Uniform Employee Student Online Privacy Protection Act Draft (UESOPPA)	ACLU Employee and Student User Name and Password Privacy Protection Model Bill (ACLU model)	Industry Employee Online Privacy Act 2016 (Industry model)	Analysis of Substantive Differences
SECTION 1. SHORT TITLE. This [act] may be cited as the Employee and Student Online Privacy Protection Act.		**Section 1 – Title.** This chapter is known as the "Employee Online Privacy Act."	The Industry model only applies to employees, whereas the UESOPPA and ACLU model would apply to employees and students
SECTION 2. DEFINITIONS. In this [act]: (1) "Educational institution" means a person that provides students at the postsecondary [or secondary] level an organized course of study that is academic, technical, trade-oriented or preparatory for gaining employment in a recognized occupation. The term includes a public or private educational institution but not a home school. The term includes a teacher, coach, school administrator or other person that acts, or that a student reasonably believes is acting, on behalf of the educational institution.	(E) "Educational institution" shall mean: (1) A private or public school, institution or school district, or any subdivision thereof, that offers participants, students or trainees an organized course of study or training that is academic, trade-oriented, or preparatory for gainful employment, as well as school employees and agents acting under the authority or on behalf of an educational institution; or (2) A state or local educational agency authorized to direct or control an entity in Section 1(E)(1).	**Section 2 – Definitions.** As used in this chapter: (1) "Adverse action" means to discharge, threaten, or otherwise discriminate against an employee	Unlike the ACLU model, the UESOPPA limits to postsecondary or secondary institutions. The UESOPPA also excludes home school. Unlike the ACLU model, UESOPPA more broadly includes agencies authorized to direct/control the school/institution/district/subdivision. UESOPPA does not define adverse action, but it does use the term in the act. The ACLU model does not use or define this term.

		in any manner that affects the employee's employment, including compensation, terms, conditions, location, rights, immunities, promotions, or privileges.	
(2) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.			
(3) "Employee" means an individual who provides services or labor to an employer in exchange for compensation. The term includes a prospective employee.	(C) "Employee" shall mean an individual who provides services or labor for an employer for wages or other remuneration. (B) "Applicant" shall mean an applicant for employment.		Both the ACLU and the UESOPPA have similar definitions for employee. The UESOPPA definition includes a prospective employee.
(4) "Employer" means a person that provides compensation to one or more employees in exchange for services or labor. The term includes a person that acts, or that an employee reasonably believes is acting, on behalf of the employer.	(D) "Employer" shall mean a person who is acting directly as an employer, or indirectly in the interest of an employer, on behalf of a for-profit, non-profit, charitable, governmental or other organized entity, in relation to an employee.	(2) "Employer" means a person, including the state or a political subdivision of the state, that has one or more workers employed in the same business, or in or about the same establishment, with the right to control and direct the work provided by such workers.	The three acts define employer differently. The Industry model includes the state or political subdivision in the meaning of a person. The ACLU model also includes governmental entities. The UESOPPA does not apply to "a federal, state, county, or local law enforcement agency that seeks to view the contents of, but not to obtain login information for, an employee's protected personal online account." (See UESOPPA Section 3(b)(3)-(4).) This is bracketed language in the UESOPPA.

			Rather than providing compensation as a basis for defining employer (as is done in the UESOPPA), the Industry model determines an employer as one "with the right to control and direct the work provided by such workers." This would seemingly include unpaid interns. The ACLU model defines employer similarly defines this term in the context of right to control.
(5) "Login information" means a user name and password, password, or other means or credentials of authentication required to access or control a protected personal online account or to access or control 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.	(G) "Specific content" shall mean data or information on a personal social media account that is identified with sufficient particularity to: (1) Demonstrate prior knowledge of the content's details; and	(3) "Law enforcement agency" is as defined in **[insert section]**.	

