WHEN YOU CANNOT "JUST SAY NO": PROTECTING THE ONLINE PRIVACY OF EMPLOYEES AND STUDENTS

Samuel A. Thumma*

---

* Chief Judge, Arizona Court of Appeals, Division One, Phoenix, Arizona. The author had the privilege of serving as chair of the Uniform Employee and Student Online Privacy Protection Act Drafting Committee. Dennis D. Hirsch, Professor of Law at Capital University Law School and Professor of Law and Faculty Director, Program on Data and Governance, at The Ohio State University Moritz College of Law, served as the brilliant and wise Reporter. The following Uniform Law Commissioners served as able members of the Drafting Committee: Jerry L. Bassett, Diane F. Boyer-Vine, Stephen Y. Chow, Brian K. Flowers, William H. Henning, Lisa R. Jacobs, Peter F. Langrock, James G. Mann, Ann R. Robinson, Steve Wilborn, and initially, Daniel A. Ivey-Soto and Nicole Bordonaro. American Bar Association Advisors, including Frank H. Langrock, provided valuable insight, as did a wonderful group of Observers who counted in the dozens. The author wishes to express his sincere appreciation to Lindsay Beaver, Legislative Counsel, Uniform Law Commission, and Dennis D. Hirsch for comments on earlier versions of this Article as well as to Professor Barbara A. Atwood, who serves as a Uniform Law Commissioner from Arizona, and her article Barbara A. Atwood & Brian H. Bix, *A New Uniform Law for Premarital and Marital Agreements*, 46 FAM. L.Q. 313 (2012) for providing valuable guidance for the structure of this Article, and to Timothy J. Berg, also a Uniform Law Commissioner from Arizona. The views expressed are those of the author and do not represent those of the Arizona Court of Appeals, the Uniform Law Commission, or any of the individuals involved in the project. The errors in this Article are solely those of the author.

I. INTRODUCTION

> Today, most individuals [in the United States] 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 [non-public] content of, a personal online account, [the owner of that account] 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 [non-

> public] content of, an employee's or student's online account, that person may find it difficult to refuse.[1]

In recent years, there have been reported incidents where employers and educational institutions have demanded, and received, such access. One of the first reported instances of such conduct "surfaced in 2009 when the city government of Bozeman, Montana, instructed [job] applicants to divulge their usernames and passwords for social media sites, including Facebook, Google, Yahoo, YouTube, and MySpace."[2] Another widely-reported incident involved Robert Collins, a Maryland correctional supply officer, who sought to return to work after taking family leave in 2010 and was "asked to log into his Facebook account as part of his reinstatement interview."[3] And another incident, this time in the school setting, occurred "in Minnesota when a young female student claimed her public school brought her into a room with a police officer present, and forced her to provide her Facebook login information and email accounts because of allegations that she had online conversations about sex with another student."[4]

In response, states have enacted legislation prohibiting such coercive demands.[5] But that legislation lacks any real uniformity in definitions, in what is prohibited, in exceptions, and in remedies for violations.[6] And no federal law exists to provide national uniformity.[7] Given this lack of national legislation and the need for uniformity, in 2013, the Uniform Law Commission (ULC) saw the need to fill the void through uniform legislation.

The ULC, "established in 1892, provides states with non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law."[8] The ULC is a nonpartisan, volunteer organization

---

1. UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT committee's prefatory note (UNIF. LAW COMM'N 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/ESOPPA_Final%20Act_2016.pdf.

2. Jennifer Delarosa, *From Due Diligence to Discrimination: Employer Use of Social Media Vetting in the Hiring Process and Potential Liabilities*, 35 LOY. L.A. ENT. L. REV. 249, 256 (2015).

3. Jeffrey Stinson, *Password Protected: States Pass Anti-Snooping Laws*, PEW CHARITABLE TRS.: STATELINE (July 8, 2014), http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/07/08/password-protected-states-pass-anti-snooping-laws.

4. Delarosa, *supra* note 2, at 256–57.

5. *See infra* Part III.

6. UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT committee's prefatory note (UNIF. LAW COMM'N 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/ESOPPA_Final%20Act_2016.pdf.

7. *Id.*

8. *About the ULC*, UNIF. LAW COMM'N, http://uniformlaws.org/Narrative.aspx?title=About the ULC (last visited May 1, 2017).

that, over the years, has promulgated "more than 300 acts that secure uniformity of state law when differing laws would undermine the interests of citizens throughout the United States."[9] The ULC is made up of more than 300 commissioners "on uniform laws from each state, the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. Virgin Islands."[10] The commissioners must be members of the bar; are lawyers, judges, law professors, and legislators; serve specific terms; and receive no salary for their service with the ULC.[11]

The ULC studied the issue and then decided to draft model legislation addressing social media privacy in the employment and educational contexts, given the importance of the topic and interests at issue and the need for uniformity.[12] In late 2016, after two years of drafting, the ULC promulgated the Uniform Employee and Student Online Privacy Protection Act (UESOPPA) to provide uniform legislation for states to adopt in addressing this important topic to prevent coercive action.

The primary goal of UESOPPA is to enable employees and students (and prospective employees and students) to decide whether, and when, to provide actual and prospective employers and educational institutions access to their personal online accounts.[13] To accomplish this goal, UESOPPA prohibits employers and post-secondary educational institutions from requiring, coercing, or requesting that employees or students (or individuals who are seeking to become employees or students) provide them with access to login information for, or non-public content of, their personal online accounts.[14] UESOPPA further prohibits employers and educational institutions from requiring or coercing these individuals to add them to the list of those given access to the account (to "friend" them, in common parlance), although it does not prohibit them from requesting to be added as a friend.[15]

This Article provides background, context, and insight into the work that yielded UESOPPA and what the Act does, and does not, protect and prohibit. The Article begins with actions considered and legislation enacted by various

---

9. *Frequently Asked Questions*, UNIF. LAW COMM'N, http://uniformlaws.org/Narrative.aspx?title=Frequently%20Asked%20Questions (last visited May 1, 2017).

10. *About the ULC*, *supra* note 8.

11. *Id.*

12. UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT committee's prefatory note (UNIF. LAW COMM'N 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/ESOPPA_Final%20Act_2016.pdf.

13. *Id.*

14. *Id.*

15. *Id.*

states starting in 2012 that prompted the ULC to study the issue.[16] The Article next discusses the drafting process, including work done by the Study Committee that recommended the ULC undertake the drafting project, followed by a discussion of the work of the Drafting Committee in preparing UESOPPA.[17] This discussion provides context for the text of, and commentary for, UESOPPA as promulgated, but even more critically, some provisions that were considered by the Drafting Committee but are not contained in UESOPPA as promulgated.[18]

The Article then provides a detailed discussion of UESOPPA, including definitions, scope, what it does (and, critically, does not do), and remedies available for violations of the Act.[19] As noted in the conclusion, UESOPPA provides consistency and uniformity; builds on the best of the current state enactments; and avoids ambiguities and uncertainties. The Act provides a thoughtful balance of the issues and interests for all involved, including protecting students and employees against coercive behavior. UESOPPA also provides individuals, entities, and their representatives much needed predictability and certainty for their conduct, relationships, policies, and procedures. The hope is that the states will recognize the need for uniformity, agree with the policies reflected in UESOPPA, and enact the Act to avoid the uncertainty and unpredictability created by current law.[20]

II. BACKGROUND

In the United States, login-protected online accounts are pervasive.[21] Although varying widely, estimates suggest that Americans have more than two billion login-protected online accounts, ranging from social media accounts,[22]

---

16. *See* discussion *infra* Part III.
17. *See* discussion *infra* Part IV.
18. *Id.*
19. *See* discussion *infra* Part V.
20. *See* discussion *infra* Part VI.
21. Indeed, the pervasiveness of such accounts has prompted study of Americans who do not use the Internet. *See* Monica Anderson & Andrew Perrin, *13% of Americans Don't Use the Internet. Who Are They?*, PEW RES. CTR. (Sept. 7, 2016), http://www.pewresearch.org/fact-tank/2016/09/07/some-americans-dont-use-the-internet-who-are-they ("13% of U.S. adults do not use the Internet").
22. *See Social Media Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/social-media/ ("Today around seven-in-ten Americans use social media to connect with one another, engage with news content, share information and entertain themselves."); *see also* Patricia Sanchez Abril, Avner Levin & Alissa Del Riego, *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 67–68 (2012) [hereinafter *Blurred Boundaries*] ("Social media, in particular, has permeated modern culture and the daily lives of the incoming workforce."); *id.* at n.16 ("Facebook, MySpace,

to bank accounts, to email accounts, to any number of other types of password-protected accounts.[23] As of early 2013, it was estimated that nearly seven out of ten American adults used Facebook alone.[24]

Login-protected online accounts are used in a variety of contexts, including on the job, at school, or completely personally. Employers and potential employers have begun asking employees and job applicants for their usernames and passwords to their personal login-protected online accounts.[25] Along with those noted in the Introduction, other examples abound. In April 2011, Kimberly Hester was placed on unpaid leave from her job as an elementary school teacher's aide in Michigan when she "refused the school

---

Twitter, and LinkedIn boast a combined 1045 million worldwide users."); Greg Mgrditchian, Note, *Employment & Social Media Privacy: Employer Justifications for Access to "Private" Material*, 41 RUTGERS COMPUTER & TECH. L.J. 108, 116 (2015) ("The world's two most popular social media sites, Facebook and Twitter, have approximately 1.11 billion and 232 million active users, respectively.").

23. Looking to Britain as a proxy, in 2012, "[t]he average Briton" was reported to have "26 online accounts." *No Wonder Hackers Have It Easy: Most of Us Now Have 26 Different Online Accounts—But Only Five Passwords*, DAILY MAIL (July 16, 2012), http://www.dailymail.co.uk/sciencetech/article-2174274/No-wonder-hackers-easy-Most-26-different-online-accounts--passwords.html. The current population of the United States is approximately 325,000,000. *U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock/ (last visited Mar. 20, 2017). Conservatively, using half of each number (162,500,000 Americans with an average of thirteen online accounts) would yield more than two billion online accounts held by Americans.

24. *See* Sara E. Stratton, Note, *Passwords Please: Rethinking the Constitutional Right to Informational Privacy in the Context of Social Media*, 41 HASTINGS CONST. L.Q. 649, 654 & n.39 (2014) (citing Maeve Duggan & Joanna Brenner, *The State of Social Media Users*, PEW RES. CTR. (Feb. 14, 2013), http://www.pewinternet.org/Reports/2013/Social-media-users/The-State-of-Social-Media-Users.aspx).

25. *See id.*; *see also* Alissa Del Riego, Patricia Sanchez Abril & Avner Levin, *Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy*, 3 J. INTERNET L. 1, 17 (2012) ("Recently, there have been several reports of employers in the United States requesting" that job candidates provide "access to their Facebook accounts before making a hiring decision."); Susan Park, *Employee Internet Privacy: A Proposed Act That Balances Legitimate Employer Rights and Employee Privacy*, 51 AM. BUS. L.J., 779, 779–81 (2014) (providing additional examples of employers asking for applicants' social media login information); Robert Sprague, *No Surfing Allowed: A Review & Analysis of Legislation Prohibiting Employers from Demanding Access to Employees' & Job Applicants' Social Media Accounts*, 24 ALB. L.J. SCI. & TECH. 481, 482 (2014) (summarizing the experience of Maryland correctional supply officer Robert Collins); *id.* at 495–96 (discussing surveys conducted on the topic, including in March 2013, indicating that the prevalence was low but that such access was being requested at times); *Blurred Boundaries*, *supra* note 22, at 68–69 (providing examples of employees being fired for what they posted on social media); Mgrditchian, *supra* note 22, at 108–09 ("[A] number of employers have gone so far as to require employees to disclose their login information to social media sites they belong to in order to monitor their activity."); Stratton, *supra* note 24, at 651 (citing examples of employers asking for applicants' social media login information).

superintendent's demand for access to her Facebook account."[26] As another example, "Justin Bassett, a statistician from New York City . . . finished an interview and was asked to 'hand over his Facebook login information after the interviewer couldn't locate his profile on the site.'"[27]

Employers have used other methods, short of requesting usernames and passwords, to gather information about employees and applicants. One such method is when employers "ask applicants to login to their social media profile in the presence of a supervisor, allowing the supervisor to review the contents of the applicant's site at that time," a practice "known as 'shoulder surfing.'"[28] Another method is when employers "require[] the applicant to 'friend' a staff member of the employer, thereby allowing that individual access to the information on the social media site," sometimes referred to as "mandatory 'friending.'"[29] Yet another method is to have employees "change the privacy settings on their social media network to make their profile publicly available."[30]

Particularly given the context, these behaviors have caused substantial concerns about coercion.

