STUDENT PRESS splc LAW CENTER

The knowledge to speak responsibly. The courage to speak freely.

1608 Rhode Island Ave. N.W., Suite 211
Washington, D.C. 20036

(202) 785-5450
www.splc.org | splc@splc.org

July 7, 2016

Members of the Uniform Law Commission
111 N. Wabash Ave., Suite 1010
Chicago, IL 60602
VIA ELECTRONIC DELIVERY AND U.S. MAIL

Dear Commission Members

The Student Press Law Center is a nonprofit center of legal research and advocacy that for 43 years has supported the work of students involved in gathering and sharing news at the college and K-12 levels. In that role, we work regularly with issues involving the confidentiality of students' records and information, in particular with the very confusing patchwork of state and federal privacy laws beginning with the Family Educational Rights and Privacy Act. Our legal staff provided expert testimony in support of Maryland H.B. 934, a social-media privacy bill signed into law by Gov. Hogan in 2015, and we have worked with advocates in other states on language tailored to protect students against "fishing expeditions" into their private, off-campus social interactions by school and college administrators.

We are writing to express significant alarm at aspects of the model Employee and Student Online Privacy Protection Act ("the Act"), elements of which would set back the privacy interests of college students rather than advancing them. We urge that the Commission vote down the proposed draft unless significant revisions are made to address the shortcomings of the Act as circulated.

The most unacceptable aspect of the Act, at Sec. 4(b), affords colleges a virtual blank check of authority to exempt themselves from the proscription against demanding access to the nonpublic portions of students' Internet accounts. As drafted, the subsection enables a college to pierce the statutory assurance of privacy for the following specified purposes (boldface emphasis supplied):

(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 information about the student's protected personal online account, access to content for the purpose of:

(A) ensuring compliance, or investigating non-compliance, with federal or state law **or an educational institution policy**; or

(B) protecting against:

(i) a threat to health or safety;

(ii) a threat to educational institution information technology or communications technology systems or to 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.**

If adopted, these exemptions would entirely negate the effectiveness of the statute, rendering its protections so readily overcome as to be illusory. To address the most troubling of the exemptions highlighted above:

First, and as a blanket comment applying to each of the exemptions addressed below, the Act is deficient insofar as it requires no showing of probable cause, or even of reasonable suspicion, before a student's statutorily protected privacy may be overcome in support of an "investigation." It appears from the plain language of the statute that simply invoking the word "investigation" is sufficient to justify any degree of intrusion, regardless of how speculative the information on which the investigation is based, how minor the infraction being investigated, or how remotely or tangentially the student's Internet accounts might relate to the subject matter of the investigation. This is flatly irreconcilable with well-established constitutional search-and-seizure principles reaffirmed as recently as the Supreme Court's cellphone-search case, *Riley v. California*, 134 S. Ct. 2473 (2014).

Enabling an institution to intrude into a student's nonpublic digital life for purposes of compliance with an "institution policy" entirely nullifies the remainder of the Act. Essentially *any* intrusion may be justified by reference to some "policy" of an institution, which might include "policies" of respect for authority or civility. The Supreme Court has categorically rejected the notion that, when a student is speaking on personal time outside of the classroom setting, a public institution may enforce standards of propriety penalizing even highly offensive speech. *See, e.g., Papish v. Board of Curators of Univ. of Mo.*, 410 U.S. 667 (overturning college's disciplinary action for student's independently produced publication that contained strong profanity and political cartoon depicting rape). To empower a college to demand access to a student's most private communications, including communications with family members, in the name of enforcing "institution policy" is an engraved invitation to abusive overreaching.

Additionally, the exemption entitling colleges to search the Internet accounts of students to protect "information in which the educational institution has a proprietary interest" or "information the educational institution has a legal obligation to keep confidential" is so open-ended that it lacks any rational end point.

"Proprietary interest" is a term undefined in the Act that, at the very least, will be understood to potentially encompass any document in which a university owns the copyright. But copyright protects *any* document memorializing work with a modicum of creativity and originality, including letters, memos, reports, maps, scholarly articles and so on. For example, courts have held that the syllabus created by a college professor is a copyright-protected document. *See, e.g., NCTQ v. Curators of University of Missouri,*

446 SW 3d 723 (Mo. App. 2014). Would an anonymous tip that a college student has posted the syllabus of a class in which she is enrolled on a Facebook discussion wall where her classmates can view it constitute sufficient grounds to demand access to that student's Facebook password? The Act as drafted suggests that the answer is "yes," and that simply cannot be the case. The Act does not require proof that the student is engaging in *illegal* distribution of a university's proprietary work, and indeed many redistributions of copyright-protected work, particularly in the nonprofit educational setting, are recognized as lawful "fair uses."