(6) "Login requirement" means a requirement that login information be provided before an online account or an electronic device can be accessed or controlled. [(7) "Metadata" means data that provides information about other data.] (8) "Online" means accessed 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 individual's online account that is protected by a login requirement. In a situation in which an employee or student has reasonable notice that the employer or educational institution may require login information for, or access to, the online account, the term does not include:	(2) Distinguish the content from other data or information on the account with which it may share similar characteristics. (A) "Personal social media account" shall mean an account with an electronic medium or service where users may create, share, and view user-generated content, including, but not limited to, uploading or downloading videos or still photographs, blogs, video blogs, podcasts,	(4) (a) "Personal Internet account" means an individual's online account that requires login information in order to access or control that account. (b) "Personal Internet account" does not include an online account that:	Both UESOPPA and the Industry model define a personal account in terms of requiring log-in credentials. The ACLU model does not address log-in credentials. It also applies more narrowly to social media accounts involving certain user-generated content.

(A) an employee's online account that an employer supplies or pays for[, except where an employer pays only for additional features or enhancements]; (B) an online account that an employee creates, maintains, or uses primarily on behalf of or under the direction of an employer in connection with that employee's employment, [or that an employee obtained by virtue of the employee's employment relationship with the employer]; (C) a student's online account that an educational institution supplies or pays for[, except where an educational institution pays only for additional features or enhancements]; or (D) an online account that a student creates, maintains, or uses primarily on behalf of or under the direction of an educational institution in connection with that student's education, [or that a student obtains by virtue of the student's educational relationship with the educational institution]. (11) "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.	messages, e-mails, or Internet website profiles or locations. Personal social media account does not include an account opened at an employer's behest, or provided by an employer, and intended to be used solely on behalf of the employer, or to an account opened at a school's behest, or provided by a school, and intended to be used solely on behalf of the school.	(A) an employer or educational institution supplies or pays for (except where an employer or educational institution pays only for additional feature sets or enhancements) or (B) an account that is used exclusively for a business purpose of the employer.	All three provide for similar exclusions related to accounts that an employer pays for/supplies or that an employee uses on the job. Both the ACLU model and the UESOPPA apply to accounts supplied by educational institutions. Unlike Industry model and the ACLU model, the UESOPPA additionally requires reasonable notice. All three provide similar, but differently worded exclusions for accounts used on the job. UESOPPA language may have a broader effect. UESOPPA excludes an account used "*primarily* on behalf of or under the direction of an employer," whereas, Industry model excludes accounts used "*exclusively* for a business purpose" and the ACLU model excludes accounts used "used *solely* on behalf "of the employer or school. The UESOPPA language is broader in that it would likely capture accounts occasionally used for non-business purposes.

(12) "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].	(H) "Student" shall mean any student, participant or trainee, whether full-time or part-time, in an organized course of study at an educational institution. (F) "Prospective student" shall mean an applicant for admission to an educational institution.		Unlike the ACLU model, the UESOPPA definition of student includes a parent or legal guardian of a student under the age of majority.
SECTION 3. APPLICABILITY. (a) Except as otherwise provided in subsection (b), this [act] applies to an employer that requires, coerces or requests an employee, and an educational institution that requires, coerces or requests a student, to provide the login information for, disclose the content of, or alter the settings of a protected personal online account, or that requires or coerces an employee or student to add the employer or educational institution to the list of contacts associated with the account. (b) This [act] does not apply to (1) employer or educational institution access to an online	Section 6. Nothing in this Act shall prevent an employer or educational institution from:	Section (3)(1)This chapter does not prohibit an employer from doing any of the following:	All three clarify that the act is not intended to apply/prohibit conduct

account or the part of an online account that is available to the general public or not protected by a login requirement; (2) employer or educational institution actions, other than the actions described in subsection (a), that are necessary to maintain or monitor the functioning of the employer's or educational institution's information and communications technology systems; [(3) the federal government;] [(4) a federal, state, county, or local law enforcement agency that seeks to view the contents of, but not to obtain login information for, an employee's protected personal online account;] [(5) a federal, state, county, or local department of corrections, including an authorized private entity that performs the same correctional functions as a state, county, or local department of corrections, that seeks to view the content of, but not to obtain login information for, an employee's protected personal online account;] or	(A) Accessing information about an applicant, employee, student, or prospective student that is publicly available;	(4) This chapter does not prohibit or restrict an employer from viewing, accessing, or using information about an employee or applicant that can be obtained without the information described in Subsection (1) or that is available in the public domain. Section (3)(3) This chapter does not prohibit or restrict an employer from complying with a duty to screen employees or applicants before hiring or to monitor or retain employee communication […] in the course of a law enforcement employment application or law enforcement officer conduct investigation performed by a law enforcement agency	associated with publically available accounts or portions thereof. Both UESOPPA and the Industry model address exceptions for law enforcement activities. In bracketed language, the UESOPPA provision is broader, providing an exclusion from applicability for federal, state, county, or local law enforcement agencies for the purposes of viewing the contents, but not to obtain log-in information. More narrowly, the Industry model language merely provides an exclusion related to hiring process or employee monitoring activities.

