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

WITH PREFATORY NOTE AND COMMENTS

*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

ABOUT ULC

The **Uniform Law Commission** (ULC), also known as National Conference of Commissioners on Uniform State Laws (NCCUSL), now in its 125th year, provides states with non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law.

ULC members must be lawyers, qualified to practice law. They are practicing lawyers, judges, legislators and legislative staff and law professors, who have been appointed by state governments as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands to research, draft and promote enactment of uniform state laws in areas of state law where uniformity is desirable and practical.

- ULC strengthens the federal system by providing rules and procedures that are consistent from state to state but that also reflect the diverse experience of the states.

- ULC statutes are representative of state experience, because the organization is made up of representatives from each state, appointed by state government.

- ULC keeps state law up-to-date by addressing important and timely legal issues.

- ULC's efforts reduce the need for individuals and businesses to deal with different laws as they move and do business in different states.

- ULC's work facilitates economic development and provides a legal platform for foreign entities to deal with U.S. citizens and businesses.

- Uniform Law Commissioners donate thousands of hours of their time and legal and drafting expertise every year as a public service, and receive no salary or compensation for their work.

- ULC's deliberative and uniquely open drafting process draws on the expertise of commissioners, but also utilizes input from legal experts, and advisors and observers representing the views of other legal organizations or interests that will be subject to the proposed laws.

- ULC is a state-supported organization that represents true value for the states, providing services that most states could not otherwise afford or duplicate.

UNIFORM 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, Room B-6, Main Capitol Bldg., P.O. Box 202228, Harrisburg, PA 17120

ANN R. ROBINSON, 324 Gannett Dr., Suite 200, South Portland, ME 04106

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

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

EX OFFICIO

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

JOHN T. MCGARVEY, 401 S. 4th 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 S. 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

UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

TABLE OF CONTENTS

UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

PREFATORY NOTE

Today, most individuals have online accounts of some type. These include social media accounts, bank accounts, and email accounts, among others. Generally, when someone asks for access to the login information for, or content of, a personal online account, an individual is free to say "no." But that is less true in the employment and educational contexts. Employers may have the power to coerce access to personal online accounts of individuals who are, or seek to become, their employees. Similarly, educational institutions may have coercive power over those who are, or seek to become, their students. When an employer or educational institution asks for the login information for, or content of, an employee's or student's online account, that person may find it difficult to refuse. In recent years, there have been a number of reports of incidents where employers and educational institutions have demanded, and received, such access.

This has led a number of states to consider or pass legislation protecting employee and student privacy with respect to their personal online accounts. *See* http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx (last visited August 24, 2016). These acts and bills vary widely. For example, some protect only employees, *see, e.g.,* CONN. GEN. STAT. § 31-40X, some protect only students, *see, e.g.,* MD. CODE ANN., EDUC., § 26-401, and some protect both employees and students, *see, e.g.,* MICH. COMP. LAWS § 37.271-37.278. Some protect only social networking accounts, *see, e.g.,* DEL. CODE ANN. tit. 19, § 709A, while others cover additional login-protected personal online accounts such as email or messaging accounts, *see, e.g.,* R.I. GEN. LAWS § 28-56-1; UTAH CODE ANN. § 34-48-102. Some of the education-related bills and acts limit themselves to post-secondary schools, *see, e.g.,* MD. CODE. ANN., EDUC., § 26-401, while others extend protections as early as kindergarten, *see, e.g.,* MICH. COMP. LAWS § 37.272. The existing bills and acts also differ in other, important ways. This creates a need for greater uniformity and consistency in state approaches to this issue.

The Uniform Employee and Student Online Privacy Protection Act (UESOPPA) provides a model for states to adopt. Its principal goal is to enable employees and students to make choices about whether, and when, to provide employers and educational institutions with access to their personal online accounts. To this end, the act prohibits employers and educational institutions from requiring, coercing, or requesting that employees or students provide them with access to the login information for, or content of, these accounts. It further prohibits employers and educational institutions from requiring or coercing an employee or student to add them to the list of those given access to the account (to "friend" them, in common parlance), though it does not prohibit them from *requesting* to be added to such a list.