> Many scholars argue that an employee's consent to particular employer demands is often suspect. One commentator argues persuasively that requiring job applicants or employees to provide their user name or login information so that employers can access personal media accounts is inherently coercive, given the nature of the relationship of the two parties.[31]

Similar conduct—and a similar concern about coercion—has arisen as a result of educational institutions requiring such access to personal login-protected online accounts of students and individuals applying for admission to educational institutions.[32]

---

26. Sprague, *supra* note 25, at 482.
27. Stratton, *supra* note 24, at 651.
28. Delarosa, *supra* note 2, at 268–74.
29. *Id.*
30. *Id.*
31. Park, *supra* note 25, at 812 & n.168 (citing Nicholas D. Beadle, Note, *A Risk Not Worth the Reward: The Stored Communications Act and Employers' Collection of Employees' and Job Applicants' Social Networking Passwords*, 1 AM. U. BUS. L. REV. 397, 403 (2012)); *see* Steven L. Willborn, *Consenting Employees: Workplace Privacy and the Role of Consent*, 66 LA. L. REV. 975, 976 (2006) (noting as a "bottom line" that "consent within the employment relationship is compromised and must be regarded with at least some skepticism").
32. *See* Delarosa, *supra* note 2, at 256–57 (referencing the Minnesota incident where "a young female student" at a public school allegedly was brought into a room with a police officer

Notwithstanding this conduct and these concerns, until comparatively recently, the law offered no meaningful protection against such coercive actions.[33] Not surprisingly, various points of view have been offered about such practices.[34] Some employers have taken the position that access to personal accounts is required to protect trade secrets or proprietary information, to comply with federal law, or to prevent employer liability; others have acknowledged that requiring access to personal accounts may be an invasion of an employee's privacy.[35] Similar concerns have been expressed in the

---

present "and forced . . . to provide her Facebook login information and email accounts because of allegations that she had online conversations about sex with another student. The ACLU of Minnesota filed a lawsuit in 2012 against the Minnewaska Area Schools and the Pope County Sheriff's Office for violating the student's constitutional rights. Specifically, the ACLU-MN argued a violation of the student's First Amendment right to freedom of speech and Fourth Amendment right to be free from unreasonable searches and seizures. Minnewaska Area Schools agreed to pay $70,000 to settle the lawsuit in March 2014 and to 'rewrite its policies to limit how intrusive the school can be when searching a student's emails and social media accounts created off school grounds.'"); *see also Blurred Boundaries*, *supra* note 22, at 115 (citation omitted) (noting the Electronic Communications Privacy Act of 1986 and stating "jurisprudence has acknowledged that an employer's mere request for access to an employee's password-protected site can constitute coercion, given the context of the employment relationship"); Michelle Poore, *A Call for Uncle Sam to Get Big Brother out of Our Knickers: Protecting Privacy and Freedom of Speech Interests in Social Media Accounts*, 40 N. KY. L. REV. 507, 511 (2013) ("[T]here is a disturbing emergence of reports of demands by public and private employers and academic institutions for access to users' private social media account content."); Talon R. Hurst, Comment, *Give Me Your Password: The Intrusive Social Media Policies in Our Schools*, 22 COMMLAW CONSPECTUS 196, 196–97 (2014) ("'Forced consent' social media policies of schools and universities have required students to give officials access to students' personal social media accounts."); *id.* at 206–08 (discussing postsecondary schools requiring students to grant officials access to their social media accounts).

33. *Blurred Boundaries*, *supra* note 22, at 112.

34. *See, e.g.*, *id.* at 69–71 (summarizing pros and cons of employer access).

35. *Access to Social Media Usernames and Passwords: 2016 Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Feb. 27, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx; *see also* Park, *supra* note 25, at 806 (citing Anita Ramasastry, *Can Employers Legally Ask for Your Facebook Password When You Apply for a Job?: Why Congress and the States Should Prohibit This Practice*, VERDICT (Mar. 27, 2012), http://verdict.justia.com/2012/03/27/can-employers-legally-ask-you-for-your-facebook-password-when-you-apply-for-a-job (exploring whether employer access to employee login information violates law and arguing that legislatures should take action in this area)); *Blurred Boundaries*, *supra* note 22, at 69–71 (summarizing pros and cons of employer access to employee social media accounts). For a thoughtful discussion of ownership rights following the end of an employer-employee relationship, an important issue beyond the scope of this Article, see Susan Park & Patricia Sanchez Abril, *Digital Self-Ownership: A Publicity-Rights Framework for Determining Employee Social Media Rights*, 53 AM. BUS. L.J. 537 (2016).

educational context.[36] Asked bluntly by one author, "[s]hould you have to surrender your privacy to go to school or hold a job?"[37]

III. STATE LEGISLATION

Federal legislation addressing the issue has been introduced from time to time but has never been enacted.[38] In the states, however, these incidents have prompted various legislative proposals and enactments.[39] Starting with a proposal in 2011, and continuing in earnest with enactments in 2012 and ever since, these concerns have prompted state legislation to prevent coercing employees to provide such information to get or keep a job, and to a lesser extent, to provide protection in the educational context.[40]

Although "Illinois was the first to propose a bill on May 18, 2011,"[41] Maryland was the first state to enact legislation protecting employees from forced disclosure,[42] and Delaware was the first state to enact legislation protecting students from forced disclosure, both of which were enacted in 2012.[43] By the end of 2012, fourteen states considered or enacted legislation prohibiting, requesting, or requiring an employee, a student, or an applicant to disclose a username or password for "a personal social media account."[44] Six states enacted such legislation in 2012, with Maryland and Illinois enacting

---

36. Hurst, *supra* note 32, at 208–11 (summarizing views of "supporters" and "opponents" of "forced consent" policies in the educational context).

37. Ken Kozlowski, 20 No. 12 *The Internet Guide to Employer Access to Social Media Passwords*, INTERNET L. RESEARCHER (LegalWorks), Dec. 2015, at 2.

38. *See* Sprague, *supra* note 25, at 483–84 & n.12 (referencing "two federal bills, the Password Protection Act of 2013 and the Social Networking Online Protection Act"); Delarosa, *supra* note 2, at 259 (referencing proposed federal laws regarding requiring login information from employees, students, and/or applicants).

39. *See* Richard W. Blackburn & Jeffrey J. Binder, 3 SUCCESSFUL PARTNERING BETWEEN INSIDE AND OUTSIDE COUNSEL § 47:10 n.82 (Robert L. Haig ed., May 2017 update) (2017) (citing Lynne Bernabei & Alan R. Kabat, *Invasions of Privacy,* NAT'L J. (July 23, 2012), http://www.nationallawjournal.com/id=1202563811801) ("[P]assword related legislation has been prompted by several government agencies that required applicants and employees to disclose nonpublic social media information. For example, some county sheriffs required applicants to 'friend' the sheriffs so they could check private Web sites.").

40. *See Access to Social Media Usernames and Passwords*, *supra* note 35; *see also* Sprauge, *supra* note 25, 482–83 ("In 2012, a total of twenty-eight bills were introduced in Congress and fourteen states prohibiting employers from requesting or requiring username and password access to employees' and job applicants' personal online accounts. Four of the state bills passed.").

41. Jordan M. Blanke, *The Legislative Response to Employers' Requests for Password Disclosure*, 14 J. HIGH TECH. L. 42, 43 (2014).

42. *See Access to Social Media Usernames and Passwords*, *supra* note 35.

43. *Id.*

44. *Id.*

laws in the employment context, Delaware and New Jersey enacting laws in the educational context, and California and Michigan enacting laws in both the employment and educational contexts.[45] Looking at these 2012 enactments provides context for subsequent proposals and enactments and for the significant differences in current state laws addressing the topic.

A. Maryland

"Maryland was the first state to enact a law protecting employees from disclosing social media login information."[46] Maryland's law was introduced on February 2, 2012, and signed by the governor on May 2, 2012, with an October 1, 2012 effective date, making it the first state social media protection act of many that would follow.[47] The Maryland enactment has been described as "the first of its kind and marked the beginning of a nationwide trend of social media privacy protection" in the employment context.[48] Adopting a structure later followed in many other states, Maryland's enactment has four basic components: (1) definitions; (2) prohibitions; (3) exceptions to the prohibitions; and (4) enforcement authorization.[49]

Maryland's enactment has just three defined terms.[50] Maryland uses an "electronic communications device" concept, expressly defining the phrase broadly to mean "any device that uses electronic signals to create, transmit and receive information," including "computers, telephones, personal digital assistants, and other similar devices."[51] Next, Maryland defines "employer" to mean "a person engaged in a business, an industry, a profession, a trade, or other enterprise" in Maryland or "a unit of State or local government" as well as "an agent, a representative and a designee of the employer."[52] Finally, and somewhat circuitously, Maryland defines "applicant" as "an applicant for employment."[53]

---

45. *Id.*

46. Stratton, *supra* note 24, at 659.

47. 2012 Md. Laws ch. 233; Blanke, *supra* note 41, at 45–46.

48. Delarosa, *supra* note 2, at 256. For a detailed discussion and critique of Maryland's law, see generally Alexander Borman, Comment, *Maryland's Social Networking Law: No "Friend" to Employers and Employees*, 9 J. BUS. & TECH. L. 127 (2014).

49. MD. CODE ANN., LAB. & EMPL. § 3-712 (West, Westlaw through legislation July 1, 2017, of 2017 Reg. Sess.); Blanke, *supra* note 41, at 48.

50. MD. CODE ANN., LAB. & EMPL. § 3-712 (West, Westlaw through legislation July 1, 2017, of 2017 Reg. Sess.).

51. *Id.* § 3-712(a)(3)(i)–(ii).

52. *Id.* § 3-712(a)(4).

53. *Id.* § 3-712(a)(2).

For prohibitions, Maryland provides that "an employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device."[54] Maryland also provides that an employer may not "discharge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee for an employee's refusal to disclose" such information or "fail or refuse to hire any applicant as a result of the applicant's refusal to disclose" such information.[55] Maryland includes prohibitions applicable to an employee, directing that "[a]n employee may not download unauthorized employer proprietary information or financial data to an employee's personal Web site, an Internet Web site, a Web-based account, or a similar account."[56]

For exceptions to these prohibitions, Maryland allows an employer to "require an employee to disclose any user name, password, or other means for accessing nonpersonal accounts or services that provide access to the employer's internal computer or information systems."[57] Maryland "does not prevent an employer . . . based on the receipt of information about the use of a personal Web site, Internet Web site, Web-based account, or similar account by an employee for business purposes, from conducting an investigation for the purpose of ensuring compliance with applicable securities or financial law, or regulatory requirements."[58] Similarly, Maryland "does not prevent an employer . . . based on the receipt of information about the unauthorized downloading of an employer's proprietary information or financial data to a personal Web site, Internet Web site, Web-based account, or similar account by an employee, from investigating an employee's actions."[59]

For enforcement, when Maryland's Commissioner of Labor and Industry[60] determines the enactment is violated, "the Commissioner shall" try to resolve the issue "informally by mediation" or ask Maryland's attorney general "to bring an action on behalf of the applicant or employee."[61] Maryland's attorney general then has the statutory authorization to seek "injunctive relief, damages, or other relief."[62]

---

54. *Id.* § 3-712(a)(b)(1).
55. *Id.* § 3-712(c).
56. *Id.* § 3-712(d).
57. *Id.* § 3-712(b)(2).
58. *Id.* § 3-712(e)(1).
59. *Id.* § 3-712(e)(2).
60. *Id.* § 3-712(f); *see id.* § 3-101(b) (showing that when statutes in the title refer to the Commissioner, that Commissioner is the Commissioner of Labor and Industry).
61. *Id.* § 3-712(f)(1).
62. *Id.* § 3-712(f)(2).

Maryland set the stage, particularly in the employment context, for many enactments that followed.[63] According to one commentator, enactments in most other states in the employment context "follow the broad contours set forth in the Maryland statute," although "they diverge widely in the details."[64] But Maryland's enactment may raise as many issues as it resolves. For example, although protecting the ability to "access" both "a personal account or service" and "nonpersonal accounts and services,"[65] Maryland does not define these terms. Similarly, no definition is provided for "employer's internal computer or information systems."[66] Maryland also does not define "applicable securities or financial law," "regulatory requirements," or "employer's proprietary information," arguably terms of art that are used in the enactment.[67] Similarly, Maryland does not define "employee," a phrase that can have quite different meanings depending upon the context.

The terms that are defined in Maryland's law appear, at times, unbounded. For example, by defining "employer" to include "a person engaged in . . . a trade,"[68] Maryland appears to include in the definition of employer individuals who traditionally would be defined as employees. By contrast, the definitions at times are quite restrictive. For example, defining "applicant" as "an applicant for employment"[69] would appear to exclude individuals contacted by a potential employer (perhaps through a recruiter), or those who contacted a potential employer in an expression of interest (perhaps at a job fair or in response to a posting for a position) but had not yet submitted an application for employment. However, open issues and vagaries aside, Maryland's enactment was the first and provided a foundation for many enactments that followed.[70]

B. Illinois

Although initially introduced on May 18, 2011, making it the first such proposal in the country, Illinois formally enacted legislation applicable in the

---

63. *See* Charles J. Stiegler, *Developments in Employment Law and Social Media*, 71 BUS. LAW. 321, 321 (2015) ("Twenty-one states have passed some version of a law intended to protect employees from employer intrusion into personal online accounts . . . . Most of these laws are loosely based on the Maryland provision . . . .").

64. *Id.* at 322.

65. MD. CODE ANN., LAB. & EMPL. § 3-712(b)(1)–(2) (West, Westlaw through legislation July 1, 2017, of 2017 Reg. Sess.).

66. *Id.* § 3-712(b)(2).

67. *Id.* § 3-712(e)(1)–(2).

68. *Id.* § 3-712(a)(4)(i)(1).

69. *Id.* § 3-712(a)(2).

70. Stiegler, *supra* note 63.

employment context on August 1, 2012, with a January 1, 2013 effective date.[71] In doing so, in many respects, Illinois took a very different approach than Maryland's law.