(6) an individual who employs another individual to provide care for a minor child, elderly adult or other vulnerable person.			
SECTION 4. EMPLOYEE PROTECTIONS. (a) Except as otherwise provided in subsections (b) and (c): (1) An employer may not: (A) require, coerce, or request an employee to: (1) disclose the login information for a protected personal online account; (2) disclose the content [or metadata] of a protected personal online account;	Section 2. An employer shall not: (A) Require, request, or coerce an employee or applicant to disclose the user name and password, password, or any other means of authentication, or to provide access through the user name or password, to a personal social media account;	**Section 3 – Prohibited and Permitted Activities** Employer may not request disclosure of information related to personal Internet account. An employer may not do any of the following: (1) request or require an employee or an applicant for employment to disclose a username and password, or a password that allows access to the employee's or applicant's personal Internet account; or	All three state that the employer cannot *require* or *request* that an employee disclose login information. Unlike the Industry model, both the ACLU model and the UESOPPA state that an employer may not *coerce* the information. In addition to a prohibition on requesting username or password, the ACLU model also prohibits requiring/requesting/coercing *"any other means of authentication, or to provide access through the user name or password*." Unlike the UESOPPA, the Industry model and the ACLU model do not address metadata.

(3) alter the settings of a protected personal online account, including settings that affect whether another individual is able to view the content of the account; or	Section 2. An employer shall not: (C) […] require, request, or otherwise coerce an employee or applicant to change the settings that affect a third party's ability to view the contents of a personal social networking account.		Unlike Industry model, the ACLU model and the UESOPPA prohibits requiring, requesting, or coercing the employee to change account settings in a way that would allow others to see the contents of the account.
(4) access the content of a protected personal online account in the presence of the employer in a manner that enables the employer to observe the content; or	(B) Require, request, or coerce an employee or applicant to access a personal social media account in the presence of the employer in a manner that enables the employer to observe the contents of such account; or	An employer may not do any of the following: (3) compel an employee or an applicant for employment to access a personal Internet account in the presence of the employer in a manner that enables the employer to observe the contents of the employee's or applicant's personal Internet account.	The UESOPPA and ACLU model says that the employer cannot require, coerce, or request shoulder surfing, whereas the Industry model prohibits only requiring (but allows requesting). UESOPPA also prohibits requiring or requesting that the employee disclose the *content* of the account (this is distinct from shoulder surfing since it could be disclosed in other ways.)
(B) require or coerce an employee to add the employer to the list of contacts associated with the employee's protected personal online account.	Section 2. An employer shall not: (C) Compel an employee or applicant to add anyone, including the employer, to their list of contacts associated with a personal social media account […]	An employer may not do any of the following: (2) compel an employee or applicant for employment to add the employer or an employment agency to the employee's or applicant's list of contacts associated with a personal Internet account;	All three say that an employer cannot require/coerce/compel (but can request) that an employee add the employer to the account's list of contacts

