July 8, 2016

Employee and Student Online Privacy Protection Act
Response of the Drafting Committee Chair and Reporter to Recent Correspondence

Dear Commissioners,

Thank you, again, for your wonderful, hard work on the Employee and Student Online Privacy Protection Act (ESOPPA). We appreciate it a great deal and are looking forward to our continued conversation in Vermont. ESOPPA is getting more and more attention, input and scrutiny, which is great. We have welcomed this input and have endeavored to account for it all along the way. We recently received letters from the Foundation for Individual Rights in Education (FIRE) as well as the Electronic Frontier Foundation and other groups (EFF) and most recently from the Student Press Law Center (SPLC). We have asked that print copies be available for all Commissioners at the annual meeting in Vermont. We appreciate the significant interest by these groups and their deeply-held concerns. There is no doubt that this input will strengthen our work.

Although our review of these letters is ongoing, we wanted to share with you our thoughts to date for your consideration. We address all the letters at once since, from our read so far, they appear to present substantially similar arguments.

The letters make a constitutional argument and three policy arguments. As we see it, the constitutional argument is based on a misreading of the draft. The policy issues are ones that the Committee weighed when it produced the draft and on which reasonable people can differ. We believe that the Committee resolved these difficult policy issues correctly.

<u>Constitutional issue</u>:

The draft contains two main sections. Section 3 governs employers. Section 4 governs educational institutions. Otherwise, these two sections are largely the same.

Sections 3 and 4 are each structured in the form of prohibitions (in subsections 3(a) and 4(a)) followed by exceptions to those prohibitions (in subsections 3(b) and 4(b)). Subsection 3(a) prohibits employers from requiring or requesting that their employees disclose login or content information for their online accounts (although they can request that the employee "friend" the employer). Subsection 4(a) imposes the same prohibition on educational institutions. Subsections 3(b) and 4(b) directly follow the prohibitions, and create exceptions to them.

In their Constitutional argument, the letters focus on the exception contained in subsection 3(b)(3) (for employers) and 4(b)(3) (for educational institutions). The relevant part of this exception states as follows:

> "(b) Nothing in subsection (a) shall prevent an employer/educational institution from . . .
> (3) requiring or requesting, based on specific information about the employee's/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 employer policy; or

(B) protecting against:

(i) a threat to health or safety;
(ii) a threat to employer information technology or communications technology systems or to 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."

The Committee included this exception for a reason. It recognized that, where an employer or educational institution has "specific information" about a violation of law or organizational policy, it may well need to investigate it by asking for account content. The prohibitions in subsection (a) would have prevented such investigations. This exception allows them.

The letters claim that the exception "authorizes" employers and educational institutions (hereinafter, "organizations") to require employees and students to turn over their login information and content where they have specific information that triggers one of the (b)(3) exceptions.[1] This, they say, violates the Fourth Amendment with respect to public employers and public schools (the entities that the Fourth Amendment governs). This argument has two flaws.

To begin with, the (b)(3) exception as written allows employers and educational institutions only to demand "content." It does not allow them to demand "login information." The Committee consciously made this distinction in order to offer greater protection for login information than for content. All three of the letters ignore the distinction, asserting that the exception allows institutions to demand both content and login information. That is incorrect.

The constitutional argument also contains a second, more significant error. The letters state that the statutory exceptions "authorize" institutions to make these demands. That is not right. The (b)(3) exceptions to which the letters refer do not affirmatively authorize institutions to do anything. They simply say that, in the specified situations (specific information about a violation of law or institutional policy, or a threat to health or property), the subsection (a) prohibition on demanding content will not apply. The key language here is the initial sentence in subsection (b): "Nothing in subsection (a) shall prevent an employer from . . . " As this language makes clear, all that the (b)(3) exceptions do is reinstate the legal status quo by suspending the subsection (a) prohibitions. They do not affirmatively authorize organizations to do anything.

Given that the (b)(3) exceptions do not authorize any particular action, they cannot violate the Fourth Amendment. They leave the legal status quo unchanged. If the Fourth Amendment prohibits a particular school or employer request, then this is part of the legal status quo that the exceptions recognize. The (b)(3) exceptions do not conflict with this; they respect it. As a result, they are fully consistent with the Fourth Amendment. This is the central flaw in the letters' constitutional argument and explains why, contrary to the assertions, the draft does not violate the Fourth Amendment even with respect to public employers and public schools.

[1] The FIRE letter says that institutions can do this "whenever" the institution claims it needs access for one of these purposes. This is incorrect. The draft states that institutions can demand access only when they have "specific information" about the individual's account indicating that one of the (b)(3) exceptions has been triggered. It does not allow them to do this "whenever" they claim there is a need to do so. The EFF letter correctly understands this, but the FIRE letter does not.

Policy arguments

The letters make three policy arguments. During its deliberations the Committee considered each of these issues. However, it reached different conclusions than those that the letters assert.