Illinois uses just one defined term: "social networking website."[72] Illinois defines the phrase to mean "an Internet-based service that allows individuals to: (i) construct a public or semi-public profile within a bounded system, created by the service; (ii) create a list of other users with whom they share a connection within the system; and (iii) view and navigate their list of connections and those made by others within the system."[73] Illinois expressly exempts electronic mail from this definition.[74]

Turning to prohibitions, Illinois makes it

> unlawful for any employer to request or require any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website or to demand access to such an account or profile.[75]

For exceptions, Illinois provides that an employer is not prohibited from obtaining "information that is in the public domain" or properly obtained under the enactment.[76] Illinois also does not limit "an employer's right" to "promulgate and maintain lawful workplace policies governing the use of the employer's electronic equipment, including policies regarding Internet use, social networking site use, and electronic mail use" as well as monitoring "usage of the employer's electronic equipment and the employer's electronic mail without requesting or requiring any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website."[77]

Thus, although enacted at about the same time as Maryland's law, Illinois took a very different approach, limiting protections to true social networking platforms and expressly exempting electronic mail (and, given the definition of

---

71. *See* 2012 Ill. Laws P.A. 87-807; Blanke, *supra* note 41. Although later amendments changed somewhat the language in Illinois's statute, this Article focuses on the original language in the 2012 enactment.

72. 820 ILL. COMP. STAT. ANN. 55/10(b)(6)(A) (West, Westlaw current through P.A. 100-25 of 2017 Reg. Sess.).

73. *Id.*

74. *Id.*

75. *Id.* 55/10(b)(1)(A).

76. *Id.* 55/10(b)(3)(A).

77. *Id.* 55/10(b)(2).

"social networking website," excluding from its protections other login-protected accounts like bank, credit card, and securities accounts).[78] There was no overlap between the defined terms used in Maryland and in Illinois and little overlap in the terms used generally in the two states.[79] So, from the start, these two early enactors took very different approaches to legislation in the employment context.

C. Delaware

In the educational context, Delaware's "Education Privacy Act," enacted July 20, 2012, with an August 19, 2012 effective date, became the first state law to afford social media privacy protection for students.[80] As with the enactments in the employer context, Delaware's enactment in the educational context has four basic components: (1) definitions; (2) prohibitions; (3) exceptions to the prohibitions; and (4) enforcement provisions.[81]

Starting with definitions, the Delaware enactment is limited to "public or nonpublic institution[s] of higher education or institution[s] of postsecondary education."[82] As defined terms, Delaware distinguishes between a student ("a person which at all relevant times is admitted into the academic institution") and an applicant ("a prospective student applying for admission into the subject academic institution").[83] Delaware also includes definitions for social networking and physical devices.[84]

> "Social networking site" means an internet-based, personalized, privacy-protected website or application whether free or commercial that allows users to construct a private or semi-private profile site within a bounded system, create a list of other system users who are

---

78. *Id.* 55/10(b)(6).

79. *Compare* MD. CODE ANN., LAB. & EMPL. § 3-712 (West, Westlaw through legislation July 1, 2017, of 2017 Reg. Sess.), *with* 820 ILL. COMP. STAT. ANN. 55/10 (West, Westlaw current through P.A. 100-25 of 2017 Reg. Sess.).

80. 78 Del. Laws, c. 354 § 1 (2012); Gary Gansle, Jessica Linehan & Kurt Whitman, *No Password for You: California Enacts Social Media Privacy Laws Affecting Employers and Postsecondary Educational Institutions*, 17 No. 10 CYBERSPACE L. 1 (2012) (noting that "California becomes the second state, joining Delaware," to enact such legislation). Although the Delaware act directed the addition of Chapter 94 to Title 14 of the Delaware Code, the enactment was codified in Chapter 81 of Title 14. *Compare* 78 Del. Laws, c. 354 § 1 (2012), *with* DEL. CODE ANN. tit. 14 §§ 8101–8105 (West, Westlaw current through 81 Laws 2017, chs. 1–66).

81. DEL. CODE ANN. tit. 14 §§ 8101–8105.

82. *See id.* § 8103; *see also id.* § 8102 (defining the academic institutions that are referred to in *id.* § 8103).

83. *Id.* § 8102(b), (e).

84. *Id.* § 8102(c), (d).

> granted reciprocal access to the individual's profile site, send and receive email, and share personal content, communications, and contacts.[85]

Further, "'[e]lectronic communication device' means a cell telephone, personal digital assistant, electronic device with mobile data access, laptop computer, pager, broadband personal communication device whether mobile or desktop, 2-way messaging device, electronic game, or portable computing device."[86]

Delaware then sets forth broad prohibitions. Specifically, "an academic institution shall not": (1) "request or require that a student or applicant disclose any password or other related account information in order to gain access to the student's or applicant's social networking site profile or account by way of an electronic communication device"; (2) "require or request that a student or applicant log onto a social networking site, mail account, or any other internet site or application by way of an electronic communication device in the presence of an agent of the institution so as to provide the institution access"; or (3) "request or require a student or applicant to add the employer or its representative to their personal social networking site profile or account."[87] Delaware also makes plain that "[a]n academic institution is prohibited from accessing a student's or applicant's social networking site profile or account indirectly through any other person who is a social networking contact of the student or applicant."[88] And the final prohibition states that "[n]o public or nonpublic academic institution shall monitor or track a student's or applicant's personal electronic communication device by installation of software upon the device, or by remotely tracking the device by using intercept technology."[89] Delaware provides that "[a]n academic institution may not discipline, dismiss or otherwise penalize or threaten to discipline, dismiss or otherwise penalize a student [or fail or refuse to admit any applicant] for refusing to disclose any

---

85. *Id.* § 8102(d).

86. *Id.* § 8102(c).

87. *Id.* § 8103(a), (b), (d). The reference in the third of these prohibitions to "the employer or its representative" appears misplaced in an act addressing academic institutions, not employers. That specific phrase, however, does not appear to have been a part of any legislation enacted when Delaware enacted the provision or since that time. In context, the proper phrase would appear to be "add the academic institution or its representative," but the statute reads as quoted in the text.

88. *Id.* § 8103(e).

89. *Id.* § 8103(c). This final prohibition is expressly applied to every "public or nonpublic academic institution," while the others are applicable to every "academic institution." *Compare id.*, *with id.* § 8103(a), (b), (d), (e). Because the statute defines "academic institution" as "public or nonpublic" institutions of higher or postsecondary education, it is unclear whether this reference is to make the prohibition applicable to all schools, regardless of the age of their students, or is included for some other reason.

information" protected in the first two categories of protected information.[90] No similar prohibition applies to the other prohibitions in the Delaware law.[91]

The exceptions state the protections "shall not apply to investigations conducted by an academic institution's public safety department or police agency who have a reasonable articulable suspicion of criminal activity, or to an investigation, inquiry or determination conducted pursuant to an academic institution's threat assessment policy or protocol."[92]

Delaware does not include any express enforcement provisions.[93]

D. New Jersey

Introduced on May 10, 2012, New Jersey approved an act "prohibiting the requirement to disclose personal information for certain electronic communications devices by institutions of higher education" effective December 3, 2012.[94] New Jersey's law appears to have been modeled on Delaware's law, with some significant differences.[95]

The New Jersey definitional terms are nearly identical to those used in Delaware.[96] Although not defining student, New Jersey defines "applicant," "electronic communications device," "public or private institution of higher education," and "social networking website" in nearly identical ways to Delaware.[97] The one exception is that New Jersey expressly states a public or private institution of higher learning includes "any employee, agent, representative, or designee of the institution."[98]

The New Jersey prohibitions broadly protect a student or applicant from disclosing information regarding a social networking website, stating "[n]o public or private institution of higher education in [New Jersey] shall"

> (1) [r]equire a student or applicant to provide or disclose any user name or password, or in any way provide access to, a personal account or service through an electronic communications device; (2) [i]n any way inquire as to whether a student or applicant has an account or profile on a social networking website; or (3) [p]rohibit a student or

---

90. *Id.* § 8104.
91. *Id.*
92. *Id.* § 8105.
93. *Id.* §§ 8101–8105.
94. 2012 N.J. Laws, c. 75, § 1.
95. *Compare* DEL. CODE ANN. tit. 14 §§ 8101–8105, *with* N.J. STAT. ANN. §§ 18A:3-29–32 (West, Westlaw current through L. 2017, c. 115 and J.R. No. 10).
96. *Compare* DEL. CODE ANN. tit. 14 § 8102, *with* N.J. STAT. ANN. § 18A:3-29.
97. *Id.*
98. N.J. STAT. ANN. § 18A:3-29.

> applicant from participating in activities sanctioned by the institution of higher education, or in any other way discriminate or retaliate against a student or applicant, as a result of the student or applicant refusing to provide or disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device.[99]

In conjunction with these broad prohibitions which, among other things, preclude a school from asking if a student or applicant has an account or profile on a social networking website, New Jersey contains a novel provision prohibiting waivers of the protections set forth in the act:

> No public or private institution of higher education in this State shall require a student or applicant to waive or limit any protection granted under this act. An agreement to waive any right or protection under this act is against the public policy of this State and is void and unenforceable.[100]

Unlike Delaware, New Jersey contains no express exceptions to these protections.[101] Unlike Delaware, New Jersey does, however, have express enforcement provisions, including providing that an aggrieved person, "in addition to any other available remedy," may file a civil action for violations of the protections.[102] The remedies available for a violation include injunctive relief, "compensatory and consequential damages incurred by the applicant as a result of the violation, taking into consideration any failure to admit the applicant in connection with the violation," as well as reasonable attorneys' fees and costs.[103] An aggrieved "current or former student" is authorized to obtain similar relief.[104]

E. California

In 2012, along with Maryland and Illinois (each in the employment context) and Delaware and New Jersey (each in the educational context), California and Michigan enacted laws in both contexts.[105] California was the

---

99. *Id.* § 18A:3-30.
100. *Id.* § 18A:3-31.
101. *Compare* DEL. CODE ANN. tit. 14 § 8105, *with* N.J. STAT. ANN. §§ 18A:3-29–32.
102. *Compare* DEL. CODE ANN. tit. 14 §§ 8101–8105, *with* N.J. STAT. ANN. § 18A:3-32.
103. N.J. STAT. ANN. § 18A:3-32(a).
104. *Id.* § 18A:3-32(b).
105. *See Access to Social Media Usernames and Passwords*, *supra* note 35.

first state to enact laws in both contexts, with provisions introduced in February 2012 and signed by the governor on September 27, 2012.[106]

The California legislation in the employment context[107] was titled "EMPLOYER USE OF SOCIAL MEDIA" but defined "social media" more broadly than a more traditional definition of the phrase.[108] In the sole definition contained in the enactment, California defines "social media" as "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."[109] Thus, any online account or service, apparently whether password-protected or not and whether publicly available or not, is included in the California definition of "social media" in the employment context.

The California prohibitions state that "[a]n employer shall not require or request an employee or applicant for employment" to "[d]isclose a username or password for the purpose of accessing personal social media"; "[a]ccess personal social media in the presence of the employer"; or "[d]ivulge any personal social media" unless a statutorily enumerated exception applies.[110] These prohibitions raise various questions that do not appear to be resolved by the statute. For example, by referencing "username or password," it is uncertain whether this would account for technology security advancements (such as fingerprint or facial recognition technology) that do not require a username or password. As another example, the prohibition of an employer from requiring disclosure of a username or password "for the purpose of accessing personal social media," suggests that an employer could require the disclosure of a username or password for other purposes. And although defining "social media" broadly, the statutory term "personal social media" is not a defined term.

Turning to the exceptions, California provides the following:

> Nothing in this section shall affect an employer's existing rights and obligations to request an employee to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and

106. *Id.* For a near-contemporaneous overview of California's enactments, see Gansle, Linehan & Whitman, *supra* note 80.

107. 2012 Cal. Legis. Serv. ch. 618 (West) (codified as CAL. LAB. CODE § 980 (West, Westlaw current with urgency legislation through ch. 164 of 2017 Reg. Sess.)).

108. CAL. LAB. CODE § 980.

109. *Id.* § 980(a).

110. *Id.* § 980(b).

> regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding.[111]

But "reasonably believed" by whom? And what level of certainty would need to support the "allegations of employee misconduct"? And what does "a related proceeding" add?

Another exception states "[n]othing in this section precludes an employer from requiring or requesting an employee to disclose a username, password, or other method for the purpose of accessing an employer-issued electronic device."[112] Although providing clarity that such information could be demanded for "an employer-issued electronic device," is it the access to the device that can be demanded, or is it the access to the device *and* applications on the device that can be demanded? And given that the prohibitions address solely "username or password," is the exception for "other method for the purpose of accessing" needed because it addresses something that is not, at least textually, prohibited by the statute?

