MEMORANDUM

To: **Social Media Privacy Drafting Committee**
From: **Dennis Hirsch, Reporter**
Re: **Committee of the Whole's comments, and Reporter's suggested revisions**
Date: **November 5, 2015**

On July 15, 2015, the Committee of the Whole considered the draft Social Media Privacy Act. The full text of those proceedings can be found in the attached transcript. This memo identifies each comment made during the proceedings and my proposed response to it. The comments are not italicized; my responses are. For each such comment, the memo cites to the transcript page and line at which the comment can be found. Some Commissioners handed up written comments that do not appear in the transcript. I have cited such comments as "Hand." A scanned version of these written comments is attached. I welcome your input on how best to address the Committee of the Whole's comments and suggestions.

Section 1: Short Title

10, 15 Support for proposed new title. *Revised draft uses the new title. Comment incorporated. If there is Committee consensus for the new title, the issue will be raised with Scope and the Executive Committee, which would decide whether to authorize a new title.*

Section 2: Definitions

13, 14 Should expand definition of "educational institution" to make clear that covers both public and private. *Comment incorporated.*

14, 1
15, 10 Should include educational institutions down to the elementary school level. *The Drafting Committee's discussions to date have centered around the proposition that elementary and middle schools have a greater need to supervise student online activity. Current draft expands educational institution to include secondary schools, but stops there. Comment incorporated, in part.*

14, 12 Consider carve-out for home schools. *Comment incorporated.*

15, 15 Define "recognized occupation." *This the same language that some state statutes use (e.g. Oregon). Although not a mathematical formula, the term seems sufficiently clear and provides sufficient flexibility with deference to local law and case law development. Comment considered. No change.*

Hand Does "metadata" mean the same thing as "catalogue of electronic communications" in the Fiduciary Access Act? If so, the two terms should be aligned. *Metadata is a broader term. It could refer to data that provides information about data other than electronic communications. Comment considered. No change.*

16, 23 Are smart phones "computers" for the purposes of the definition of "online"? Do we need to define "computer" to make sure that they are included within the statutory scope? *Smart phones are included in the concept and, as reflected in dictionary definitions of "computer," are generally understood to be included in the term. The ULC's Fiduciary Access to Digital Assets Act does not define "computer." No need identified to provide further specificity in the statutory definitions section. Comment considered. No change.*

17, 11 Statute should define, not only "employer" and "employee," but also "employment." *This seems unnecessary and we may create a definitional issue that we do not foresee. Comment considered. No change.*

17, 22 Definition of "employer" is too broad because it does not contain the normal limiting factor of control over the employees' actions, especially given the non-waivability of the statute's protections. For example, it might cover an organization that manages volunteers and provides them with meals, or a customer who tips a waitress. *The revised draft removes the non-waivability clause. In so doing, it partially addresses this comment. It does not add the control element to the definition. Other definitions of "employer" likely add the control element for the purposes of tort law. The idea is that the employer should be held liable for the tortious acts of the employee only where the employer controls those acts. Our concern is different. It is about coercion. The relevant concern is therefore not whether the employer controls the employee's tortious actions, but rather whether the employer can coerce the disclosure of login information. There are other definitions of "employer" that leave out the control element. For example, Webster's Dictionary defines "employer" as "a person who works for another person or for a company for wages or a salary." That is quite close to the draft's definition.*

Still, the question remains as to whether the definition is so broad that it encompasses an organizer of volunteers who provides meals, or a customer who tips a waitress. There are two ways to narrow this breadth. First, A Reporter's Note could explain that "employer" means only those that provide compensation sufficient to give them coercive power over the employee. Alternatively, the draft could add to the statutory text itself the word "significant" ("significant compensation.") The Reporter requests the Committee's input as to which of these alternatives is preferable, or whether there is a third alternative that the Committee should consider. Comment incorporated, in part.

