

INTRODUCTION TO THE EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

June 10, 2016

Samuel A. Thumma, Drafting Committee Chair
Dennis D. Hirsch, Drafting Committee Reporter

This memorandum provides an introduction to the draft Employee and Student Online Privacy Protection Act (ESOPPA) to be considered at the meeting of the Uniform Law Commission Committee of the Whole in Stowe, Vermont, in July 2016. This memorandum addresses ten questions, in summary form, to introduce ESOPPA. The relevant provisions of ESOPPA referenced in this document provide far more detail. This memorandum provides only a basic roadmap; specific questions and issues are best addressed by referencing the text of ESOPPA.

1. What is the focus of ESOPPA? ESOPPA and related state statutes arose in response to incidents in which employers and educational institutions demanded that employees and students provide them with access to the employees' and students' personal online accounts. ESOPPA prevents employers and educational institutions—which hold significant power over employees and students—from making such demands. It thereby enables employees and students to maintain the privacy of their personal online accounts. ESOPPA is limited in scope. Its protections apply only in two contexts: (1) employer and employee (including prospective employee); and (2) educational institution and student (including prospective student).

2. What does ESOPPA prohibit? Where applicable, ESOPPA provides that an employer or prospective employer may not require, coerce, or request that an employee or prospective employee disclose the login information for or content of a protected personal online account. ESOPPA allows employers to request (but not require or coerce) the employee or prospective employee to add it to the set of persons to whom the employee grants access to the account (a “friend request,” in Facebook terms). *See* Section 3(a). ESOPPA has similar provisions regarding educational institutions and students or prospective students. *See* Section 4(a).

3. To whom does ESOPPA Apply? ESOPPA applies to: (1) an employer and (2) a public or private educational institution providing a postsecondary organized course of study or training, and an agent or designee of such an employer or educational institution. Sections 2(2) (“Educational Institution”), 2(6) (“Employer”).

4. Who is protected by ESOPPA? ESOPPA protects: (1) employees and prospective employees and (2) students and prospective students. Sections 2(5) (“Employee”), 2(14) (“Student”).

5. What is protected? ESOPPA protects the login information for and content and settings of “protected personal online accounts.” A protected personal online account is an individual’s online account that is protected by a login requirement. Section 2(12). Given this definition, a protected personal online account can be a variety of things, including an online bank or trading

account; an electronic mail account or a social media account. The key is that that account be “protected” by a login requirement, and that it be “personal” not public. ESOPPA does not limit employers’ or educational institutions’ ability to access account information that is publicly available. Section 2(12)(A). Several other exceptions also apply. Sections 2(12)(A) & (B).

6. Can an employer or educational institution retaliate against an employee or student who fails to comply with an unlawful demand for access? No. An employer and an educational institution may not take or threaten to take adverse action against an employee or student for failure to comply with a requirement, coercive action or request that violates ESOPPA. *See* Sections 3(a)(2) & 4(a)(2).

7. Are there exceptions to the prohibitions of ESOPPA? Yes. ESOPPA does not prevent an employer or educational institution from accessing publicly available information or complying with a federal or state law or a rule of a self-regulatory organization established by federal or state statute. ESOPPA also does not prevent an employer or educational institution from exercising its existing rights to require or request, based on specific information about the employee’s or student’s protected personal online account, access to content to ensure compliance with, or investigate non-compliance with, federal or state law or an employer policy or protect against specified threats or disclosure of certain proprietary or confidential information. *See* Sections 3(b)(1)-(3); 4(b)(1)-(3).

8. Does ESOPPA address lawful network-monitoring or device-monitoring technology used for network security? Yes. *See* Sections 3(d); 4(d).

9. Who can enforce ESOPPA? An Attorney General or an employee or student harmed by conduct in violation of ESOPPA. *See* Section 5.

10. What remedies are available under ESOPPA? An Attorney General can obtain injunctive or other equitable relief and a civil penalty of up to [\$1,000] for each violation, but if the same act causes more than one violation, the maximum penalty is [\$100,000]. Section 5(a). An employee or student may obtain injunctive and other equitable relief; actual damages and costs and reasonable attorneys’ fees. Section 5(b).