The California statute also defines what discipline an employer can and cannot impose:

> An employer shall not discharge, discipline, threaten to discharge or discipline, or otherwise retaliate against an employee or applicant for not complying with a request or demand by the employer that violates this section. However, this section does not prohibit an employer from terminating or otherwise taking an adverse action against an employee or applicant if otherwise permitted by law."[113]

This prohibition, however, discusses "a request or demand by the employer," while the prohibitions state an employer "shall not require or request."[114] Presumably, "demand" and "require" are intended to mean different things (otherwise a single term would be used in both places), but what? And it is unclear why the first sentence discussed "discharge, discipline, threaten to discharge or discipline, or otherwise retaliate," while the second sentence talks of "terminating or otherwise taking an adverse action."[115]

California provides no express private enforcement mechanism in the employment context. Indeed, the sole provision regarding enforcement states that "[n]otwithstanding any other provision of law, the Labor Commissioner,

---

111. *Id.* § 980(c).
112. *Id.* § 980(d).
113. *Id.* § 980(e).
114. *Compare id.* § 980(e), *with id.* § 980(b).
115. *Id.* § 980(e).

who is Chief of the Division of Labor Standards Enforcement, is not required to investigate or determine any violation of this act."[116]

The California enactment in the educational context has a similar history, with some similar provisions, but also with some important differences.[117] Introduced two days after the employer provision, the education provision includes an express statement of legislative intent not included in the employer provision:

> The Legislature finds and declares that quickly evolving technologies and social media services and Internet Web sites create new challenges when seeking to protect the privacy rights of students at California's postsecondary educational institutions. It is the intent of the Legislature to protect those rights and provide students with an opportunity for redress if their rights are violated. It is also the intent of the Legislature that public postsecondary educational institutions match compliance and reporting requirements for private nonprofit and for-profit postsecondary educational institutions imposed by this act.[118]

Using the same definition for "social media" adopted in the employer provision,[119] the education provision states "[p]ublic and private postsecondary educational institutions, and their employees and representatives, shall not require or request a student, prospective student, or student group to" do the same acts prohibited by the employer provision.[120] It is unclear why the reference to "their employees and representatives" is included in the education provision but is not included in the employer provision. And the "except as provided" exception to the prohibition on divulging personal social media information in the employer provision[121] is not contained in the education provision.

---

116. 2012 Cal. Legis. Serv. ch. 618 (A.B. 1844) (West).

117. 2012 Cal. Legis. Serv. ch. 619 (S.B. 1349) (West) (codified as CAL. EDUC. CODE §§ 99120–99122 (West, Westlaw current with urgency legislation through ch. 164 of 2017 Reg. Sess.)).

118. *Id.*

119. CAL. EDUC. CODE § 99120.

120. *Id.* § 99121(a). Even then, however, there were some differences in the prohibitions that context does not easily explain. For example, an employer is prohibited from requiring or requesting disclosure of "a username or password for the purpose of accessing personal social media," CAL. LAB. CODE § 980(b)(1) (West, Westlaw current with urgency legislation through ch. 164 of 2017 Reg. Sess.), while a school is prohibited from requiring or requesting disclosure of "a user name or password for accessing personal social media," CAL. EDUC. CODE § 99121(a)(1). Whether, and to what extent, this difference is intended to truly be a difference is unclear.

121. CAL. LAB. CODE § 980(b)(3) (West, Westlaw current with urgency legislation through ch. 164 of 2017 Reg. Sess.).

Significantly, the limitations on how information obtained in an investigation in the educational context does not contain the limitation in the employment provision that any social media obtained be "used solely for purposes of that investigation or a related proceeding."[122] Finally, the education provision requires that the applicable school "shall post its social media privacy policy on the institution's Internet Web site."[123]

These differences and apparent inconsistencies in these California enactments have not been resolved by case law or legislatively. And some would appear to cause mischief in attempting to reconcile identical, or nearly identical, language used in two very different contexts. Regardless, California was the first in the nation to enact legislation to protect personal online accounts in both the employer and educational institution contexts.[124]

F. Michigan

Michigan was the second state to enact laws in both the employment and educational contexts, with a proposal introduced in March 2012, signed by the governor on December 27, 2012, and made effective December 28, 2012.[125] Unlike California, Michigan did so in a single act called the "internet privacy protection act,"[126] the stated purpose of which is

> to prohibit employers and educational institutions from requiring certain individuals to grant access to, allow observation of, or disclose information that allows access to or observation of personal internet accounts; to prohibit employers and educational institutions from taking certain actions for failure to allow access to, observation of, or disclosure of information that allows access to personal internet accounts; and to provide sanctions and remedies.[127]

---

122. *Compare* CAL. LAB. CODE § 980(c), *with* CAL. EDUC. CODE § 99121.

123. CAL. EDUC. CODE § 99122.

124. *See Access to Social Media Usernames and Passwords*, *supra* note 35.

125. *Id.* As enacted, House Bill 5523 (2012) was codified at Mich. Comp. Laws Ann. §§ 37.271–37.278 (2012). H.B. 5523, 96th Leg., Reg. Sess. (Mich. 2012) (codified at MICH. COMP. LAWS ANN. §§ 37.271–37.278 (West, Westlaw current through P.A. 2017, No. 108, also 112 and 117, of the 2017 Reg. Sess., 99th Leg.)). In addition, House Bill 5623 (2012), which contained similar provisions, was introduced in May 2012 and referred to a committee, but no further action was taken. H.B. 5623, 96th Leg., Reg. Sess. (Mich. 2012).

126. MICH. COMP. LAWS ANN. §§ 37.271–37.278.

127. H.B. 5523, 96th Leg., Reg. Sess. (Mich. 2012) (codified at MICH. COMP. LAWS ANN. §§ 37.271–37.278).

For definitions, Michigan uses the phrase "personal internet account," defined as "an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data."[128] Although differing in terminology from California's "social media" definition, the term covers approximately the same ground, appearing to apply to any online service or account.[129] Significantly, Michigan's definition of "personal internet account" does not appear to limit coverage to personal accounts, as opposed to Internet-based accounts that require a user to input or store information electronically.[130] For example, the definition as written appears to apply equally to a personal Internet-based bank account as well as an Internet-based account provided by an employer or school and used by the person solely for employer or school purposes.

Michigan also expressly defines "access information," "educational institution," and "employer."[131] "'Access information' means user name, password, login information, or other security information that protects access to a personal internet account."[132] In contrast to California's legislation applying only to postsecondary education, Michigan's definition of "educational institution" includes schools of all kinds, including "an academy; elementary or secondary school; extension course; kindergarten; nursery school; school system; school district; intermediate school district; business, nursing, professional, secretarial, technical, or vocational school; public or private educational testing service or administrator; and an agent of an educational institution."[133] By express directive, "[e]ducational institution shall be construed broadly to include public and private institutions of higher education to the greatest extent consistent with constitutional limitations."[134] "Employer" is defined as "a person, including a unit of state or local

---

128. MICH. COMP. LAWS ANN. § 37.272(d).

129. *Compare* CAL. LAB. CODE § 980(a) (West, Westlaw current with urgency legislation through ch. 164 of 2017 Reg. Sess.) (defining "social media"), *and* CAL. EDUC. CODE § 99120 (West, Westlaw current with urgency legislation through ch. 164 of 2017 Reg. Sess.) (defining "social media"), *with* MICH. COMP. LAWS ANN. § 37.272(d) (defining "personal internet account").

130. MICH. COMP. LAWS ANN. § 37.272(d).

131. *Id.* § 37.272(a)–(c).

132. *Id.* § 37.272(a).

133. *Id.* § 37.272(b).

134. *Compare* CAL. EDUC. CODE § 99121 (West, Westlaw current with urgency legislation through ch. 164 of 2017 Reg. Sess.) (referring to public and private postsecondary education institutions), *with* MICH. COMP. LAWS ANN. § 37.272(b) (including a broad range of schools and education related institutions).

government, engaged in a business, industry, profession, trade, or other enterprise in [Michigan] and includes an agent, representative, or designee of the employer."[135]

In setting forth the prohibitions, Michigan provides that an employer "shall not . . . [r]equest an employee or an applicant for employment to grant access to, allow the observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account."[136] Given the breadth of Michigan's definition of "personal internet account," this could be read as precluding an employer from requiring an employee's disclosure of information contained in the employer's Internet-based account. Michigan also provides that an employer shall not "[d]ischarge, discipline, fail to hire, or otherwise penalize an employee or applicant for employment for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account."[137] In the educational context, Michigan enacted nearly identical provisions, modified slightly to account for context.[138]

Turning next to exceptions, the Michigan enactment "does not prohibit an employer from . . . [r]equesting or requiring an employee to disclose access information to the employer to gain access to or operate" an "electronic communications device paid for in whole or in part by the employer" or an "account or service provided by the employer, obtained by virtue of the employee's relationship with the employer, or used for the employer's business purposes."[139] These exceptions, then, counter some of the breadth of the "personal internet account" definition.[140] And the exceptions are both device-driven (allowing access to everything on a device if even a portion of the device was paid for by the employer)[141] and account-driven (allowing access to everything in an account if even a portion of the account was "used for the employer's business purposes").[142]

Michigan's exceptions do not prohibit employers from: "[d]isciplining 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"; "[r]estricting or prohibiting an

---

135. MICH. COMP. LAWS ANN. § 37.272(b).
136. *Id.* § 37.273(a).
137. *Id.* § 37.273(b).
138. *Id.* § 37.274.
139. *Id.* § 37.275.
140. *Compare id.* (providing permissible employer acts related to access), *with id.* § 37.272(d) (defining "personal internet account").
141. *Id.* § 37.275(1)(a)(i).
142. *Id.* § 37.275(1)(a)(ii).

employee's access to certain websites while using an electronic communications device paid for in whole or in part by the employer or while using an employer's network or resources, in accordance with state and federal law"; or "[m]onitoring, reviewing, or accessing electronic data stored on an electronic communications device paid for in whole or in part by the employer, or traveling through or stored on an employer's network, in accordance with state and federal law."[143]

As with California, Michigan has an investigation exception, which does not prohibit an employer from

> [c]onducting an investigation or requiring an employee to cooperate in an investigation in any of the following circumstances: (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] (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.[144]

Michigan's law also does not "prohibit or restrict" an employer "from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under federal law or by a self-regulatory organization" as defined in 15 U.S.C. § 78c(a)(26).[145] Furthermore, Michigan "does not prohibit or restrict an employer from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain."[146]

For educational institutions, Michigan also contains exceptions.[147] Akin to the employer exceptions, Michigan does not prohibit "an educational institution from requesting or requiring a student to disclose access information to the educational institution to gain access to or operate . . . [a]n electronic communications device paid for in whole or in part by the educational institution" or "[a]n account or service provided by the educational institution that is either obtained by virtue of the student's admission to the educational

---

143. *Id.* § 37.275(1)(b), (d), (e).
144. *Id.* § 37.275(1)(c).
145. *Id.* § 37.275(2).
146. *Id.* § 37.275(3).
147. *Id.* § 37.276.

institution or used by the student for educational purposes."[148] And Michigan "does not prohibit or restrict an educational institution from viewing, accessing, or utilizing information about a student or applicant that can be obtained without any required access information or that is available in the public domain."[149] There is no statutory investigatory exception applicable to schools.

Michigan law makes plain that the "act does not create a duty for an employer or educational institution to search or monitor the activity of a personal internet account."[150] The act also provides that an employer or educational institution is not liable for failing to request or require access to the personal internet account of an employee, applicant for employment, student, or prospective student.[151]

For enforcement, Michigan provides statutory penalties and remedies for violations.[152] An employer or educational institution that violates the prohibitions "is guilty of a misdemeanor punishable by a fine of not more than $1,000.00."[153] On the civil side, "[a]n individual who is the subject of a violation of this act may bring a civil action" to enjoin the violation and "may recover not more than $1,000.00 in damages plus reasonable attorney fees and court costs."[154] To recover civil damages, the individual seeking damages is required to make a pre-litigation written demand "of the alleged violator" seeking such damages.[155] Michigan provides that "[i]t is an affirmative defense to an action under this act that the employer or educational institution acted to comply with requirements of a federal law or a law of this state."[156]

G. Other 2012 Legislative Proposals

In 2012, along with these enactments, legislative proposals addressing online privacy protection in the employment or educational contexts were introduced but not enacted in Massachusetts, Minnesota, Missouri, New York, Ohio, Pennsylvania, South Carolina, and Washington.[157] Other proposals and enactments followed in subsequent years,[158] such that "a majority of states (forty-four) and both the U.S. House of Representatives and U.S. Senate have

148. *Id.* § 37.276(1).
149. *Id.* § 37.276(2).
150. *Id.* § 37.277(1).
151. *Id.* § 37.277(2).
152. *Id.* § 37.278.
153. *Id.* § 37.278(1).
154. *Id.* § 37.278(2).
155. *Id.*
156. *Id.* § 37.278(3).
157. *Access to Social Media Usernames and Passwords*, *supra* note 35.
158. *See* Delarosa, *supra* note 2, at 257–58 (summarizing legislative proposals).

either enacted or considered enacting employee password protection legislation."[159]

Although these provisions evidence some common concerns and protections, they contain significant and irreconcilable differences. These differences include: (1) a "lack of uniformity" in definitions (including what type of account or device is covered); (2) what the statutes prohibit; (3) what exceptions exist; and (4) what remedies are available for violations.[160] As referenced in hindsight, one commentator noted that the differences in the employment context

> provide a flavor of the idiosyncrasies that employers must contend with. Any employer considering reviewing or accessing an employee's or applicant's personal online or social media account—for any reason—would be well served to tread carefully and to carefully review the legislation (and pending legislation) of all states where it does business.[161]

And as another commentator noted, "the differences from state to state are significant enough that they will likely pose real challenges to multistate

---

159. Park, *supra* note 25, at 787–93; *see id.* App. A (providing a comparison of password privacy legislation).

160. *See* Sprague, *supra* note 25, at 485–94 (summarizing similarities and differences in provisions enacted as of early 2014 in Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, and Washington); *see also* Park, *supra* note 25, at 788–93 (discussing differences in various state legislation and selected bills in "six broad categories: (1) the parties to whom the statutes apply, (2) the applicable online accounts, (3) prohibited acts, (4) exemptions or exceptions, (5) enforcement provisions, and (6) unique provisions"); Sprague, *supra* note 25, at 510–11 (noting that, at that time, "[o]nly four of the enacted statutes directly or indirectly address employees 'Friending' their employer," adding that "New Jersey's statute prohibits employers from requiring an individual to waive or limit any protection granted under its act as a condition for applying for or receiving an offer of employment"); Stratton, *supra* note 24, at 662 (footnotes omitted) (noting Delaware law "only protects applicants applying for admission into a university, not applicants applying for employment," while "California's law only protects applicants to private employment, not applicants to public employment," and Illinois "only protects applicants from being forced to disclose social networking passwords, leaving open the possibility of employers being permitted to request usernames and passwords to other social media websites, such as blogs"); *see generally* Blanke, *supra* note 41 (providing a thoughtful, helpful, and detailed overview of state legislation enacted in the area as of the date of the article, including similarities and differences in enactments).

