat to educational institution information technology or communications technology systems or to educational institution property; or

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

 (c) An educational institution that accesses student content for a purpose specified in subsection (b)(3):

 (1) shall attempt reasonably to limit its access to content that is relevant to the specified purpose;

 (2) shall use the content only for the specified purpose; and

 (3) may not alter the content unless necessary to achieve the specified purpose.

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

(2) shall make a reasonable effort to keep the login information secure;

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

(4) shall, if the educational institution retains the login information for use in an ongoing investigation of an actual or suspected breach of computer, network, or data security, make a reasonable effort to keep the login information secure and dispose of it as soon as, as securely as, and to the extent reasonably practicable after completing the investigation.

# SECTION 5. CIVIL ACTION.

 (a) The [Attorney General] may bring a civil action against an employer or educational institution for 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] 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 individual’s employer or educational institution for a violation of this [act]. A prevailing employee or student may obtain:

 (1) injunctive and other equitable relief;

 (2) actual damages; and

 (3) costs and reasonable attorney’s fees.

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

(d) This [act] does not affect a right or remedy available under law other than this [act].

***Legislative Note:*** *In subsection (a) an enacting state should replace “[Attorney General]” with the appropriate enforcement authority for the state.*

*In subsection (a)(2), an enacting state that opts to empower its enforcement authority to seek civil penalties for violation of the act should replace “$[1000]” with the penalty amount it determines is appropriate, and should replace “$[100,000]” with the amount it determines should be the maximum penalty for all violations arising from the same event.*

SECTION 6. UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this [act], consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

 SECTION 7. 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 8. 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 9. REPEALS; CONFORMING AMENDMENTS.

 (a) ……

 (b) ……

 (c) ……

***Legislative Note:****UESOPPA is promulgated as an integrated whole by the Uniform Law Commission. A jurisdiction that wishes to adopt only a part of UESOPPA will need to make significant adjustments to it.*

 *A jurisdiction that wishes to adopt only the employee provisions of the UESOPPA should consider at least the following adjustments, including renumbering to account for omitted provisions:*

*Section 1: Short Title.* Revise appropriately

*Section 2: Definitions.*

 *(2) Educational institution.* Omit

 *(6) Login information.* Remove reference to “educational institution” and “student”

 *(10) Protected personal online account.* Remove references to “educational institution” and “student”

 *(14) Student.* Omit

*Section 4: Protection of Student Online Account.* Omit

*Section 5. Civil Action.* Remove references to “educational institution” and “student”

 *A jurisdiction that wishes to adopt only the student provisions of the UESOPPA should consider at least the following adjustments, including renumbering to account for omitted provisions:*

*Section 1: Short Title.* Revise appropriately

*Section 2: Definitions.*

 *(4) Employee.*Omit

 *(5) Employer.*Omit

 *(6) Login information.* Remove reference to “employer” and “employee”

 *(10) Protected personal online account.*Remove references to “employer” and “employee”

*Section 3. Protection of Employee Online Account.*Omit

*Section 5. Civil Action.* Remove references to “employer” and “employee”

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