19, 18 Should the term "employer" refer only to those who are in a direct line of command with respect to the employee, or should it also refer to others in the organization who have an indirect ability to direct the employee? The Commissioner gives the example of the Dean of a faculty member's specific college, and the Deans of other colleges at the same university. *It seems that the coercive power in this example comes from the organization, the university. The university is the employer. The Dean has coercive power because she represents the university. Other deans or university employees (President, Provost, etc.) could also have coercive power to the extent that they are authorized to represent the university with respect to that employee. Thus, one way to address this comment would be to add that "employer" also includes those who represent the employer. Several state statutes (e.g. Maryland, Michigan) do this. I have revised the definition of "employer" to include such representatives. Comment incorporated, in part.*

Hand In reference to the term "employee," a Commissioner writes that "In Hawaii union dues are required by law for civil servants." *The relevance of this comment to the definition is not apparent and so I have not sought to address it. Comment considered. No change.*

Hand A Commissioner suggests that the revised statute employ the definitions of "employer" and "employee" contained in the Wage Withholding and Unemployment Insurance Procedures Act (2004). Those definitions are as follows:

> "Employee" means an individual [who is subject to, or would be subject to if not excluded by Sections 4 through 8, withholding of income tax under the laws of this state or] for whom an employer is required to make, or would be required to make if not excluded by Sections 4 through 8, at any time during the calendar year, contributions under the unemployment insurance laws of this state. The term does not include an independent contractor. (2) "Employer" means a person that pays remuneration to an individual who is the person's employee.

The Wage Withholding Act's definition of "employee" seems specifically geared to the context of wage withholding and unemployment insurance. To date, the Committee's discussion has reached more broadly to all employers who have coercive power over their employees, and not just those who withhold income tax for them. The Wage Withholding Act's definition of "employer" is very close to ours. I take some comfort in that. Comment considered. No change.

The revised draft changes the definition of "online" by removing the words "connected to" and replacing them with the words "accessed by means of." I did this in order to clarify that data on a computer hard drive is covered, even though that data is stored on, rather than "connected to," a computer. I would appreciate the Drafting Committee's feedback on this change.

25, 20 The term "protected personal online account" does not include an account that an employer or educational institution pays for. The Commissioner points out that an employer should not have access to an account that an educational institution pays for, and an educational institution should not have access to an account that an employer pays for. The exclusion would appear to allow such access, and so sweeps too broadly. *I have addressed this by clarifying that the term does not include <u>employee</u> accounts that an employer supplies or pays for, and <u>student</u> accounts that an education institution supplies of pays for. Comment incorporated.*

Hand The word "supply" in the definition of "protected personal online account" could be interpreted as providing the device (e.g. a computer) that allows an individual to access a private account such as a Gmail account. The statute should perhaps clarify this. *I do not think that courts would interpret the term in this way. There is a difference between supplying the device, and supplying the account that one accesses on that device. Do we need to clarify this in a Reporter's Note? Comment considered. No change.*

79, 5
82, 9
86, 4
Does it make sense for the definition of protected personal online account to exempt e-mail accounts that schools provide, the way that it does for accounts that employers provide, such that these accounts would not be entitled to protection? Many more students use their university accounts as personal accounts than do employees their business-provided accounts. *The Commissioner makes a valid point about how many students use their school accounts. That said, there is a benefit in a bright line rule. If the institution, be it a school or employer, provides the account, then it can access it. Such a bright line rule will provide clear notice to employees and students, and so allow them to structure their actions accordingly. There are other e-mail*

services that individuals can use of they do not like this arrangement. In addition, removing this exception would require us to try to identify, and list, those instances in which a school needs access to student online accounts that the school has provided. For example, one of the Commissioners (transcript p. 86, line 4) mentions that schools do use student e-mail accounts for university business, such as interacting with research assistants or TA's. Comment considered. No change.

Hand Does the exemption for school-provided email accounts apply to accounts that alumni or board members utilize? Should the school be able to access these? *This statute protects students and employees. Others must rely on existing constitutional, statutory or tort law. That goes for alumni or board members who maintain a relationship with a school and accept an e-mail account from it, as it would for anyone else who accepts an e-mail account from an organization (e.g. club, service organization, etc.) If the statute were to include special protection for alumni or board members it would be affording them protections that most other members of society do not have, and that go beyond the charge of our Committee. Comment considered. No change.*

28, 22 It muddies the definition of "login information" to incorporate information that provides access to a device that, in turn, gives automatic access to an account. *It is important to clarify that the term extends this far to protect accounts that remain logged in on a device. The relationship between the two pieces of the definition should not be so complicated as to be confusing. Comment considered. No change.*