(2) An employer may not take or threaten to take an adverse action against an employee for noncompliance with a requirement, coercive demand, or request that violates paragraph (1).	Section 3. An employer shall not: (A) Take any action or threaten to take any action to discharge, discipline, or otherwise penalize an employee for an employee's refusal to disclose any information specified in Section 2(A), for refusal to take any action specified in Section 2(B) or for refusal to add the employer to their list of contacts associated with a personal social media account or to change the settings that affect a third party's ability to view the contents of a personal social media account, as specified in Section 2(C); or (B) Fail or refuse to hire any applicant as a result of the applicant's refusal to disclose any information specified in Section 2(A) for refusal to take any action specified in Section 2(B) or for refusal to add the employer to their list of contacts associated with a personal social media account or to change the settings that affect a third party's ability to view the contents of a personal	An employer may not do any of the following: (4) take adverse action, fail to hire, or otherwise penalize an employee or applicant for employment for failure to disclose information or take actions specified in subsection (1)-(3). ["Adverse action" means to discharge, threaten, or otherwise discriminate against an employee in any manner that affects the employee's employment, including compensation, terms, conditions, location, rights, immunities, promotions, or privileges.]	All three address (adverse) actions, for an employee's (or prospective employee's) refusal to comply with a prohibited action. The Industry model and the ACLU model define adverse action in similar ways.

	social media account, as specified in Section 2(C).		
(3) An employer that, without violating paragraph (1), inadvertently acquires login information for, or the login-protected content [or metadata] of, an employee's protected personal online account: (A) does not, solely by acquiring that information, violate this section; (B) may not use the login information to access or alter an employee's protected personal online account; (C) may not take or threaten to take an adverse employment-related action against the employee based on the content [or metadata] of the employee's protected personal online account; (D) may not record or share the login information for, or the content [or metadata] of, the employee's protected personal online account; (E) shall, as soon as and to the extent practicable, dispose of the login information for, and the content [or metadata] of, the employee's protected personal online account; [and]	Section 7. If an employer or educational institution inadvertently receives the user name and password, password, or other means of authentication that provides access to a personal social media account of an employee, applicant, student, or prospective student hat monitors the employer or school's network or employer-provided or school-provided devices, the employer or school is not liable for having the information, but may not use the information to access the personal social media account of the employee, applicant, student, or prospective student, may not share the information with anyone, and must delete the information immediately or as soon as is reasonably practicable.		Both UESOPPA and the ACLU model address issues of inadvertent disclosure. The Industry model does not. The ACLU model is narrower in that the provision covers inadvertent disclosure *through the use of an otherwise lawful virus scan or firewall.* The UESOPPA does not limit in this way. In brackets, the UESOPPA requires that the employer notify the employee.

[(F) shall, as soon as and to the extent practicable, notify the employee of its acquisition of the information.]			
(b) Subsection (a) does not apply to an employer action that is necessary to: (1) comply with federal or state law, 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 statute that requires an employer to inspect or monitor an employee's protected personal online account;	Section 6. Nothing in this Act shall prevent an employer or educational institution from: (B) Complying with state and federal laws, rules, and regulations and the rules of self-regulatory organizations, where applicable;	(3) This chapter does not prohibit or restrict an employer from complying with a duty to screen employees or applicants before hiring or to monitor or retain employee communications that is established under federal law, by a self-regulatory organization under the Securities and Exchange Act of 1934, 15 U.S.C. Sec. 78c(a)(26), or in the course of a law enforcement employment application or law enforcement officer conduct investigation performed by a law enforcement agency.	All three address exceptions required to comply with rules of a self-regulatory organization.
(2) investigate whether the employee has violated, is violating or is reasonably likely to violate federal or state law or a non-pretextual employer policy that is in writing or otherwise in a record,	(C) Requesting or requiring an employee or applicant to share specific content that has been reported to the employer, without requesting or requiring an employee or	(1)This chapter does not prohibit an employer from doing any of the following: […] (c) conducting an investigation or requiring an employee to cooperate in an investigation in any of the following: […]	All three contain exceptions for violations of the law. Both the