Employee and student privacy interests extend, not only to their social networking accounts, but also to their email, messaging, financial, and other login-protected online accounts. UESOPPA accordingly adopts the approach of those jurisdictions whose statutes cover this broader ground. The term "protected personal online account" defines this broader scope. It also sets some important limits on it. As the term makes clear, the act governs only "online"

accounts and does not cover those accounts that are not accessed by means of a computer network or the Internet. The act governs accounts that are "protected" by a login requirement and does not cover employee or student online accounts, or those portions thereof, which are publicly available. The act governs "personal" online accounts and does not cover those that the employer or educational institution supplies or pays for in full, or that the employee or student creates or uses primarily on behalf of or under the direction of the employer or educational institution, so long as the employer or educational institution has notified the employee or student that it might request the login information for, or content of, such an account. The terms "online," "protected," and "personal" thus go a long way toward defining the scope of the act.

UESOPPA seeks to bolster individual choice. It therefore allows employees and students voluntarily to share non-public "protected personal online account" content and login information with their employers or educational institutions, should they choose to do so.

UESOPPA is divided into 10 sections. Section 1 is the short title. Section 2 defines important terms used in the act. Section 3 delineates protections for employee protected personal online accounts and creates exceptions to these protections. Section 4 delineates protections for student protected personal online accounts and creates exceptions to these protections. Section 5 provides remedies for violations of the act, including a private right of action. The remainder of the act contains provisions generally included by the National Conference of Commissioners on Uniform State Laws in Uniform Acts. Section 6 contains a uniformity of application and construction provision. Section 7 modifies portions of the Electronic Signatures in Global and National Commerce Act. Section 8 is a suggested severability provision. Section 9 is a placeholder provision should enactment in any given state repeal or require conforming amendments to other law. Section 10 is an effective date provision.

UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

SECTION 1. SHORT TITLE. This [act] may be cited as the Uniform 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, 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).*

Comment

The definition of "content" includes those portions of an individual's protected personal online account that the account holder has access to and could turn over to an employer or educational institution. It thus corresponds to the act's core purpose which is to protect employees and students against coercive demands and requests. The definition makes clear that the act does not prohibit employers or educational institutions from accessing publicly available information.

The definition of "educational institution" encompasses only post-secondary educational institutions. This is consistent with the majority of existing state laws. *See, e.g.,* CAL. EDUC. CODE § 99121; DEL. CODE ANN. tit. 14, § 8102; MD. CODE ANN., EDUC., § 26-401; UTAH CODE ANN. § 53B-25-102. The term includes both public and private educational institutions. It further includes an agent or designee of an educational institution such as a teacher, administrator, or coach. The definition narrows the scope to those educational institutions that offer "an organized program of study or training that is academic, technical, trade-oriented, or preparatory for gaining employment" and that grant academic credit. This limiting language excludes educational programs, such as a music school at which the individual takes guitar

lessons, that do not typically serve as gatekeepers to degrees and employment and so are not in a position to coerce access to their students' protected personal online accounts.

The definition of "employee" includes not only full-time employees but also part-time employees, independent contractors, unpaid interns, and prospective employees. An employer may have coercive power over each of these categories of individuals. The act accordingly applies to them all. The act applies to prospective employees, where no employer-employee relationship has yet been created nor compensation paid, since employers can hold significant leverage over those who wish to work for them. This important addition creates a risk of overbreadth since, in some sense, any individual is a "prospective employee" of any given employer. To address this, the act covers only a prospective employee who has "expressed to the employer an interest in being an employee of the employer, has applied to or is applying to, or is being recruited by, the employer." This limitation narrows the field to those individuals with respect to whom the employer is likely to hold significant coercive power.

The definition of "employer" builds on the broad definition of employee and includes an agent or designee of an employer such as a supervisor, manager, or executive.