29, 22 "Protected personal online account" excludes those situations in which the employer or educational institution pays for the device or the account. What about if the employee owns a mobile device, but the employer pays for the plan that provides minutes or data? *If an employer pays for the specific account (e.g. a particular app or service), then it makes sense that the employer should have access to that particular account. However, the fact that the employer pays for the minutes or data for a device should not give the employer access to all accounts that the employee accesses on the device. The same would apply to educational institutions and students. Comment considered. No change.*

31, 14 Should the statute define the term "account"? For example, where a single employee/student
35, 4 uses a home computer, would the files on that computer constitute an account? *At various junctures, the statute uses the term "online account." Given the importance of this term, and the Commissioner's confusion as to whether it would cover files on a home computer, it is important to define this term. The revised draft defines "Online account" as "a discrete set of online information concerning or established by an individual that the individual can access and control." Under this definition, it should be clear that password-protected access to a home computer would constitute an online account. The definition fits with later provisions that either prohibit or allow an employer/educational institution to access and control an employee/student's online account. Comment incorporated.*

36, 4 What about the situation where an employee/student rents a device from an employer /educational institution? How does the statute address this situation? *The employee/student would have something akin to a leasehold interest in the device. This is a kind of property interest. So, such a device would be employee/student-owned for the lease period, with the employer/educational institution having a reversionary interest. The employer/educational institution should not have access during the time that the employee/student owns the*

possessory interest. Perhaps this should be clarified in a Reporter's Note? Comment considered. No change.

37, 10 If the protections are non-waivable, then would this prevent a university from asking a student or the student's parent/guardian for their online Free Application for Federal Student Aid (or FAFSA) report? *The revised draft removes the non-waiver provision and so would allow the parent or student to waive protections, and share the FAFSA report with the university, in such a situation. Comment considered. No additional change.*

39, 3 Consider defining "device" in the way that the Colorado statute does. *The Colorado statute defines "electronic communications device" as "a device that uses electronic signals to create, transmit, and receive information, including computers, telephones, personal digital assistants, and other similar devices." I do not see the benefit in defining "device" in this way and, given the rapid pace at which technology is changing, believe such a definition could become outmoded. The statute should cover any device that allows access to a protected online account, not just "electronic communications devices." Comment considered. No change.*

39, 20 The statute should not pre-empt or undermine other statutes, such as HIPAA, that protect personal information. *This would be a state statute so it would not pre-empt a federal law such as HIPAA. It might, however, be read to pre-empt state law privacy protections. The statute could address this by including a saving clause that makes clear that it does not remove privacy protections that other state laws provide. The revised statute adds such a saving clause. Comment incorporated.*

42, 19 Are there situations in which a parent should be able to waive a student's protections under the Act? If so, would the non-waiver provision prevent this? *The revised draft removes the non-waiver provision. That should address this concern. Comment considered. No additional change.*

<u>Section 3: Applicability</u>

46, 8
53, 19 This section should have an affirmative statement as to where it applies, not just a list of exclusions from applicability. In particular, the statute should express the "behind the wall vs. in front of the wall" idea that the Reporter used to introduce the statute at the meeting of the Committee of the Whole. That would allow those who read the statute to grasp more easily its scope. *The revised draft includes a brief, affirmative statement as to the statute's applicability. It is intentionally concise and user-friendly, like the "behind the wall and in front of the wall" metaphor, as the Commissioner suggested. Comment incorporated.*

Reporter's question: Should the draft exclude the federal government as an employer? Does it have to do so? My research thus far suggests that, where the federal government has not passed pre-empting legislation of its own, state laws governing the federal government's behavior as an employer do not violate the Supremacy Clause. The existing state social media privacy statutes do not exempt the federal government. The Reporter would appreciate the Drafting Committee's input on this point.