and of which the employee had reasonable notice, where: (A) the employer reasonably suspects that the employee has violated or is violating or is reasonably likely to violate the law or policy; and (B) the employer accesses only an account, content, [or metadata] that it reasonably believes to be relevant to the investigation; (3) take adverse action against the employee for violating federal or state law or a non-pretextual employer policy that is in writing or otherwise in a record and of which	applicant to provide a user name and password, password, or other means of authentication that provides access to a personal social media account, for the purpose of: (1) Ensuring compliance with applicable laws or regulatory requirements; (2) Investigating an allegation, based on receipt of specific information, of the unauthorized transfer of an employer's proprietary or confidential information or financial data to an employee or applicant's personal social media account; or (3) Investigating an allegation, based on receipt of specific information, of unlawful harassment in the workplace.	(i) if there is specific information about activity on the employee's personal Internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct; or (1)This chapter does not prohibit an employer from doing any of the following: […] (2) Conducting an investigation or requiring an employee to cooperate in an investigation as specified in Subsection (1)(c) includes requiring the employee to share the content that has been reported in order to make a factual determination.	UESOPPA and the Industry bill provide exceptions for violations of workplace policy. UESOPPA requires that the employer policy be in a record and notice provided to the employee. The ACLU model more specifically allows for investigation of workplace harassment, where specific information has been received. The Industry bill also requires specific information. UESOPPA requires "reasonable suspicion" of a violation of law or policy. The ACLU model permits requesting or requiring an employee or applicant to share specific content that has been reported to the employer, *without requesting or requiring an employee or applicant to provide a user name and password, password, or other means of authentication that provides access to a personal social media account.* UESOPPA restricts access only to accounts, content, [or metadata] that it reasonably believes to be relevant to the investigation. Unlike the UESOPPA, the Industry model and the ACLU model do not address permissible adverse action

the employee had reasonable notice; or (4) protect against: (A) a threat to health or safety; or	(E) Prohibiting an employee, applicant, student, or prospective student from using a personal social media account for business or school purposes; or (F) Prohibiting an employee, applicant, student, or prospective student from accessing or operating a personal social media account during business or school hours or while on business or school property.		against an employee for violating federal or state law or an employer policy.
(B) a significant threat to employer information or communications technology systems or other employer property; or		(1)This chapter does not prohibit an employer from doing any of the following: (a) requesting or requiring an employee to disclose a username or password required only to gain access to the following: (i) an electronic communications device supplied by or paid for in whole or in part by the employer; or (ii) an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes; […]	Both the UESOPPA and the Industry bill address exceptions for dealing with threats to employer information, systems, or property. However, Industry model provisions provide more detail about what activities are not prohibited. UESOPPA defines "Login information" to include a user name and password, password, or other

		(d) restricting or prohibiting an employee's access to certain websites while using an electronic communications device supplied by, or paid for in whole or in part by, the employer or while using an employer's network or resources, to the extent permissible under applicable laws; or (e) monitoring, reviewing, accessing, or blocking electronic data stored on an electronic communications device supplied by, or paid for in whole or in part by, the employer, or stored on an employer's network, to the extent permissible under applicable laws.	means or credentials of authentication required to access or control a protected personal online account, or to access or control 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.* Therefore, in both UESOPPA and Industry model, employers are not prohibited from requesting or requiring an employee to disclose a username or password required only to gain access to these types of employer supplied/paid for accounts and devices.
(C) disclosure of information in which the employer has a proprietary interest or that the employer has a legal obligation to keep confidential.		Section 3 (1)This chapter does not prohibit an employer from doing any of the following: […] (b) disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal Internet account without the employer's authorization;[…] (c) conducting an investigation or requiring an employee to cooperate in an investigation in any of the following:[…]	Both the Industry model and the UESOPPA address exceptions for dealing with disclosure of proprietary or confidential information. However, Industry model provisions provide additional details about what specific

(c) Subsection (b) does not permit an employer to: (1) use its access to, or the content [or metadata] 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 a court order requires or authorizes the employer to alter the settings or content; or (C) to do so is necessary to protect against a threat to health or safety; or		(ii) if the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's personal Internet account;	activities are not prohibited. (i.e. disciplining, discharging, and investigating)

(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).			
SECTION 5. STUDENT PROTECTIONS. (a) Except as otherwise provided in subsections (b) and (c): (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 [or metadata] of a protected personal online account; (3) alter the settings of a protected personal online account, including settings that affect whether another individual is able to view the content of the account; or	Section 4. An educational institution shall not: (A) Require, request, or coerce a student or prospective student to disclose the user name and password, password, or any other means of authentication, or provide access through the user name or password, to a personal social media account; (C) Compel […]or otherwise coerce a student or applicant to change the settings that affect a third party's ability to view the contents of a personal social networking account.		The UESOPPA addresses the disclosure of metadata. Substantially similar provisions.