The suggestion that students might be using personal Internet accounts to disseminate "information the educational institution has a legal obligation to keep confidential" simply misapprehends the scope of legally protected confidentiality in ways that will invariably lead to abuse.

By definition, the Family Educational Rights and Privacy Act ("FERPA") applies only to "education records" that contain nonpublic information and are centrally "maintained" in a college's records repository. It should go without saying that a student's personal Facebook account is not an official college records repository, and the set of circumstances under which a student might realistically compromise FERPA by sharing information on a personal Internet account is so farfetched as to be unworthy of statutory recognition. As the Supreme Court has told us, even students' classroom academic work in the hands of fellow students does not obtain FERPA protection unless and until it is "maintained" in a centralized school database. *Owasso Indep. School Dist. No. I-011 v. Falvo*, 534 U.S. 426 (2002). The set of documents that a non-employee student might possess that would fall within the confidentiality strictures of FERPA will be, for all practical purposes, an empty set. Any education records that might have been misappropriated by a student *employee* will already be covered by the strictures in Section 3 of the Act regarding employee Internet accounts, rendering subsection 4(b)(3)(b)(iii) at best confusingly redundant and at worst a "fishing license" for ill-motivated administrators.

It is documented beyond dispute that educational institutions routinely and purposely misinterpret the scope of FERPA to advance their illicit interests in concealing truthful information damaging to their reputations. *See, e.g., The News and Observer Publishing Co., et al. v. Baddour*, No. 10-CVS-1941 (N.C. Super. Ct. May 12, 2011) (university miscategorized athletes' parking tickets and coaches' cellphone bills as confidential FERPA records to withhold records from journalists investigating athletic-department academic scandal). If colleges are given legal sanction to invade the privacy of students' email accounts and social-media accounts simply by invoking copyright law or FERPA, there will be no principled stopping point and essentially any intrusion, no matter how unfounded, will be impervious to challenge.

Notably, subsection 4(b)(3)(b)(III) does not limit itself to searches for actual violations of FERPA but for information that the *college* has a duty to keep confidential, even if the student Internet accountholder is herself under no such duty. For example, take the example of a student whistle-blower who wishes to contact the news media to share

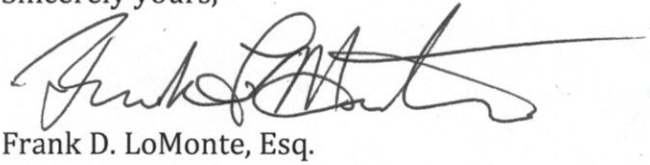
copies of her Title IX sex discrimination complaint against her university. A Title IX complaint is, to use the terms of the statute, "information the educational institution has a legal obligation to keep confidential." Would the Act empower colleges to search the Internet accounts of student journalists and their confidential sources to find out who has a copy of a Title IX complaint, even though the journalists are themselves under no obligation to keep that information confidential? Again, a literal reading of the Act suggests that the answer is "yes," and that cannot be the right answer.

The combined effects of subsections 4(b)(3)(A) and 4(b)(3)(b) would place college students in a worse position than they are today, as few institutions (particularly public ones where constitutional safeguards apply) would believe themselves to have such audaciously broad search authority in the absence of legislative ratification.

Finally, we hope that you will consider upon further reflection including the privacy of K-12 as well as college students within the scope of the model Act, which as it stands applies only to those enrolled in postsecondary education, leaving the most vulnerable students unprotected. The litany of abuses of students' digital privacy by K-12 schools is depressingly long, but perhaps best exemplified by the case of *R.S. v. Minnewaska Area School District*, 894 F.Supp.2d 1128 (D. Minn. 2012), In that case, a high school administrator (accompanied by a uniformed police officer) forced a 12-year-old girl to log into Facebook in his office so that he could read her private one-on-one chat messages exchanged during out-of-school off-hours after receiving a complaint from a parent that the girl was engaged in "naughty" sexual banter with her preteen boyfriend. The traumatic impact of such an invasion on minors is qualitatively greater than the impact on a 20-year-old college student, who is far more likely to have the fortitude to refuse an illicit demand or to contact legal counsel in the face of institutional coercion. The Act is woefully incomplete if it omits protection for K-12 students, and will affirmatively set back efforts to pass more comprehensive statutes such as Michigan's excellent Internet Privacy Protection Act, enacted in 2012 and codified at MCLS § 37.271 *et seq.*

We would be pleased to work with the Commission on a more comprehensive approach to digital privacy that advances the safety of all students, most especially the student journalists who must have confidence in the security of their communications to tell important stories informing their communities.

Sincerely yours,



Frank D. LoMonte, Esq.
Executive Director
Student Press Law Center