161. Stiegler, *supra* note 63, at 322; *see* Park, *supra* note 25, at 783 (noting that although proposed federal enactments and state legislation have some similarities, they "differ dramatically in a number of ways, including the specific prohibited acts, the definitions of important terms such as 'social media' and 'personal account,' whether exceptions or exemptions apply, and language regarding enforcement and penalties").

employers as they attempt to navigate them."[162] Significant criticism followed as well.[163] Not surprisingly, these state-to-state differences prompted some commentators to suggest the need for uniform legislation addressing the topic.[164]

Given this lack of federal action and significant lack of uniformity by the states, and on the crest of what would follow in 2013 when legislation in one or both contexts was considered in at least thirty-six states,[165] and after,[166] the ULC saw the need to fill the void through one act addressing the issues that would be promulgated for enactment by the states.[167]

IV. THE ULC DRAFTING PROCESS

There are several steps in the ULC's studying, drafting, and promulgating legislation to be made available for enactment by the states.[168] The ULC's Committee on Scope and Program receives proposals from a variety of sources.[169] If a proposal looks promising, the Committee on Scope and Program then typically assigns the proposal to a study committee, "which researches the topic and decides whether to recommend that an act be drafted."[170] After that

---

162. Park, *supra* note 25, at 784 (noting the need for "model legislation" in the area).

163. Indeed, one commentator bluntly criticized the effort in an article written as of October 2013 titled "The Spectacular Failure of Employee Social Media Privacy Laws." Eric Goldman, *The Spectacular Failure of Employee Social Media Privacy Laws*, TECH. & MKTG. LAW BLOG (May 31, 2014), http://blog.ericgoldman.org/archives/2014/05/state_laws_to_p.htm.

164. *See* Park, *supra* note 25, at 817 (noting issues that "lead to a conclusion that the uniformity by adopting a model statute is desirable" and proposing such a provision); Hurst, *supra* note 32, at 223 (footnotes omitted) ("It is critical to have uniform legislation prohibiting these forced consent policies because it will prevent situations where students are made to choose between cooperation and embarrassment, or between cooperation and penalization.").

165. *Access to Social Media Usernames and Passwords*, *supra* note 35.

166. *See* Kozlowski, *supra* note 37 (summarizing then-current state enactments addressing "employee (and a little bit of student) privacy and social media accounts," and stating "[w]ith this number of states having already passed laws or having them in the pipeline, it is probably only a matter of time before all 50 states follow suit"); Sprague, *supra* note 25, at 483–84 (footnotes omitted) ("In 2013, at [sic] total of sixty-one such bills were introduced in Congress and thirty-five states, with eight states enacting legislation. As of January 14, 2014, some thirty bills in sixteen states have been reintroduced or carried over, with two states, Florida and Oklahoma, introducing such legislation for the first time."); Brittanee L. Friedman, Note, *#PasswordProtection: Uncovering the Inefficiencies of, and Not-So-Urgent Need for, State Password-Protection Legislation*, 48 SUFFOLK U. L. REV. 461, 463 (2015) (similar).

167. Minutes for Annual Meeting of the Committee on Scope and Program, UNIF. LAW COMM'N 11–12 (July 7–8, 2013), http://www.uniformlaws.org/shared/docs/Scope/Scope%20Minutes%20070713%20FINAL.pdf.

168. *Frequently Asked Questions*, *supra* note 9.

169. *Id.*

170. *Id.*

research, the study committee will recommend to the Committee on Scope and Program whether to proceed with drafting.[171] The Committee on Scope and Program then considers the study committee's report and makes a recommendation to the ULC's Executive Committee, and the Executive Committee then determines whether a drafting project should proceed.[172] If the Executive Committee approves a drafting project, a ULC drafting committee is created, consisting of ULC commissioners (one of whom will serve as chair of the drafting committee), a Reporter (who is an expert in the field of law and typically a law professor), Advisors from the American Bar Association, and Observers, including those from interested organizations.[173] The drafting committee then researches, drafts, considers, and recommends an act for consideration by the ULC Committee of the Whole, where all ULC commissioners provide feedback on the draft and then vote on whether to approve the draft.[174] UESOPPA is the product of each of these typical steps.

A. The ULC Study Committee

Martha L. Walters, Oregon Supreme Court Associate Justice and the first female president of the ULC, is credited with first formally raising the idea of studying whether the organization should draft an act on social media privacy.[175] In July 2013, after considering research provided by ULC legislative staff, the ULC Committee on Scope and Program noted

> [a]s the use of social media has grown, so have employers' and schools' concern about its employees and students use of those outlets. It is not uncommon for employers to ask prospective and current employees for access to social media accounts. In response, many states have introduced or passed legislation aimed to protect

171. *Id.*
172. *Id.*
173. *Id.*
174. *Id.*
175. Minutes for Annual Meeting of the Committee on Scope and Program, UNIF. LAW COMM'N 11–12 (July 7–8, 2013), http://www.uniformlaws.org/shared/docs/Scope/Scope%20Minutes%20070713%20FINAL.pdf; *The Honorable Martha L. Walters*, SUP. CT. OR. JUD. DEP'T, http://www.courts.oregon.gov/Supreme/pages/biowalters.aspx (last visited Feb. 20, 2017).

> individuals from such intrusions, while allowing employers and schools to access accounts under certain circumstances.[176]

As a result, the ULC Committee on Scope and Program adopted a resolution, approved by the ULC's Executive Committee, "that a study committee be formed to study the need for and feasibility of drafting an act on social media privacy."[177]

Frederick P. Stamp Jr., United States District Judge for the Northern District of West Virginia and ULC Commissioner from West Virginia, served as chair of the Study Committee on Social Media Privacy.[178] The Study Committee was not charged with the responsibility of drafting an act, "but of studying the subject and of conducting research to determine whether, in the opinion of that committee, the subject is one on which an act should be drafted."[179]

By January 2014, the Study Committee reported that it had reviewed a great deal of background material and legislation on social media.[180] Noting most of the material was in the employer and educational institution contexts, the committee continued to consider other social media privacy concerns.[181] After an April 2014 stakeholders meeting in Washington, D.C., and further study, in May 2014, the Study Committee voted to recommend that the ULC establish a drafting committee to draft an act on social media privacy.[182]

Based on the Study Committee's final report, the ULC Committee on Scope and Program adopted a resolution in July 2014, approved by the ULC's Executive Committee, "that a drafting committee on Social Media Privacy be formed, and that the scope of the act *be limited to* issues related to employer's

---

176. Minutes for Annual Meeting of the Committee on Scope and Program, UNIF. LAW COMM'N 11–12 (July 7–8, 2013), http://www.uniformlaws.org/shared/docs/Scope/Scope%20Minutes%20070713%20FINAL.pdf.

177. *Id.* at 11.

178. Minutes for Midyear Meeting of the Committee on Scope and Program, UNIF. LAW COMM'N 5 (Jan. 17, 2014), http://www.uniformlaws.org/shared/docs/Scope/Scope%20Minutes%201-17-14%20FINAL.pdf; *Frederick Pfarr Stamp Jr.*, WIKIPEDIA, https://en.wikipedia.org/wiki/Frederick_Pfarr_Stamp_Jr. (last visited Feb. 20, 2017).

179. *Criteria for New Projects*, UNIF. LAW COMM'N, http://www.uniformlaws.org/Narrative.aspx?title=Criteria%20for%20New%20Projects (last visited Sept. 4, 2017).

180. Minutes for Midyear Meeting of the Committee on Scope and Program, UNIF. LAW COMM'N 5 (Jan. 17, 2014), http://www.uniformlaws.org/shared/docs/Scope/Scope%20Minutes%201-17-14%20FINAL.pdf; *Frederick Pfarr Stamp Jr.*, WIKIPEDIA, https://en.wikipedia.org/wiki/Frederick_Pfarr_Stamp_Jr. (last visited Feb. 20, 2017).

181. *Id.*

182. Minutes for Annual Meeting of the Committee on Scope and Program, UNIF. LAW COMM'N 4 (July 12–13, 2015), http://www.uniformlaws.org/shared/docs/Scope/Scope%20Minutes%20071214%20FINAL.pdf.

access to employees' or prospective employees' social media accounts and educational institutions' access to students' or prospective students' social media accounts."[183]

B. The ULC Drafting Committee

The Drafting Committee on Social Media Privacy was created soon after and held the first of its many meetings in November 2014.[184] The Drafting Committee's drafts were considered by the ULC Committee of the Whole (all ULC commissioners) at the July 2015 ULC Annual Meeting, revised, and then considered and approved by the ULC Committee of the Whole at the July 2016 ULC Annual Meeting.[185] After some additional editorial changes, UESOPPA was approved by the ULC Executive Committee in late 2016 and submitted to the American Bar Association for approval. In February 2017, the American Bar Association's House of Delegates approved UESOPPA "as an appropriate [Act] for those states desiring to adopt the specific substantive law suggested therein."[186] This drafting process, however, is best viewed in two stages: (1) work leading up to the 2015 ULC Annual Meeting and (2) work leading up to the 2016 ULC Annual Meeting.

1. The Drafting Process Leading up to the 2015 ULC Annual Meeting

The Drafting Committee met four times before the July 2015 ULC Annual Meeting: (1) November 2014 (by telephone to discuss process, scope, and scheduling); (2) February 2015 (by telephone to begin substantive discussions); (3) three days in late February/early March 2015 (in person); and (4) three days in April 2015 (in person).[187]

Before the February 2015 in-person meeting, Drafting Committee Reporter Professor Dennis D. Hirsch provided the Drafting Committee with a "structure and variables" document, listing the structure of a draft act and identifying

---

183. *Id.* at 4–5 (emphasis added).

184. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 1 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf.

185. *Id.* at 2.

186. *ABA HOD Approves Five Uniform Acts*, UNIF. LAW COMM'N (Feb. 6, 2017), http://www.uniformlaws.org/NewsDetail.aspx?title=ABA%20HOD%20Approves%20Five%20Uniform%20Acts.

187. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 1 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf.

some primary issues to consider.[188] The meeting started with an interactive PowerPoint presentation by Sara H. Jodka, a labor and employment lawyer with expertise in social media-related legal issues, demonstrating how various social media platforms work and how they differ in terms of technology and functionality.[189] The Drafting Committee then engaged in a robust discussion, worked through the issues identified in the structures and variables document, and provided useful initial drafting guidance.[190] After that meeting, Reporter Hirsch prepared two separate draft acts (one addressing the educational context, the other the employment context) to focus further discussion at the April 2015 meeting.[191] With the benefit of another robust discussion at the April 2015 meeting, the Drafting Committee prepared a single draft act that covered both contexts, which was then presented to the Committee of the Whole (all ULC commissioners) at the 2015 ULC Annual Meeting.[192]

During the drafting process, the Drafting Committee and the ULC solicited input and viewpoints from a wide variety of individuals and entities with various and conflicting points of view.[193] Along with ULC commissioners, the Drafting Committee included three American Bar Association Advisors as well as dozens of Observers. Observers included individuals and representatives of organizations representing, advocating for, and/or governing: colleges and universities; the technology, securities, financial services, and banking industries; state governments, legislatures, and courts; education; independent businesses; victim's rights; privacy rights; social media service providers; e-commerce businesses and online consumers; and civil liberties organizations.[194] As with any group of individuals involved in any project, some Observers

---

188. Social Media Privacy Drafting Committee, *Statutory Structure and Variables*, UNIF. LAW COMM'N (Feb. 13, 2015), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2015feb13_SMPA_Statutory%20Structure%20and%20Variables_Hirsch.pdf.

189. Sara H. Jodka, *Social Media Platforms and Privacy Controls*, PowerPoint Presentation, UNIF. LAW COMM'N (Feb. 2015), http://www.uniformlaws.org/Committee.aspx?title=Employee%20and%20Student%20Online%20Privacy%20Protection%20Act (follow February 2015 PowerPoint Presentation hyperlink).

190. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 1 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf.

191. *Id.*

192. *Id.* at 2–3.

193. *Id.* at 2.