(4) access the content of a protected personal online account in the presence of the educational institution in a manner that enables the educational institution to observe the content; or	B) Require, request, or coerce a student or prospective student to access a personal social media account in the presence of a school employee or school volunteer, including, but not limited to, a coach, teacher, or school administer, in a manner that enables the school employee or school volunteer to observe the contents of such account; or		Substantially similar provisions.
(B) require or coerce a student to add the educational institution to the list of contacts associated with the student's protected personal online account.	(C) Compel a student or prospective student to add anyone, including a coach, teacher, school administrator, or other school employee or school volunteer, to their list of contacts associated with a personal social media account or require, request, […]		Substantially similar provisions.
(2) An educational institution may not take or threaten to take an adverse action against a student for noncompliance with a requirement,	Section 5. An education institution shall not: (A) Take any action or threaten to take any action to discharge, discipline, prohibit from participating in curricular or extracurricular activities, or otherwise penalize a student for a student's refusal to disclose any information		Substantially similar provisions; except that the ACLU model provides more detail regarding what constitutes an adverse action. (e.g. Prohibit student

coercive demand, or request that violates paragraph (1).	specified in Section 4(A), for refusal to take any action specified in Section 4(B) or for refusal to add a coach, teacher, school administrator, or other school employee or school volunteer to their list of contacts associated with a personal social media account or to change the settings that affect a third party's ability to view the contents of a personal social media account, as specified in Section 4(C); or (B) Fail or refuse to admit any prospective student as a result of the prospective student's refusal to disclose any information specified in Section 4(A) or for refusal to take any action specified in Section 4(B), for refusal to add a coach, teacher, school administrator, or other school employee or school volunteer to their list of contacts associated with a personal social media account or to change the settings that affect a third party's ability to view the contents of a personal social media account, as specified in Section 4(C).		from participating in curricular or extracurricular activities.)

(3) An educational institution that, without violating paragraph (1), inadvertently acquires login information for, or the login-protected content [or metadata] of, a student's protected personal online account: (A) does not, solely by acquiring that information, violate this section; (B) may not use the login information to access or alter a student's protected personal online account; (C) may not take or threaten to take an adverse education-related action against a student based on the content [or metadata] of the student's protected personal online account; (D) may not record or share the login information for, or the content [or metadata] of, the student's protected personal online account; (E) shall, as soon as and to the extent practicable, dispose of the login information for, and content [or metadata] of, the student's protected personal online account; and	**Section 7.** If an employer or educational institution inadvertently receives the user name and password, password, or other means of authentication that provides access to a personal social media account of an employee, applicant, student, or prospective student through the use of an otherwise lawful virus scan or firewall that monitors the employer or school's network or employer-provided or school-provided devices, the employer or school is not liable for having the information, but may not use the information to access the personal social media account of the employee, applicant, student, or prospective student, may not share the information with anyone, and must delete the information immediately or as soon as is reasonably practicable.		Both UESOPPA and the ACLU model address issues of inadvertent disclosure. The ACLU model is narrower in that the provision covers inadvertent disclosure *through the use of an otherwise lawful virus scan or firewall.* The UESOPPA does not limit in this way. In brackets, the UESOPPA requires that the educational institution notify the student.

[(F) shall, as soon as and to the extent practicable, notify the student of its acquisition of the information.] (b) Subsection (a) does not apply to an educational institution's action that is necessary to: (1) comply with federal or state law, or with the rules of a self-regulatory organization established by statute that requires an educational institution to inspect or monitor a student's protected personal online account; (2) investigate whether the student has violated, is violating or is reasonably likely to violate federal or state law or a non-pretextual educational institution policy that is in writing or otherwise in a record and of which the student had reasonable notice, where: (A) the educational institution reasonably suspects that the student has violated, is violating or is reasonably likely to violate the law or policy; and (B) the educational institution accesses only an account, content, [or metadata] that it reasonably	Section 6. Nothing in this Act shall prevent an employer or educational institution from: (B) Complying with state and federal laws, rules, and regulations and the rules of self-regulatory organizations, where applicable; (D) Requesting or requiring a student or prospective student to share specific content that has been reported to the school, without requesting or requiring an student or prospective student to provide a user name and password, password, or other means of authentication that provides access to a personal social media account, for the purpose of: (1) Ensuring compliance with applicable laws or regulatory requirements; or (2) Investigating an allegation, based on receipt of specific information, of the unlawful harassment or bullying of another student by the student		Substantially similar. While both allow for exceptions to ensure compliance with laws, ACLU model still prohibits the requesting of user name and password. In addition to violation of laws, the exception in UESOPPA also applies to violations of (written) policy. The ACLU model also applies to violation of school in instances where there is specific information of unlawful harassment or bullying. UESOPPA requires "reasonable suspicion" of a violation of law or policy.