The definition of "login information" refers not only to passwords and usernames but also to any "other means or credentials of authentication" required to control or gain access to an online account. This broad, technology-neutral language can adapt to emerging methods of authentication such as bio-metric identification. The definition recognizes that some individuals stay logged into their personal accounts on their personal devices. It therefore includes login information for "an electronic device . . . which itself provides access to or control over a protected personal online account."

The definition of "online" includes accounts accessed "by means of a computer network or the Internet." It does not include an individual's computer, or those portions thereof, that are not connected to a computer network or the Internet. Other statutes, such as the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, offer some protection in such contexts.

The definition of "protected personal online account" provides a roadmap for determining whether a given account is covered by the act. The act governs only those online accounts that are "protected" and does not cover employee or student online accounts, or those portions thereof, which are publicly available. The act governs only "personal" online accounts and does not cover those that the employer or educational institution supplies or pays for in full, or that the employee or student creates or uses primarily on behalf of or under the direction of the employer or educational institution, so long as the employer or educational institution has notified the employee or student that it might request the login information for or content of such an account. The act governs only "online" accounts and does not cover accounts that are not accessed by means of a computer network or the Internet.

The definition of "student" faces the same overbreadth issue as the definition of employee. Virtually any individual could be viewed as a "prospective student" of a given educational institution. To address this, the definition treats as a prospective student only an individual that "expresses an interest in being admitted to, applies for admission to, or is being

recruited by, the educational institution." This limitation narrows the field to those individuals with respect to whom the educational institution is likely to hold significant coercive power. Because some students are minors, the definition of "student" includes "a parent or guardian" of a minor student so that these parents and guardians and their minor students have the same protections as students who have reached the age of majority.

The definitions of "electronic," "person" and "record" are standard definitions used by the National Conference of Commissioners on Uniform State Laws and are identical to those used in numerous other Uniform Acts.

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.

Comment

Section 3 is divided into four subsections: subsection (a), which prohibits an employer from taking certain actions that would compromise the privacy of an employee's protected personal online account; subsection (b), which creates exceptions to these prohibitions; subsection (c), which provides additional protections for employee content if an employer accesses employee content for a purpose specified in subsection (b)(3); and subsection (d), which provides additional protections when an employer, by virtue of lawful system monitoring technology, gains access to login information for an employee's protected personal online account.

Subsection 3(a)(1) provides that an employer may not require, coerce, or request that the employee provide it with access to login information or content. However, it allows an employer to request (though not to require or coerce) that the employee add it to the list of persons to

whom the employee grants access to the account (to "friend" them, in common parlance). The intent is to balance the need to protect employees against coercion with employees' understandable interest in forming social connections with one another and with their employer.

Subsection 3(a)(2) provides that an employer may not punish an employee for failing to comply with a requirement, coercive action, or request referred to in subsection 3(a)(1). This ensures that, even with respect to a request to be added to the list of contacts, the employee retains the ability to say "no" without fear of reprisal.

Subsection 3(b) contains exceptions to the prohibitions in subsection 3(a). Subsection 3(b)(2) lifts the act's prohibitions where an employer needs to access employee content or login information in order to comply with a federal or state law or court order, or with the rule of a self-regulatory organization established by federal or state statute. The principal self-regulatory organizations intended here are those defined the Securities and Exchange Act of 1934, 15 U.S.C. § 78c(a)(26). These self-regulatory organizations must access certain employee online account information in order to fulfill their obligations to prevent market fraud and manipulation. The act exempts them so that they can perform this vital role. This exception is a narrow one. It is intended to apply only to self-regulatory organizations, like those identified in the Securities and Exchange Act of 1934, that are established by a federal or state statute. It is not intended to encompass a self-regulatory organization that an industry group or sector establishes absent such statutory recognition.

Subsection 3(b)(3) establishes exceptions with respect to certain employer demands or requests for *content*. It does not create any exceptions for employer demands or requests for *login information*. This important distinction is intended to ensure that login information, the disclosure of which poses special concerns and dangers, including to cybersecurity, remains fully protected even in those exceptional situations in which content does not.