194. *See generally* Social Media Privacy Drafting Committee, Minutes for Conference Call, UNIF. LAW COMM'N (Nov. 17, 2014), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2014nov17_SMPA_Conf%20Call_Minutes.pdf; Social Media Privacy Drafting Committee, Minutes for Conference Call, UNIF. LAW COMM'N (Feb. 5, 2015), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2015feb5_SMPA_Conference%20Call%20Minutes.pdf.

provided more input than others; Observers received updated drafts of the project and provided critical insight and input throughout the project.[195]

The draft presented for discussion at the 2015 ULC Annual Meeting introduced many concepts that were retained in the final act.[196] For the definitions used, that draft introduced a "protected personal online account" concept that included accounts beyond traditional social media:

> "Protected personal online account" means an individual's online account that requires login information in order to access or control that account. The term does not include an online account that:
>
> (A) an employer or educational institution supplies or pays for;
>
> (B) an employee creates or maintains on behalf of or under the direction of an employer in connection with that employee's employment; or
>
> (C) a student creates or maintains on behalf of or under the direction of an educational institution in connection with that student's education.[197]

Recognizing the ongoing nature of the effort and the need for additional study, the draft used bracketed language to reflect a tentative structure for the definition of "educational institution," which was defined as "a person that provides to students at the post-secondary[, secondary or middle-school] level an organized course of study [that is academic, technical, trade-oriented or preparatory for gaining employment in a recognized occupation.]"[198] The definition of "employer" was a simple sentence that would later change significantly: "'Employer' means a person that provides compensation to an employee in exchange for services or labor."[199] And although it would later change as well, the 2015 draft definition of "employee" was "an individual who provides services or labor to an employer in exchange for compensation."[200] The term included a prospective employee who has expressed an interest in or

---

195. *Id.*

196. Social Media Privacy Act: 2015 Annual Meeting Draft, UNIF. LAW COMM'N (June 1, 2015), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2015AM_SocialMediaPrivacy_Draft.pdf.

197. *Id.* at 2.

198. *Id.* at 1.

199. *Id.*

200. *Id.*

applied for employment or whom an employer is otherwise considering for employment.[201]

The basic structure of the Act (setting forth definitions, protections, exceptions, and remedies) provided a road map used throughout the drafting process, although there were substantial changes along the way.[202]

Acknowledging the comparatively tentative nature of this early draft, the Drafting Committee expressly solicited comments on various topics at the 2015 ULC Annual Meeting.[203] An issues memorandum summarized the work of the Drafting Committee, provided background on social media, discussed the scope of the Drafting Committee's work, and sought input on specific issues.[204] In addressing scope, the Drafting Committee recognized that the employer and educational institution contexts were not the only coercive situations that might merit protection of social media privacy, but that the ULC Committee on Scope and Program directed that the effort be confined to those two contexts:

> The draft submitted is limited to preventing: (1) employers coercing their employees or prospective employees to provide login information for or access to their protected personal online accounts; and (2) educational institutions coercing their students or prospective students to provide login information for or access to their protected personal online accounts. There may be other coercive situations (the landlord-tenant relationship is one such situation that has been suggested) in which individuals can be pushed to provide such information. The scope of the Committee's work, however, is limited to the employment and education contexts. This scope is consistent with the vast majority of legislation enacted by the states. Accordingly, although recognizing that there may be other coercive situations, the Committee has limited (and will continue to limit) its work to these two critically-important contexts.[205]

Although soliciting input on all aspects of the draft, the Drafting Committee then highlighted four specific issues for consideration.[206]

---

201. *Id.*

202. *See* Social Media Privacy Act: 2015 Annual Meeting Draft, *supra* note 196.

203. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 2 (June 1, 2015), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2015AM_SocialMediaPrivacy_IssuesMemo.pdf.

204. *Id.* at 1–2.

205. *Id.* at 2.

206. *Id.* at 2–3.

First, the Drafting Committee noted "there appears to be consensus that the act should apply to post-secondary schools," but the Committee further noted that it was "particularly interested in comments on whether the act should apply to secondary or even middle-schools."[207]

Second, the Drafting Committee sought input on the definitions of "employee" and "employer," noting that definitions of the "terms var[y] substantially depending upon context and origin and that there is not one generally-accepted definition of either term."[208] "The Committee has no desire to attempt to provide new, whole cloth definitions of the terms."[209] "The draft does, however, use comparatively broad definitions so that independent contractors are included."[210] "The Committee is particularly interested in comments on the definitions used."[211]

Third, highlighting the use of the phrase "protected personal online account," the Drafting Committee noted

> [t]he draft protects all online accounts, not just social media accounts. Existing state acts vary on this point. Some acts govern only social media accounts, while others govern all personal online accounts. The reasons for protecting social media accounts—to prevent employers and educational institutions from using their coercive power in order to invade a private realm—appear to apply with equal force to personal e-mail, messaging, photo-sharing, video-sharing and other such online accounts. In addition, a significant number of states have adopted acts protecting personal online accounts (not just social media accounts), meaning a focus on protected personal online accounts may enhance enactability. Accordingly, the draft applies to protected personal online accounts, a phrase that would cover all login-protected, personal online accounts. The Committee welcomes comments and thoughts on this approach.[212]

Finally, the 2015 ULC Annual Meeting draft had a provision stating that the protections of the Act generally could not be waived "[e]xcept where necessary to demonstrate a skill or proficiency that is directly related to the employee's employment or application for employment," or the "student's

---

207. *Id.* at 2.
208. *Id.*
209. *Id.* at 3–4.
210. *Id.* at 3.
211. *Id.*
212. *Id.*

education or application for admission to an educational institution."[213] The Drafting Committee expressly solicited "input on the no waiver provision, including whether the draft provides the proper exceptions to it."[214]

The Drafting Committee then entertained questions, comments, concerns, critiques, and other offerings at the 2015 ULC Annual Meeting.[215] The Drafting Committee then continued its work to prepare a revised draft for final consideration at the 2016 ULC Annual Meeting.

2. The Drafting Process Leading up to the 2016 ULC Annual Meeting

After receiving comments at the 2015 ULC Annual Meeting, the Drafting Committee met five times before the 2016 ULC Annual Meeting: (1) two days in November 2015 (in person); (2) two days in February 2016 (in person); (3) in April 2016 (by telephone in preparation for review by the ULC's Committee on Style); (4) in May 2016 (by telephone to discuss feedback from the ULC's Committee on Style); and (5) in June 2016 (by telephone).[216] These meetings involved discussion of the comments received at the 2015 ULC Annual Meeting[217] and from other interested individuals and entities, as well as

---

213. Social Media Privacy Act: 2015 Annual Meeting Draft, *supra* note 196, at 8; *see* N.J. STAT. ANN. § 18A:3-31 (West, Westlaw current through 81 Laws 2017, chs. 1–66) ("No public or private institution of higher education in this State shall require a student or applicant to waive or limit any protection granted under this act. An agreement to waive any right or protection under this act is against the public policy of this State and is void and unenforceable.").

214. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 2 (June 1, 2015), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2015AM_SocialMediaPrivacy_IssuesMemo.pdf; *see* Park, *supra* note 25, at 822 (setting forth a proposed employee internet privacy act including a provision that "[t]he rights provided by this Act may not be waived, by contract or otherwise").

215. *See* Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 2 (June 1, 2015), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2015AM_SocialMediaPrivacy_IssuesMemo.pdf.

216. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 1 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf.

217. Of particular interest is a twelve-page summary of the suggestions received at the 2015 Annual Meeting and the responses and summary of the changes that were incorporated. *See generally* Memorandum from Dennis D. Hirsch to Social Media Privacy Drafting Committee, UNIF. LAW COMM'N (Nov. 5, 2015), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2015nov6_SMPA_Reporter%20Memo_Comments%20and%20responses.pdf.

additional research, thought, and consideration by Drafting Committee members, Advisors, and Observers.[218]

The "protected personal online account" concept identified by the Drafting Committee early in the process was retained and refined.[219] Accordingly, at the 2015 ULC Annual Meeting, the Committee on Scope and Program and the Executive Committee approved the Drafting Committee's request for clarification that the protected personal online account concept (which is somewhat broader than a traditional definition of a social media account) did not exceed the Drafting Committee's charge.[220] Following this clarification, the Executive Committee approved the Drafting Committee's request for a name change from Social Media Privacy to Employee and Student Online Privacy Protection, which is more descriptive of the focus and scope.[221] Accordingly, by the time of the 2016 ULC Annual Meeting, the Drafting Committee's name had changed, and the draft was named the Employee and Student Online Privacy Protection Act.[222]

The draft submitted for consideration at the 2016 ULC Annual Meeting was substantially revised and refined from the draft considered at the 2015 ULC Annual Meeting.[223] As relayed by the Drafting Committee in advance of the 2016 ULC Annual Meeting,

> [g]iven the robust discussion at and after the 2015 Annual Meeting, we have had significant further discussions, evolution and refinement in our work. The project also has attracted more and more active interest and input from divergent groups who have thoughtful, deeply-held perspectives on what the draft should and should not do and how the draft should read. Along with input from Committee members, Advisors and Observers, we have received input from industry groups and companies; privacy advocates and consultants; trade associations; academics; universities and colleges and many others. This additional involvement and input, which is ongoing, is very much appreciated and, although complicating significantly the work of the Committee, has helped strengthen the current draft. The Committee also received,

---

218. *See* Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 2 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf.

219. *See id*. at 3–4.

220. *Id.* at 1.

221. *Id.*

222. *Id.*

223. *Id.* at 2.

> accounted for and appreciates formal review and feedback from the Style Committee.[224]

The Drafting Committee solicited input for the draft submitted for consideration at the 2016 ULC Annual Meeting, highlighting five specific issues:

> 1. As the table of contents demonstrates, the structure of the draft has been revised somewhat from last year. For example, the "No Waiver" provision (discussed more fully below) has been removed.
>
> 2. Definition of "Educational institution." Section 2(2). After substantial consideration, input and research, the Committee recommends that the Act apply only to postsecondary educational institutions. As noted above, state legislation varies on this point. Some state statutes apply to primary and secondary schools, in addition to postsecondary schools. Although conceding there are arguments for coverage in primary and secondary schools, the reasons for the recommendation that the Act only apply to postsecondary schools include the greater responsibility that primary and secondary schools have for their students' welfare and the fact that the majority of the state statutes limit coverage to post-secondary schools.
>
> 3. Definition of "Employee" and "Employer." Sections 2(5) and (6). These definitions are broad and differ from those being proposed by the Wage Garnishment Act Drafting Committee. This difference is intentional for a variety of reasons, including that this Act is intended to apply to prospective employees with respect to whom no employer-employee relationship yet exists (and may never exist). Similarly, the protections in this Act do not depend upon the transfer of money, as would appear to be the case in the context of the Wage Garnishment Act.
>
> 4. Removal of "No Waiver" Provision. Given comments received and further research, the Committee elected to remove a provision in an earlier draft of the Act that would have prohibited employees and students from waiving the Act's protections. In addition, the revised draft allows an employer or educational institution to request that an employee or student add the employer or educational institution to the

---

224. *Id.*

> set of persons that are granted access to the individual's protected personal online account (a "friend request," in Facebook terms). This is consistent with the notion that privacy consists, in large part, of the ability to control one's personal information and that voluntary waiver is, accordingly, consistent with prevailing notions of privacy.[225] The Act, however, still prohibits coercive action, meaning any waiver must be voluntary.
>
> 5. Section 5 (Civil Action) has been changed and simplified. Section 5 now allows for a civil action by the [Attorney General] to obtain equitable relief and a civil penalty of up to [$1000] for each violation (with a maximum penalty of [$100,000] for the same act causing more than one violation). Section 5 also allows an employee or student, or prospective employee or student, to obtain equitable relief, actual damages and costs and reasonable attorneys' fees. The relief available to an [Attorney General] and an employee or student, or prospective employee or student, is not mutually exclusive.[226]

The Drafting Committee then entertained questions, comments, concerns, critiques, and other offerings at the 2016 ULC Annual Meeting in two different sessions, revising the draft in between the sessions. The draft was then approved by a vote of the states on July 14, 2016, as the ULC Annual Meeting ended.[227]

Following that approval, the final Act was submitted for review by the ULC Committee on Style; those comments were accounted for and incorporated into the Act, and in late 2016, the Act was then approved as a uniform act[228] by the ULC Executive Committee and named the Uniform Employee and Student Online Privacy Protection Act (UESOPPA). On February 6, 2017, UESOPPA was approved by the American Bar Association's

---

225. *See* Steven L. Willborn, *Notice, Consent, and Nonconsent: Employee Privacy in the Restatement Symposium: Assessing the Restatement of Employment Law: Essay*, 100 CORNELL L. REV. 1423, 1430–38 (2015).

226. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 3–4 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf.

227. UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT §§ 1–10 (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 2016).

228. As used by the ULC, "[a] uniform act is one that seeks to establish the same law on a subject among the various jurisdictions. When the term 'uniform' is used in the nation's laws, it is highly likely that the ULC drafted the act. The ULC also promulgates 'model' acts. An act may be designated as 'model' if the act's principal purposes can be substantially achieved even if the act is not adopted in its entirety by every state." *Frequently Asked Questions*, *supra* note 9.

House of Delegates "as an appropriate Act for those states desiring to adopt the specific substantive law suggested therein."[229] With that approval, UESOPPA officially became available for consideration by state legislatures for enactment.[230] To date, UESOPPA has been introduced as proposed legislation in the legislatures of Minnesota, New York, and Hawaii.[231]

In its work, the Drafting Committee tried to identify the best policies and practices on numerous key issues. In doing so, the Drafting Committee considered wildly divergent points of view and competing concerns of employees, prospective employees, and employers; students, prospective students, and educational institutions; law enforcement; regulatory agencies; privacy advocates; trade associations; academics; and other interested individuals and entities.[232] The pursuit of the Drafting Committee was to prepare a thoughtful, balanced, and workable act that will be enacted in the various states, and an eye on enactability was certainly a key component in the work. As a result, UESOPPA does not take extreme positions; rather, the Act takes a balanced approach, providing protection for employees and students while ensuring those protections are not so strident that they leave employers and educational institutions powerless to take action to ensure public safety, safety in the workplace and school contexts, and also protect their own rights. The hope, as with any new act, is that UESOPPA will offer needed clarity, uniformity, predictability, and fairness and will be enacted broadly.