47, 12
50, 16 The exceptions for child care and home health care providers may be underinclusive. There may be other employers that hire people to care for vulnerable individuals. These employers, too,

53, 4 may need access to the online accounts of their employees in order properly to protect these vulnerable individuals. Consider turning the exclusion into a general one for employers in this situation. *The specific references to child care providers and home health care providers are useful in that they make clear the types of situations that the Committee intends this exception to cover. The revised draft addresses the Commissioners' concerns by including, as well, a more general exclusion that encompasses other situations in which employers may need access to employees' online accounts in order to protect vulnerable third parties. Query to the Drafting Committee: does the exclusion now sweep too broadly? Comment incorporated.*

Hand A Commissioner asked whether child care and home health care employers must be licensed by the state in order to come within this exception. *It makes sense to narrow the exception in this way. Unlicensed child and home health care providers are not subject to the same accountability and oversight and so should not be given the power to access their employees' protected personal accounts. Comment incorporated.*

50, 23 The statute contains general exclusions in Section 3, and then specific exceptions for employers in Section 4, and educational institutions in Section 5. The Committee should consider the relationship among these various exceptions. *The broad exclusions in Section 3 are different than the exceptions in Sections 4 and 5. The latter do not exclude entire groups of employers or educational institutions but rather create context-specific exceptions for employers or educational institutions to whom the statute would otherwise apply. It therefore makes sense to state the broad exclusions separately in Section 3, and then to follow them with more context-specific exceptions in Sections 4 and 5. Comment considered. No change.*

Hand Some universities have their own law enforcement agencies. Would those law enforcement agencies be excluded? Or would these personnel be protected? *To this question I might add the additional issue of private security companies that provide security at particular locations or events. The reason for the exception granted to law enforcement agencies is that such they need to monitor their officers' social media and accounts in order to determine whether they have connections to gangs or other criminals. This concern would seem to be less acute in the university context. We should err on the side of keeping the exception narrow. I favor a bright line rule that exempts only federal, state, country or local law enforcement agencies. Private security companies, and those who provide university security, do not have as great a need for, and would not be entitled to, the exception. Comment considered. No change.*

Hand Alaska and Louisiana do not have counties. The ULC generally brackets "county." *Comment incorporated.*

51, 15 The Army and Air National Guard occupy a place between federal and state government. They are arms of the state government until mobilized onto active duty, at which point they become part of the Army or Navy, as the case may be, and so federal employees. The statute should clarify their status for its purposes. If the state national guard has a large number of federal employees, should it qualify as a federal agency? In addition, each National Guard has a number of federal military and civilian employees, and state military and civilian employees. How are each treated for the purposes of the statute? *Military personnel are state employees until such time as they are called up for federal duty, at which point they become federal employees. If the statute continues to exempt the federal government, then the National Guard would be exempt, and could require the disclosure of login information, at such time as the personnel in question*

are called up for federal duty. It would be better to handle this is a Reporter's Note than in the text of the statute itself. Comment considered. No change.

52, 16 What is meant by the "federal government." Does that include federal agencies like the TVA? *Generally the term "federal government" does include federal agencies. Moreover, both case law and statutes treat the TVA as a federal agency, see* Ashwander v. TVA, 297 U.S. 288, 315, 56 S. Ct. 466, 80 L. Ed. 688 (1936) (referring to TVA as "an agency of the Federal Government"); Civil Service Reform Act; Federal Employees Compensation Act.

52, 22 Does the exclusion for federal and state departments of correction include private corrections facilities that perform the same functions as federal and/or state corrections departments? *The purpose of this exclusion is to allow corrections departments to ascertain whether their employees have connections to gangs or other criminals or criminal groups. Private corrections facilities have the same need for this information. The revised draft expressly includes these facilities. Comment incorporated.*

54, 16 What about other federal contractors? Does the fact that the federal government contracts with these private entities remove them from the reach of the statute. *If the draft eliminates the exception for the federal government, that will resolve this issue. If it retains this exemption, then the Reporter proposes that federal contractors not benefit from this exemption. Many companies receive federal contracts. To exempt all or many of them would create major gaps in coverage. Comment considered. No change.*