believes to be relevant to the investigation; (3) take adverse action against the student for violating federal or state law or a non-pretextual educational institution policy that is in writing or otherwise in a record and of which the student had reasonable notice; or (4) protect against: (A) a threat to health or safety (B) a significant threat to educational institution information or communications technology systems or other educational institution property; or (C) disclosure of information in which the educational institution has a	or prospective student from whom the content is requested or required. (E) Prohibiting an employee, applicant, student, or prospective student from using a personal social media account for business or school purposes; or (F) Prohibiting an employee, applicant, student, or prospective student from accessing or operating a personal social media account during business or school hours or while on business or school property.		

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 [or metadata] of, a student's protected personal online account obtained pursuant to subsection (b) for a purpose unrelated to a purpose specified in subsection (b); or (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 that content; (B) federal or state law or a court order requires or authorizes the educational institution to alter those settings or that content; or (C) to do so is necessary to protect against a 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).			
SECTION 6. CIVIL ACTION.	Section 8. Enforcement	**Section 4 – Remedy**	

(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 $[ ] for each violation. (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): (1) an employee or student may obtain: (A) injunctive and other equitable relief; (B) [for each violation, damages in the amount of $[ ] or] actual damages[, whichever is greater]; and (C) costs and reasonable attorneys' fees; and (2) the court may award a prevailing employer or educational institution costs and reasonable attorneys' fees if the court determines the action was frivolous.	(A) Any employer or educational institution, including its employee or agents, who violates this Act shall be subject to legal action for damages and/or equitable relief, to be brought by any other person claiming a violation of this Act has injured his or her person or reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured on account of violation of the provisions of this Act, and a reasonable attorney's fee and other costs of litigation. (B) Any educational institution employee or agent who violates this Act may be	(1) The state Attorney General may bring may bring a civil cause of action against an employer in a court of competent jurisdiction on behalf of a citizen an aggrieved by a violation of this chapter. (2) In an action brought under Subsection (1), if the court finds a violation of this chapter, the court shall award the state not more than $500 per violation.	Both the UESOPPA and the Industry bill provide for the AG to bring a civil action. Both allow for a civil penalty. The UESOPPA also allows for injunctive and other equitable relief. Only the ACLU model and UESOPPA allows for a private cause of action.

	subject to disciplinary proceedings and punishment. For school employees who are represented under the terms of a collective bargaining agreement, this Act prevails except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.		The ACLU model addresses disciplinary proceedings and collective bargaining agreements.
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.	Section 9. Severability:	**Section 6. Severability Clause**	

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.*	The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person, entity, or circumstance, is held invalid, the remainder of this Act, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.	If any provision of this chapter or the application of any provision of this chapter is found invalid, the remainder of this chapter shall be given effect without the invalid provision or application.	
SECTION 10. REPEALS; CONFORMING AMENDMENTS. (a) …… (b) …… (c) ……		**Section 7. Repealer Clause** The following laws are hereby repealed:	
SECTION 11. EFFECTIVE DATE. This [act] takes effect	Section 10. Effective Date: This Act shall take effect upon passage.	**Section 5 – Effective Date** This act takes effect upon approval by the Governor.	
		Section 3 – Prohibited and Permitted Activities **Chapter does not create duties.** (1) This chapter does not create a duty for an employer to search or monitor the activity of a personal Internet account.	Nothing similar in UESOPPA.

		(2) An employer is not liable under this chapter for failure to request or require that an employee or applicant for employment grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant for employment's personal Internet account.	