V. OVERVIEW OF UESOPPA

UESOPPA is, quite intentionally, a very short act. The text of UESOPPA contains less than 2,200 words and, single-spaced, easily fits on five pages. Even double-spaced and with a detailed prefatory note and comments, UESOPPA is seventeen pages long.[233] Although containing ten sections, the

---

229. *See ABA HOD Approves Five Uniform Acts*, *supra* note 186.

230. *Frequently Asked Questions*, *supra* note 9.

231. *Employee and Student Online Privacy Protection Act*, UNIF. LAW COMM'N, http://uniformlaws.org/Act.aspx?title=Employee%20and%20Student%20Online%20Privacy%20Protection%20Act (last visited Apr. 17, 2017).

232. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 2 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf.

233. The approved final text of UESOPPA, with prefatory note and comments, as well as additional information about the ULC, appears as Appendix A to this Article. *See infra* app. A. By way of comparison, other acts that have been widely adopted are far longer. *Compare* UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT §§ 1–10 (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 2016) (seventeen pages with prefatory note and comments), *with* UNIF. ANATOMICAL GIFT ACT §§ 1–11 (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1968) (sixty-four pages with prefatory note and comments), UNIF. CHILD CUSTODY JURISDICTION

key provisions of UESOPPA appear in four of those sections, starting with definitions.

A. Prefatory Note

In a page and a half, the UESOPPA Prefatory Note summarizes the pervasive use of online accounts and related privacy issues and legislative responses and provides an overview of the Act.[234] The Prefatory Note provides a helpful introduction to the specific provisions of UESOPPA and, although providing a lengthy quote, is provided here in its entirety:

> 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/ telecomm unications-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

---

& ENF'T ACT §§ 101–405 (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1997) (seventy-three pages with prefatory note and comments), *and* UNIF. PROB. CODE §§ 1.101–8.102 (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 2008) (803 pages with prefatory note and comments).

234. UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT committee's prefatory note at 1–2 (UNIF. LAW COMM'N 2016), http://www.uniformlaws.org/shared/docs/social%20media% 20privacy/ESOPPA_Final%20Act_2016.pdf.

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.[235]

With this overview, the following discussion gives a more detailed overview of UESOPPA.[236]

B. Definitions

1. "Protected Personal Online Account"

Section 2 of UESOPPA contains the definitions.[237] A cornerstone of UESOPPA is the "protected personal online account" concept, which is defined as follows:

---

235. *Id.*

236. *See* Barbara Atwood, Tim Berg & Sam Thumma, *Uniform Law Commission Addresses Arbitration, Online Privacy, More*, 53 ARIZ. ATT'Y 32, 37–42 (Nov. 2016) (providing a brief overview of UESOPPA).

237. UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT § 2.

> "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.[238]

There is a good deal to this definition of "protected personal online account." Working through the definition, by referencing other defined terms, is the best way to further illuminate both the meaning of the first sentence (which defines the outer limits of the phrase) and then the remainder of the definition (which limits the meaning of the phrase). The best place to start is with who is protected ("employee" and "student") and the corresponding definitions of "employer" and "educational institution."

2. "Employee" and "Employer"

"Employee" is broadly defined as "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."[239] The drafting process made plain that the definition of "employee" can vary greatly depending upon the context. This definition was designed to focus on the nature of the relationship and whether coercion might be used to gain access to a protected personal online account, not merely whether money was provided for services or labor performed. Accordingly, the definition does not require payment for services or labor performed, but it expressly includes relationships where the individual providing the services or labor was given academic credit,

---

238. *Id.* § 2(10) at 4.
239. *Id.* § 2(4) at 3.

occupational experience, or otherwise (including an unpaid intern) even though no money changed hands.[240]

The definition of "employee" goes even further to include a prospective employee who "has expressed to the employer an interest in being an employee" or "has applied for or is applying for employment by, or is being recruited for employment by, the employer."[241] The term also expressly includes "an independent contractor."[242]

In sum, employee includes an individual providing services or labor in exchange for money, academic credit, or occupational experience, and an individual who has expressed to the employer an interest in becoming an employee, who has applied or is applying for such employment, or is being recruited by the employer, and also includes an independent contractor. As explained in the Comment discussing the definition, this breadth was intentional and was designed to account for potentially coercive relationships:

> 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.[243]

UESOPPA relies on this broad definition of "employee" to define, in a mirror image fashion, "employer." "'Employer' means a person that provides salary, wages, or the equivalent 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."[244]

---

240. *Id.*
241. *Id.*
242. *Id.*
243. *Id.* § 2 cmt. at 6.
244. *Id.* § 2(8) at 3–4.

3. "Student" and "Educational Institution"

"Student" similarly is broadly defined as "an individual who participates in an educational institution's organized program of study or training."[245] Akin to the definition of "employee," the definition of "student" includes "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."[246] Recognizing that some students may be minors, the term also includes "a parent or legal guardian of a student under the age of" majority.[247] The corresponding Comment discusses some of the similarities and differences between the definition of "student" and "employee":

> 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.[248]

Unlike the definition of "employer," the definition of "educational institution" limits the universe of schools subject to UESOPPA.[249] "'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."[250] The term includes public and private institutions and an agent or designee of the educational institution.[251] The import of this definition is that, for educational institutions and students,

---

245. *Id.* § 2(14) at 5.
246. *Id.*
247. *Id.*
248. *Id.* § 2 cmt. at 6–7.
249. *Id.*
250. *Id.* § 2(2).
251. *Id.* § 2(2)(A)–(B).

UESOPPA applies only in the postsecondary level (and not to primary or secondary schools).[252]

Whether UESOPPA should apply to primary or secondary schools was discussed by the Drafting Committee throughout the drafting process and expressly raised when the drafts were considered at the 2015 and 2016 ULC Annual Meetings.[253] As explained in the Comment discussing the definition, the limitation to postsecondary schools "is consistent with the majority of existing state laws."[254] As noted by the Drafting Committee in advance of the draft being considered at the 2016 ULC Annual Meeting, this line of demarcation also reflects the greater responsibility that primary and secondary schools have for the welfare of their students.[255] And although not expressly stated in UESOPPA, from an enactability perspective, in at least some jurisdictions, issues of local control by school boards may be a powerful force with strong resistance to legislation that would diminish that local control.[256]

4. "Online," "Login Requirement," and "Login Information"

The other defined terms implicated by the first sentence of "protected personal online account" include "online," "login requirement," and, as a consequence, "login information."[257]

"'Online' means accessibility by means of a computer network or the Internet."[258] Although broad, this definition is significant for what it does not include. As explained in the Comment, the "online" definition "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

---

252. *Id.* § 2 cmt. at 5.

253. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 3 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf.

254. UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT § 2 cmt. at 5.

255. Memorandum from Samuel A. Thumma and Dennis D. Hirsch to Committee of the Whole, UNIF. LAW COMM'N 3 (June 10, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016AM_EmplStudentOnlinePrivProtect_Issues%20memo.pdf; *cf.* Boisson v. Ariz. Bd. of Regents, 343 P.3d 931, 934–35 (Ariz. App. 2015) (discussing duty in the context of the student-school relationship in primary, secondary, and college and university contexts, noting in the primary and secondary school context, "the relationship is custodial").

256. *Cf.* Tiffani N. Darden, *Parental Exclusion from the Education Governance Kaleidoscope: Providing a Political Voice for Marginalized Students in our Time of Disruption*, 22 WM. & MARY BILL RTS. J. 1093, 1122 (2014) ("School board politics unearth controversial debates surrounding local control, resources, and community participation.").

257. *See* UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT § 2(10) at 4.

258. *Id.* § 2(8) at 4.

such cases."[259] A key point is that a stand-alone computer, not connected to a computer network or the Internet, does not fall within the definition of "online" and, accordingly, falls outside the scope of UESOPPA.[260]

"Login requirement" is a transitional phrase which "means a requirement that login information be provided before an online account or electronic device can be accessed or controlled."[261] "Login information," in turn, "means a user name and password, password, or other means or credentials of authentication required to access or control" either a protected personal online account or an electronic device "which the employee's employer or student's educational institution has not supplied or paid for in full, that itself provides access to or control over the account."[262] As explained in the Comment, this broad definition is designed to account for future changes in technology:

> 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."[263]

Rounding out the definitions unique to UESOPPA, "content" is defined as "information, other than login information, that is contained in a protected personal online account, accessible to the account holder, and not publicly available."[264] "'Publicly available' means available to the general public."[265] The key aspect of these definitions is they make plain that UESOPPA applies to restrict access only to non-publicly available information.[266] As noted in the Comment,

> [t]he definition of "content" includes those portions of an individual's protected personal online account that the account holder has access to

---

259. *Id.* § 2 cmt. at 6.
260. *See id.*
261. *Id.* § 2(7) at 4.
262. *Id.* § 2(6) at 4.
263. *Id.* § 2 cmt. at 6.
264. *Id.* § 2(1) at 3.
265. *Id.* § 2(11) at 5.
266. *Id.* § 2 cmt. at 5.

> and could turn over to an employer or educational institution. It thus corresponds to [UESOPPA's] . . . core purpose which is to protect employees and students against coercive demands and requests. The definition makes clear that [UESOPPA] does not prohibit employers or educational institutions from accessing publicly available information.[267]

UESOPPA also includes standard definitions for "electronic,"[268] "person,"[269] "record,"[270] and "state,"[271] which are used by the ULC for all acts when applicable and are not unique to UESOPPA.[272]

C. Protections and Exceptions

With these definitions in hand, what does UESOPPA prohibit, require, do, and not do? The Act has two parallel sections. Section 3 addresses employees and employers,[273] and Section 4 addresses students and educational institutions.[274] These sections contain similar prohibitions and requirements, although tailored to reflect the differences in employment and education.[275]

Stated simply, these sections are divided into four subsections:

- Subsection (a) prohibits an employer or educational institution from taking certain actions that would compromise the privacy of an employee's or student's protected personal online account;
- Subsection (b) creates exceptions to the prohibitions in Subsection (a);
- Subsection (c) provides additional protections and limitations if an employer or educational institution accesses content in a protected personal online account for a purpose specified in Subsection (b)(3); and
- Subsection (d) provides additional protections when an employer or educational institution, by operation of lawful monitoring technology, obtains login information for an employee's or student's protected personal online account.[276]

---

267. *Id.*
268. *Id.* § 2(3) at 3.
269. *Id.* § 2(9) at 4.
270. *Id.* § 2(12) at 5.
271. *Id.* § 2(13) at 5.
272. *Id.* § 2 cmt. at 7.
273. *Id.* § 3 at 7.
274. *Id.* § 4 at 11.
275. *Id.* § 3 at 7–9; *id.* § 4 at 11–13.
276. *Id.* § 3 cmt. at 9; *id.* § 4 cmt. at 13.

Each of these four subsections merit a closer look.

1. Prohibitions

Subject to exceptions discussed in the next subsection, UESOPPA contains two types of prohibitions: (1) prohibiting an employer or educational institution from requiring, coercing, or requesting an employee or student to make login information or content of a protected personal online account available to the employer or educational institution; and (2) prohibiting an employer or educational institution from taking adverse action against an employee or student for failing to comply with a prohibited requirement or request.[277]

Starting with the first category, UESOPPA provides that an employer or an educational institution may not "require, coerce, or request" an employee or student to (1) disclose login information for a protected personal online account; (2) disclose the content of a protected personal online account ("except that an employer [or educational institution] may request an employee [or student] to add the employer [or educational institution] to, or not remove the employer [or educational institution] from, the set of persons to which the employee [or student] grants access to the content"); (3) alter the settings of the protected personal online account so that login information, or content of, the account is "more accessible to others"; or (4) access the account in the presence of the employee [or student] that allows the employer [or educational institution] to see the login information for or content of the protected personal online account.[278]

As stated in the Comment in the employment context and echoed in the Comment in the educational institution context, these prohibitions mean

> 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.[279]

---

277. *Id.* § 3(a)(2)(A) at 7; *id.* § 4(a)(2)(A) at 11–12.

278. *Id.* § 3(a)(1) at 7; *id.* § 4(a)(1) at 11.

279. *Id.* § 3 cmt. at 9–10; *see id.* § 4 cmt. at 13 ("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.'").

The ability of an employer or educational institution to request to be added as a "friend" was designed, among other things, to allow individuals whose creative efforts were resident in a protected personal online account to share that information with an actual or prospective employer or educational institution. For example, absent this exception, it is uncertain whether a design company or educational institution could ask an applicant to provide access to non-public information resident on an applicant's protected personal online account containing the applicant's creative portfolio. The non-coercive personal choice to decide whether to share such information is a key aspect of the privacy rights UESOPPA is designed to protect.[280]

UESOPPA next provides that an employer or educational institution may not "take, or threaten to take, adverse action" against an employee or student for failing to comply with a requirement, coercive action, or request that violates these prohibitions, or for failing to comply with a request to add the employer or educational institution to, or not remove it from, those persons the employee or student grants access to the content of a protected personal online account.[281] The reason for this category of prohibitions is to ensure that all prohibitions have meaning. As crisply stated in the Comment, "[t]his ensures that, even with respect to a request to be added to the list of contacts, the employee [or student] retains the ability to say 'no' without fear of reprisal."[282]

2. Exceptions to the Prohibitions

The prohibitions are subject to certain enumerated exceptions.[283] The exceptions, however, simply provide that nothing in the prohibitions "shall prevent an employer [or educational institution] from" doing certain enumerated things.[284] Critically, these exceptions *do not* authorize such enumerated things but, instead, simply state that the prohibitions do not prohibit the actions described in the enumerated exceptions.[285] This limitation is designed to prevent any confusion about whether UESOPPA authorizes actions described in the enumerated exceptions.[286] As the Comment makes plain,

> [t]he subsection 3(b) exceptions limit the scope of the subsection 3(a) prohibitions. ***They do not create affirmative rights.*** Thus, if a 3(b)

280. *Id.* prefatory note at 1.
281. *Id.* § 3(a)(2) at 7; *id.* § 4(a)(2) at 11–12.
282. *Id.* § 3 cmt. at 10; *see id.* § 4 cmt. at 13.
283. *See id.* § 3(b) at 8; *id.* § 4(b) at 12.
284. *Id.*
285. *See id.* § 3 cmt. at 10.
286. *See id.*

> 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.[287]

With that essential caveat, these exceptions fall into three categories.