1. The breadth of the exception

First, the letters take issue with the exception, contained in (b)(3)(A), for situations in which the organization demands or requests content information for the purpose of "ensuring compliance, or investigating non-compliance, with . . . an employer/educational institution policy." The EFF and FIRE letters assert that this would allow organizations intentionally to institute broad workplace or school policies and then use alleged violations of them as a vehicle for demanding wide access to account content.

The Committee considered this concern when preparing the draft. It noted, first, that the exception applies only where the organization has "specific information" about the individual's account that indicates a violation of organizational policy. The FIRE letter ignores this important limitation (see footnote 1, above), although the EFF letter recognizes it.

The Committee further determined that any attempt to narrow the exception would create more problems than it solves. One way to narrow it would be to specify particular policies (e.g. sexual harassment), the violation of which triggers the exception. The problem with this is that it is impossible to identify all important employer and school policies in advance. The draft would almost certainly miss some. This would make the exception too narrow. It would create a situation in which employers have specific information about a violation of an important policy and yet are unable to investigate it by asking to see the content in question. Another way to narrow it would have been for the draft to state that the exception applies only where the organization has information about the violation of an "important" or "significant" organizational policy. But what counts as "important" or "significant"? It is unclear. Such a standard would generate great uncertainty and litigation. The Committee decided that, of the three alternatives (violation of any organizational policy, violation of specified policies, and violation of important or significant policies) the broader exception made the most sense.

Aware that the exception could sweep quite broadly, the Committee took steps to limit its breadth. It defined the terms "employer policy" and "educational institution policy" as "a policy an employer/school establishes for the institution, which is in a record, of which students have reasonable notice, and which was not created primarily to gain access to a protected personal online account." (see subsections 2(3) and 2(7)). As a result, the exception applies only where the policy in question is in a record of which the employee/student has notice. It also prevents organizations from intentionally creating a broad policy as a vehicle for justifying access to individual accounts. It says that such policies – those "created primarily to gain access" to an account – do not count as employer or educational institution policies for the purposes of the exception. This should allow courts to address those situations in which employers or educational institutions pass broad policies whose real purpose is to give them an opportunity to demand access. The Committee took the approach that, with this limitation in place, it makes sense to select the broader exception. This is a reasonable choice and, we believe, the correct one.

2. Limiting access to relevant content

The draft creates additional precautions. It includes sections 3(c) (for employers) and 4(c) (for educational institutions) which state that:

> "(c) An employer/school that accesses employee/student content for a purpose specified in subsection (b)(3):
>
> (1) shall reasonably attempt to limit its access to content that is relevant to the specified purpose;
>
> (2) shall use its access only for the specified purpose; and
>
> (3) shall not alter the content of the employee's protected personal online account unless necessary to achieve the specified purpose."

Instead of taking comfort in these limitations, the letters make them the subject of their second policy objection. They claim that once an organization uses a (b)(3) exception to require disclosure of content, it will not practically be able to limit itself to "content that is relevant to the specified purpose" and so will gain broader access than the statute intends.

As we read this objection, the letters are saying that, once provided with login information, employers and educational institutions will not be able to restrict their investigation to the relevant information but will inevitably review other data as well. But this concern is premised on the misunderstanding described above – the idea that the exceptions allow organizations to demand login information. They don't. They only allow them to request or demand access to content. The individual employee or student will provide the access, either by printing out the relevant content or by otherwise showing the content to the organization. In either case, the individual will be involved in providing the content and can limit it to that relevant to the request.

Even if the organizations somehow gain access to non-relevant content, the draft prevents them from using it. Subsection (c)(2) states that organizations can only "use" their access for the specified purpose. They cannot go on a fishing expedition and use the results for a purpose unrelated to the specific information that justified the access in the first place. In short, the Committee decided to allow access and try to limit it in the ways specified in subsections 3(c) and 4(c). The other alternative would have been to prohibit demands for access to content even when, based on specific information, employers and educational institutions had reason to believe that the employee or student was violating the law or organizational policy or posing a threat to health or property. The draft opts for allowing access in these circumstances, with some meaningful limits. Again, we believe that this is a reasonable and correct choice.

3. Meaning of educational institution

The third policy concern is that the draft defines "educational institution" to include only post-secondary schools (see subsection 2(2)). Its protections do not apply to primary or secondary school students. As a Committee, we have been aware of this issue, have discussed it in great length and have decided to limit the draft to post-secondary schools. The Committee's reasoning includes the greater responsibility that primary and secondary schools have for their students' welfare, and the fact that more state statutes currently limit their scope to post-secondary schools than do not. The Committee believes that, were the act to apply to primary and/or secondary schools, this would likely create enactibility issues.

In closing, we very much appreciate that these groups have shared their concerns and suggestions and to respond to them briefly here. We look forward to continuing our conversation and consideration of these and other issues in Stowe.

Sam Thumma, ESOPPA Drafting Committee Chair
Dennis Hirsch, ESOPPA Drafting Committee Reporter