Subsection 3(b)(3)(A)(ii) lifts the subsection 3(a) prohibitions regarding accessing content (but not those prohibitions regarding login information) when an employer is investigating whether an employee has violated an employer policy. This is intended to be a narrow exception. As the act makes clear, it applies only where: an employer bases its demand or request on "specific facts about the employee's protected personal online account;" the employer policy is in a record of which the employee had advance notice; the employer policy concerns "work-related employee misconduct;" and the employer created the policy for a bona fide business purpose and not primarily as a justification for accessing protected employee online content. These conditions are intended to ensure that the exception is used only for good faith investigations into work-related employee misconduct, and not to undermine the act's prohibitions absent compliance with this narrow exception.

The subsection 3(b) exceptions limit the scope of the subsection 3(a) prohibitions. ***They do not create affirmative rights.*** Thus, if a 3(b) exception were to lift the 3(a) prohibitions with respect to a particular employer action, but another law (e.g., the Fourth Amendment) were to forbid such employer action, the action in question would remain illegal under that other law. The subsection 3(b) exceptions function solely to limit the subsection 3(a) prohibitions. They do

not affect other federal or state laws that also may prohibit the actions in question and, instead, would require reference to other law to determine if such actions are lawful.

Subsection 3(c) clarifies that, even where the subsection 3(b)(3) exception applies, it does not give employers carte blanche to access or alter the content of the employee's protected account. Instead, subsection 3(c) requires an employer utilizing the exception to reasonably attempt to limit its access to content that is relevant to the purpose that justified the exception, use the content only for this purpose, and refrain from altering content.

Subsection 3(d) takes account of the fact that employers, in conducting information and communications system monitoring required for maintenance and cybersecurity, may inadvertently gain access to login information for an employee's protected personal online account. It makes clear that, while such capture of login information does not, in itself, violate the act, employers must exercise care with respect to such information. They should take reasonable steps to secure the login information and should dispose of it as soon and as securely as is reasonably practicable.

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.

Comment

Section 4 is similar to Section 3 except for the fact that it protects students from educational institution demands and requests for access, rather than employees from employer demands and requests. The comments that follow Section 3 apply equally to Section 4, with the exception that "student" should be substituted for "employee," and "educational institution" for "employer."

Subsection 4(b)(2) creates an exception for educational institution compliance with the rules of self-regulatory organizations established by federal or state statute. This exception is intended to apply only to self-regulatory organizations that a federal and state statute recognizes in the way that the Securities and Exchange Act of 1934, 15 U.S.C. § 78c(a)(26), recognizes self-regulatory organizations for certain employers. It is not intended to encompass a self-regulatory organization that an educational group or sector establishes absent such statutory recognition.

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.

Comment

Subsection 5(a)(2) gives an enacting state the option to define a maximum civil penalty

for each violation, and a maximum civil penalty for all violations caused by the same act. The cap on the total penalty for all violations caused by a single act is intended to prevent civil penalties from escalating to disproportionate levels. For example, absent such a cap, where a state set the maximum civil penalty per violation at $1000, an employer that sent an e-mail to 1000 employees requesting the login information for, or content of, their protected online accounts in violation of the act would face a penalty of up to $1,000,000 for this single act. Subsection 5(a)(2) is intended to avoid such disproportionate penalties by capping the maximum civil penalty for all violations caused by the same act at a level that the enacting state deems appropriate.

Subsection 5(b) establishes a private right of action for employees and students.

No mental state is specified for a cause of action under either subsection 5(a) or 5(b).

Subsection 5(d) states that the act does not displace or otherwise affect a right or remedy that may be available under law other than this act.

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).

Comment

This section responds to the specific language of the Electronic Signatures in Global and National Commerce Act and is designed to avoid preemption of state law under that federal legislation.

[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"

Comment

An enacting state may need to amend the state's laws by repealing any conflicting statutory provisions. It may place these repeals in this section of the act.

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