First, the prohibitions do not prevent an employer or educational institution from "accessing information about an employee [or student] which is publicly available."[288] This exception is consistent with the focus of UESOPPA, including the definitions of "protected personal online account" and "content," which is to protect information that is "not publicly available."[289]

Second, the prohibitions do not prevent an employer or educational institution from "complying with a federal or state law, court order, or rule of a self-regulatory organization established by federal or state statute," and for an employer (but not an educational institution), "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)."[290] This exception recognizes the supremacy of federal law as well as the need to comply with other aspects of state law and court orders.

The Comment to this exception focuses on self-regulatory organizations both in the employment and educational institution contexts.[291] In the employment context, the Comment states:

> The principal self-regulatory organizations intended here are those defined [in] 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

---

287. *Id.* § 3 cmt. at 10–11; *accord id.* § 4 cmt. at 13–14 ("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.'").

288. *Id.* § 3(b)(1) at 8; *id.* § 4(b)(1) at 12.

289. *Id.* § 2(1) at 3; *id.* § 2(10) at 4; *see id.* prefatory note at 2.

290. *Id.* § 3(b)(2) at 8; *id.* § 4(b)(2) at 12.

291. *Id.* § 3 cmt. at 10; *see id.* § 4 cmt. at 14 ("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.'").

> 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.[292]

In the educational institution context, the Comment states:

> 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*.[293]

These Comments make plain that this exception is limited and is not intended to apply to regulations or guidelines established by self-regulatory organizations that are not established by federal or state statute.[294] This prevents employers or educational institutions from establishing a self-regulatory organization without statutory authorization to promulgate a rule that would negate the protections in UESOPPA.[295]

Third, the prohibitions do not prevent an employer or educational institution from "requiring or requesting, based on specific facts about the employee's [or student's] protected personal online account, access to the content of, but not the login information for, the account in order to" undertake certain defined investigations or protection.[296] The limitations hard-wired into this third exception are intentionally substantial.

This exception requires "specific facts," not mere general facts or allegations.[297] The "specific facts" must be about the employee's or student's "protected personal online account,"[298] not about issues unrelated to such an

---

292. *Id.* § 3 cmt. at 10.
293. *Id.* § 4 cmt. at 14 (emphasis added).
294. *Id.* § 3 cmt. at 10; *id.* § 4 at 14.
295. *See id.*
296. *Id.* § 3(b)(3) at 8; *id.* § 4(b)(3) at 12.
297. *See id.*
298. *Id.*

account. And the exception expressly does not allow access to "the login information for" the protected personal online account.[299] Indeed, nowhere does UESOPPA allow an employer or educational institution to compel the production of login information for an employee's or student's protected personal online account.[300]

Based on specific facts about an employee's or student's protected personal online account, an employer or educational institution may require or request access to the content of an employee's or student's protected personal online account to "ensure compliance, or investigate non-compliance, with . . . federal or state law."[301] This exception is consistent with the exception allowing an employer or educational institution to comply with federal or state law, by allowing (based on specific facts about the relevant protected personal online account) to take action to comply with, and investigate non-compliance with, such law.[302]

Based on specific facts about an employee's or student's protected personal online account (as applicable), access to an employee's or student's protected personal online account may be required or requested:

- by an employer to "ensure compliance, or investigate non-compliance, with . . . 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,
- by an educational institution to "ensure compliance, or investigate noncompliance, with . . . 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

299. *Id.*

300. *See id.* prefatory note at 1–2, §§ 1–10 at 3–17.

301. *Id.* § 3(b)(3)(A)(i) at 8; *id.* § 4(b)(3)(A)(i) at 12.

302. *Compare id.* § 3(b)(3)(A)(i) at 8 (allowing employer to require or request access to content of the employee's protected personal online account in order to "ensure compliance, or investigate non-compliance" with state or federal law, when such request or requirement is, based on certain facts relating to that account), *and id.* § 4(b)(3)(A)(i) at 12 (allowing educational institution to require or request access to content of the student's protected personal online account in order to "ensure compliance, or investigate non-compliance" with state or federal law, when such request or requirement is, based on certain facts relating to that account), *with id.* § 3(b)(2) at 8 (stating prohibitions in subsection (a) do not prevent an employer from complying with state or federal law), *and id.* § 4(b)(2) at 12 (stating prohibitions in subsection (a) do not prevent an educational institution from complying with state or federal law).

> created primarily to gain access to a protected personal online account."[303]

Again, these provisions contain substantial limitations, including that the prohibition for which compliance is being investigated must be (1) an employer or educational institution prohibition; (2) against employee or student misconduct; (3) of which the employee or student has reasonable notice; (4) in a record; and (5) which is "not created primarily to gain access to a protected personal online account."[304] As noted in the Comment applicable in both the employer and educational institution contexts,

> [t]his 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.[305]

Finally, based on specific facts about an employee's or student's protected personal online account (as applicable), access to that account may be required or requested by an employer or educational institution to "protect against: (i) a threat to safety; (ii) a threat to employer [or educational institution] information technology or communications technology systems or to employer [or educational institution] property; or (iii) disclosure of information in which the employer [or educational institution] has a proprietary interest or information the employer [or educational institution] has a legal obligation to keep confidential."[306] These are limited exceptions to the protections of UESOPPA, which require specific facts about the relevant protected personal online account, and even then, allow access to the content of (but not login information for) the account to protect against a threat to safety, information

---

303. *See* UNIF. EMP. & STUDENT ONLINE PRIVACY PROT. ACT § 3(b)(3)(A)(ii) at 8; *id.* § 4(b)(3)(A)(ii) at 12.

304. *Id.*

305. *Id.* § 3 cmt. at 10; *see id.* § 4 cmt. at 13 ("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.'").

306. *Id.* § 3(b)(3)(B) at 8; *id.* § 4(b)(3)(B) at 12.

technology or communications system, employer or educational institution property, or disclosure of proprietary information or information the employer or educational institution has a legal duty to keep confidential.[307]

3. Use of Content

Along with the restrictions on how an employer or educational institution may require or request access to content in this third category, UESOPPA contains important limitations on the use of such information if it is accessed.[308] This limitation on use provides additional protections if an employer or educational institution properly accesses content in a protected personal online account for a purpose specified in Subsection (b)(3) of the Act.[309] Those limitations are that an employer or educational institution that accesses content for such a purpose: "(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."[310] As noted in the Comment, again applicable in both the employer and educational institution contexts,

> [s]ubsection 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.[311]

4. Use of Login Information

The final restriction set forth in UESOPPA applies when an employer or educational institution acquires login information for a "protected personal online account by means of otherwise lawful technology that monitors the employer's [or educational institution's] network, or employer- [or educational institution-] provided devices, for a network security, data confidentiality, or

---

307. *Id.*

308. *Id.* § 3 at 7–9; *id.* § 4 at 11–13.

309. *See id.*

310. *Id.* § 3(c) at 8–9; *id.* § 4(c) at 13.

311. *Id.* § 3 cmt. at 11; *see id.* § 4 cmt. at 13 ("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.'").

system maintenance purpose."[312] In that event—where an employer or educational institution has obtained login information through lawful monitoring technology—UESOPPA provides four additional protections regarding that login information.[313] Specifically, the employer or educational institution:

> (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 [or 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.[314]

As reflected in the Comment, this further limitation

> takes account of the fact that employers [and educational institutions], in conducting information and communications system monitoring required for maintenance and cybersecurity, may inadvertently gain access to login information for an employee's [or student's] protected personal online account. It makes clear that, while such capture of login information does not, in itself, violate [UESOPPA], employers [and educational institutions] 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.[315]

---

312. *Id.* § 3(d) at 9; *id.* § 4(d) at 13.

313. *Id.* § 3(d)(1)–(4) at 9; *id.* § 4(d)(1)–(4) at 13.

314. *Id.*

315. *Id.* § 3 cmt. at 11; *see id.* § 4 cmt. at 13 ("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.'").

D. Enforcement Provisions

UESOPPA expressly provides that civil actions may be brought either by an appropriate governmental enforcement agency (presumptively, the relevant state's attorney general) or by the employee or student harmed by a violation of the Act.[316] These actions are not mutually exclusive, and both can be brought for the same violation.[317] Similarly, UESOPPA "does not effect a right or remedy available under law other than" the Act, meaning other statutory or common law claims could be asserted along with a claim for a violation of the Act.[318]

The available remedies under UESOPPA depend upon whether the action is brought by an appropriate governmental enforcement agency or by an employee or student.[319] A prevailing governmental enforcement agency "may obtain[: (1)] injunctive and other equitable relief [; and (2) a civil penalty of up to $[1,000] for each violation but not exceeding $[100,000] for all violations caused by the same event]."[320] As explained in the Comment, by bracketing the monetary amounts, this provision

> 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. [This provision] 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.[321]

316. *Id.* § 5(a)–(b) at 14.
317. *See id.* § 5(c) at 14.
318. *Id.* § 5(d) at 14; *see id.* § 5 cmt. at 15.
319. *Id.* § 5(a)–(b) at 14.
320. *Id.* § 5(a) at 14.
321. *Id.* § 5 cmt. at 14–15; *accord id.* § 5 legislative note at 14.

The brackets surrounding the monetary penalty language (the second alternative) allow states to authorize the appropriate governmental enforcement agency to seek only injunctive or equitable relief (but not a civil penalty).[322]

For private civil litigation, UESOPPA provides that a prevailing employee or student may obtain against the relevant employer or educational institution "(1) injunctive or other equitable relief; (2) actual damages; and (3) costs and reasonable attorney's fees."[323] To avoid any uncertainty, the Comment provides that this provision "establishes a private right of action for employees and students."[324] "No mental state is specified for a cause of action" under the Act.[325] Finally, UESOPPA expressly states that it "does not affect a right or remedy available under law other than" the Act.[326]

E. Other Guidance in UESOPPA

Along with the statutory text and corresponding Comments, UESOPPA also includes Legislative Notes.[327] In promulgating UESOPPA, the ULC sought to provide protections, exceptions, and other guidance in the employer-employee context and the educational institution-student context.[328] The ULC promulgated UESOPPA "*as an integrated whole*" to be enacted by state legislatures in both contexts.[329] However, recognizing that some states have enacted legislation in one of these contexts (but not both), the Legislative Notes include a user's guide for states as to what sections of UESOPPA should be enacted if a state "wishes to adopt only the employee provisions of the UESOPPA" or "wishes to adopt only the student provisions of the UESOPPA."[330]

VI. CONCLUSION

UESOPPA attempts to strike a delicate balance to protect and reflect legitimate rights of employees and employers as well as students and educational institutions. Using the "protected personal online account" concept as the cornerstone, UESOPPA deals with similarly situated accounts similarly

322. *Id.* § 5 legislative note at 14.
323. *Id.* § 5(b) at 14.
324. *Id.* § 5 cmt. at 15.
325. *Id.*
326. *Id.* § 5(d).
327. *Id.* § 5 legislative note at 14; *id.* § 8 legislative note at 16; *id.* § 9 legislative note at 16.
328. *Id.* prefatory note at 1–2.
329. *See id.* § 9 legislative note at 16.
330. *Id.*

and provides protection to true social media as well as more general (and more pervasive) login-protected online accounts.

In substance, UESOPPA does four things: (1) provides specific protections for protected personal online accounts held by employees and students against coercive disclosure by employers and educational institutions; (2) provides certain narrowly-tailored exceptions to those protections; (3) limits an employer's or educational institution's use of information obtained from an employee or student based on specific facts about that individual's protected personal online account obtained to ensure compliance with or investigate non-compliance with law or to protect against a threat to safety or information or proprietary interests; and (4) severely limits an employer's or educational institution's use of login information for a protected personal online account if obtained as a result of lawful monitoring.[331] UESOPPA then provides civil remedies for violations of these provisions.[332]

UESOPPA provides consistency and uniformity, builds on the best of the current state enactments, and avoids ambiguities and uncertainties. UESOPPA provides a thoughtful balance of the issues and interests for all involved, including protecting students and employees against coercive behavior.[333] UESOPPA also provides employees and employers, as well as students and educational institutions, much needed predictability and certainty for their conduct, relationships, policies, and procedures. As UESOPPA gains widespread acceptance, the current uncertainty and unpredictability that exists because of significant variations in various state laws should abate. UESOPPA can provide guidance for individuals, entities, and their representatives and add certainty in their conduct, relationships, policies, and procedures. The hope is that the states will recognize the need for uniformity in these areas, agree with the policies reflected in UESOPPA, and enact it.

331. *Id.* § 3 at 7–9; *id.* § 4 at 11–13.
332. *Id.* § 5 at 14.
333. *See id.* prefatory note at 1–2.

*

APPENDIX A

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

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

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 . . . .