Section 4: Employee Protections

20, 20 A Commissioner indirectly suggests that the scope of the employee protections is too broad in that it covers any request for login information, not just coercive requests. *One way to address this would be to remove the words "require" and "request" from Section 4(a)(1) and simply say that an employer may not "coerce" an employee to reveal her login information. However, the Drafting Committee's intent, as I understand it, has been to protect against simple requests on the grounds that they are inherently coercive. Removing the word "request" might accordingly open up a gap in the statute's protections. The Commissioner's objection seems to be that some requests may not be coercive. Another way to address this is to add the word "otherwise." Employers may not "require, request or* otherwise *coerce." This would allow an employer to argue that the particular request, in its particular context, was not coercive and so not covered by the statute. In so doing, it would address the Commissioner's concerns without opening up an unintended loophole. Comment incorporated, in part.*

Hand A Commissioner suggested replacing the phrase "An employer may not require, request or coerce" with "An employer may request, but shall not require or coerce . . ." *The Drafting Committee's view, as I have understood it, is that employer requests are inherently coercive. Comment considered. No change.*

59, 13 The statute allows employers to coerce the disclosure of login information when investigating
67, 2 violations of employer policies of record of which the employee had notice. This could lead to a
67, 14 loophole in which employers institute broad policies that, when allegedly violated, give them the right to "investigate" and so to gain access to employee online accounts. *Our committee has placed great emphasis on the investigative exception. It helps to establish a balance between*

the employee's privacy and the employer's bona fide need for account information to protect against violations of the law or its own policies. I do not think we want to remove or unduly narrow this exception. I have added that the employer's policy must be "bona fide." In a Reporter's Note, we can clarify that this means it must have a substantial purpose beyond that of providing access to protected employee online accounts when violated. This should allow courts to sort bona fide employer policies from those intended primarily to create a loophole that allows employer access to employee online accounts. I have made the same change in Section 5 on Student Protections. Comment incorporated.

60, 5 A Commissioner points out the oddity of providing that employers "may possess" protected employee account information when they receive it from a third party, when the whole point of the statute is to prevent employers from gaining access to that information. Is there another way to deal with the situation where a third party gives the information to the employer? Couldn't the statute instead say that such possession is not a violation of the act? *The revised statute adopts the suggested approach. Comment incorporated.*

Hand A Commissioner asked whether § 4(a)(3), which prohibits employers from taking adverse action against an employee based on protected information that it inadvertently received, means that the employer could not sue that employee for slander or libel. *I suppose that it does. Such a lawsuit would likely constitute an adverse action. If the Drafting Committee wanted to permit such defamation or libel actions, it could clarify that only adverse employment actions are prohibited. This seems to make sense. The thing we are protecting against is the employer's coercive power qua employer. When an employer sues for defamation or libel it is acting like any other litigant. Same goes for an educational institution. I have added the qualifying term. Comment incorporated.*

61, 24 Sometimes, an employee will have access to another employee's protected personal online account. For example, an assistant may have access to his boss's LinkedIn or Facebook account where the account is being used for some business purposes. This could allow an end-run in which the employer asks the assistant for his boss's login information. Can the statute protect against this? *The statute already addresses this. It prevents an employer from coercing an employee into giving access to "a" protected account, not just "the employee's protected account." In order to make this approach entirely consistent, I have changed "the employee's list of contacts" at 4(a)(1)(C) to read "the list of contacts" associated with the account. I have made the same change in Section 5 on Student Protections. Comment incorporated.*

64, 8
84, 5 One Commissioner stated that, in his view, an employer should be able to ask an employee for access to her protected online accounts, regardless of whether the employer was investigating that employee for a particular violation, and should be able to fire the employee if she fails to turn over the login information. The Commissioner stated that, unless the statute is changed to allow such requests, it will run into employer and school administrator opposition that could prevent state enactments of the draft. *This comment calls into question the very premises of the statute and, arguably, the Drafting Committee's charge as approved by Scope and the Executive Committee. Undoubtedly there are different views on statutes already enacted regarding social media privacy. That said, many states have enacted such provisions and many such enactments were passed without any votes against. For example, in Tennessee, the Senate passed the Employee Online Privacy Protection Act by a vote of 32-0 in the Senate, and 96-0 in the House. See https://legiscan.com/TN/bill/SB1808/2013 . The Governor signed it into law. The*

Tennessee Act, much like the act that our Committee has drafted, prevents employers from "Request[ing] or require[ing] an employee or an applicant to disclose a password that allows access to the employee's or applicant's personal Internet account." Many other states have already passed such legislation. It appears that state legislatures will, in fact, enact bills such as the one we have been asked to draft. Comment considered. No change.

68, 2 A Commissioner asserted that the Supreme Court, in City of Ontario v. Quon, 560 U.S. 746 (2010), had held that a supervisor's statements may create a greater expectation of privacy than do written employer policies, and so our requirement that the employer policy be in writing could inadvertently end up limiting employee privacy rather than protecting it. *This comment speaks to employer policies regarding employee privacy rights. By contrast, the statute addresses employer policies that, if violated by the employee, could give the employer reason to investigate that employee. If supervisor statements weakened employer policies of the second type this would decrease the employers' ability to use the investigation exception, not increase it. So it would not give rise to the concern that the Commissioner raises. There is an important reason for requiring that the employer policy, which is to be the basis of the investigation exception, be in writing or otherwise in a record. This ensures that employees have notice of such a policy. Thus, the current language serves an important purpose. In addition, the draft statute already adds that the employee must "have reasonable notice" of the policy. This should give an employee the ability to argue, in the situation where verbal policies are more privacy protective than written ones, that the supervisor's statements contradicting the written policy confused matters and so did not provide reasonable notice. Finally, upon reading the case, it seems clear that the Quon Court expressly decided not to reach the question of whether a supervisor's statements can override employer written policies. So it does not clearly establish the principle that the Commissioner attributed to it. Comment considered. No change.*

69, 18 The exception for employer compliance with federal, state or local law, or the rules of a self-regulatory organization under the Securities and Exchange Act, should be extended to include bona fide self-regulatory organizations in other sectors that need regularly to screen employees, such as the gaming industry. *In the draft considered by the COTW, the only self-regulatory organizations whose rules can form the basis for an exception are those organized under the Securities and Exchange Act. Including too broad an exception for the rules of other self-regulatory organizations could open up a loophole. Industry sectors could establish a self-regulatory organization for the purpose of establishing policies that justify intrusions into protected employee online accounts. The self-regulatory organizations in the securities industry are different in that Congress authorized them by statute. I have added language to include the rules of other self-regulatory organizations, established by statute, that have a legal duty to inspect protected employee online accounts. I have added similar language to the Student Protection sections. Comment incorporated.*

Hand Would the statute allow heavily regulated employers (such as banks and healthcare companies) to monitor employee compliance with privacy regulations. *The exception for employer actions needed to "comply with federal, state or local law" should cover this. Comment considered. No change.*

70, 21 Can an employer require that an employee include it on an emergency contact list on the employee's personal account? Or would that violate the prohibition on employers requesting that they be added to an employee's list of contacts (Section 4(a)(1)(C))? *Such an employer*

request would appear to violate this section of the draft statute. Since we are removing the non-waiver provision, an employee would be able to include the employer of its own volition, though the employer could not request such inclusion. In those situations where health or safety truly were at stake, the exception for employer/educational institutions intended to protect health and safety would cover a request to be added to an emergency contact list. That reduces the problem. Perhaps a Reporter's Note could clarify this. Comment considered. No action.

Hand The requirement that an employer "dispose of" login, content and metadata information that it inadvertently received, is ambiguous. What does it mean to "dispose of" it? Is it sufficient to delete it? Must it be over-written? *The statute should stay as technology-neutral as possible. The technology that constitutes effective disposal today (e.g. over-writing) may not in five years. Moreover, it is often difficult to truly eliminate information to the point that someone able to invest tremendous resources in the task could not retrieve it. I have tried to clarify the requirement by adding that the employer/educational institution must dispose of the information "in such a way as to make it infeasible for the employer to retrieve it."*

Hand The provision allowing for maintenance and monitoring of an employer's information communications technology system where this can be done without requiring login information or otherwise violating the core prohibitions, does not provide enough latitude. Consider reversing the language and stating that an employer is exempt from the prohibitions in 4(a) where necessary to maintain or monitor its systems. *In my experience, such maintenance and monitoring generally involve observation of the system as a whole, not an individual's account. In addition, the statute allows an employer/educational institution to access devices or accounts that it pays for or supplies. It also allows access where the employer/educational institution reasonably believes that the employee/student has violated a policy, including policies intended to protect the integrity of information and communications technology systems. The draft provides sufficient opportunities for employers/educational institutions to obtain login information in order to maintain and monitor their systems. I think that allowing a claim of maintenance or monitoring (broad terms) to trump the core protections creates a risk of abuse. Comment considered. No change.*

<u>Section 5: Student Protections</u>

76, 22 There is a lot of duplication between Sections 4 (Employee Protections) and 5 (Student Protections). Why can't these two sections be combined into one, shorter section? *There are two reasons that we have done it this way. First, a combined approach leads to very cumbersome and, to some extent, confusing language. Second, we want states to be able to adopt one set of protections, or the other, or both. This is made easier by setting out the two different types of protections (employee, and student) in two different sections. Comment considered. No change.*

81, 10 The reference to the student's online account in Section 5(c) should include the words "protected, personal." *Correction made. Comment incorporated.*

Hand A Commissioner asked whether the draft addressed the situation of a student who was engaged in work-study and so was both a student and an employee. *Such an individual would be both a student and an employee, and so would benefit from both sets of protections. The protections*

are substantially similar. I do not see a need to address this in the text of the statute itself. Comment considered. No change.

Section 6: No Waiver

88, 2
91, 9
94, 10

A Commissioner voiced a philosophical objection to the No Waiver provision. Privacy is often defined as control over one's personal information. By preventing waiver, we remove the ability to exercise control. The Commissioner recommends that, if coercion is what we are worried about, then the statute should in the earlier provisions specify that consent must be informed and voluntary. It should not prohibit consent. The Commissioner gave examples of situations where students might, justifiably, want to share the content of their online accounts with the school. For example, a student might want to show the teacher the contents of his social networking account to prove that he did not use social networking to cheat with others on a paper or exam. Several other commissioners stated their support for this concern. One portrayed it as a free speech issue. By preventing people from sharing the contents of their online accounts, we are impinging on their free speech rights. *The Committee of the Whole did not seem comfortable with the No Waiver provision, which is a novel provision. The draft included the provision with the thought it would help to prevent the unraveling of the statute's protections as employees and students compete with one another in a race to the bottom. The Drafting Committee should probably yield here to the strongly expressed views of the Committee of the Whole. The revised draft removes the non-waiver provision. In addition, it provides in Section 4 that "An employee may, of the employee's own initiative, give informed, voluntary consent to having others, including the employer, access or control the employee's protected personal online account." It makes a similar addition with respect to students in Section 5. Comment incorporated.*

Removing the non-waiver provision raises a question about the prohibition on employers and educational institutions "requesting" employee or student logins. If the employee or student can consent, why cannot the employer or school request? I think that there is a reason to continue to prohibit requests. If an employee/student wants, of his or her own accord, to give the employer/school access to a protected account, then the employee/student can now do so. That is what removal of the non-waiver provision means. But it is a different thing to allow the institutions to request the login information. The Drafting Committee has, in past meetings, expressed its feeling that a request from an employer or school is, in many cases, inherently coercive. I have therefore left the prohibition on requests in the statute.

91, 17

As mentioned above, a Commissioner suggested that, were we to remove the non-waiver provision, we could bolster true consent by providing that such consent must be free and voluntary. *In response to this comment, and for the Drafting Committee's review, I have tentatively added language to Sections 4 and 5 stating that "An employee/student may, of the employee's/student's own initiative, give informed, voluntary consent to having others, including the employer/educational institution, access or control the employee's protected personal online account." I am interested in the Drafting Committee's thoughts on this addition. Comment incorporated.*

Section 7: Civil Action

96, 3
98, 13 A Commissioner suggested deleting subsection (a) which authorizes a public authority to bring a civil action against an employer/educational institution to enforce the statute, and relying solely on private actions for enforcement. Another Commissioner stated that the statute should define public authority. Chair Thumma explained that the purpose of this subsection was to allow public authorities such as the attorney general to bring such an action. A Commissioner suggested referring to the "state Attorney General," in that case. The revised draft includes this language. *Comment incorporated.*

99, 4 Consider adding language that allows a parent or guardian to bring the suit on behalf of a minor child. *The parent or guardian are included in the definition of "student." There is no need to make specific reference to them in the Civil Action section. Comment considered. No change.*