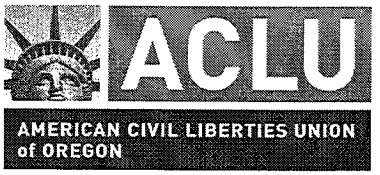

Testimony of Becky Straus, Legislative Director
In Support of SB 344A
House Committee on Business and Labor
May 22, 2013

Chair Doherty and Members of the Committee:

SB 344A would prohibit institutions of higher education from compelling access to students' personal social media accounts. Thank you for the opportunity to testify in support of the bill.

This committee held a public hearing on this concept as HB 2654 on February 20, after which it was determined that HB 2654 would move forward to address only social media privacy in the employment context and this bill, SB 344, would be the vehicle for social media privacy in the higher education context. The Senate passed SB 344A by a vote of 28-0-2.

SB 344A has been negotiated to address concerns from representatives of the Oregon University System and includes provisions to clarify that nothing in the bill would prevent institutions from investigating specific instances of student misconduct, utilizing cyber-security software, or accessing otherwise public information about students. The ACLU and OUS did not reach agreement on our desire to include a prohibition against teachers or coaches requiring that a student add them to their list of social media contacts, a practice referred to as "coercive friending," but all parties have agreed to take up that issue at a later date. We are otherwise pleased with the product of these negotiations and we ask for your support.

Social media passwords vulnerable to privacy violation

A growing number of schools nationwide are demanding that applicants and students hand over the passwords to their private social networking accounts such as Facebook. Such demands constitute an invasion of privacy. Private activities that would never be intruded upon offline should not receive less privacy protection simply because they take place online. Of course a school official would not be permitted to read an applicant's or student's diary or postal mail, listen in on the chatter at private gatherings with friends, or look at that person's private videos and photo albums. We do not believe that they should expect the right to do the electronic equivalent.

In states across the country, examples of this abuse are surfacing. We commend the proponents for their foresight to put in place the necessary legal protections before we hear of a great number of instances in Oregon.

Examples in Schools in Other States

- Schools around the country are requiring student-athletes to "friend" a coach or compliance officer, giving that person access to their "friends-only" social media posts – or they are outsourcing the task to automated social media monitoring companies like

UDiligence and Varsity Monitor, companies that offer a "reputation scoreboard" to coaches and send schools "threat level" warnings about individual athletes.[1]

- The ACLU of Minnesota represented a Minnesota public school student forced to turn over login information for her Facebook and email accounts because of allegations that she had online conversations about sex with another student off-campus.[2]

Implications for third parties and legal liability

Once a person shares his or her social media or other electronic account passwords, that person can be subject to screening not just at that time but on an ongoing basis. Some companies even sell software that performs such continual screening automatically, alerting employers, coaches, or others to any behavior or speech they might find objectionable.[3]

Further, when a person is forced to share the password to a private account, not only that person's privacy has been violated, but also the privacy of friends, family, clients, and anyone else with whom he or she may have communicated or shared files.

In fact, these types of practices also violate Facebook's own policies. Facebook's Statement of Rights and Responsibilities states under the "Registration and Account Security" section that Facebook users must make ten commitments to the company relating to the registration and maintenance of the security of the account. The Eighth Commitment states, "You will not share your password, (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account."[4] Thus, sharing one's password or access to one's account with potential or current employers violates these terms of agreement.

Finally, sharing a social network password may also expose a lot of information about an applicant – such as age, religion, ethnicity, pregnancy. When not disclosed by the applicant voluntarily, the concern is that the information can unknowingly expose an applicant to unlawful discrimination.

Thank you for the opportunity to provide testimony and for your consideration. We urge you to move the bill to the House floor. Please be in touch at any time with comments or questions. Thank you.

---

[1] Sullivan, Bob. "Govt. agencies, colleges demand applicants' Facebook passwords." *NBC News*. 6 March 2012. http://redtape.nbcnews.com/_news/2012/03/06/10585353-govt-agencies-colleges-demand-applicants-facebook-passwords

[2] ACLU-MN files lawsuit against Minnewaska Area Schools. 6 March 2012. http://www.aclu-mn.org/news/2012/03/06/aclu-mn-files-lawsuit-against-minnewaska-area-schools (Legal complaint: http://www.aclu-mn.org/files/6213/3107/2399/R_S___S_S__v__Minnewaska_School_District_Complaint.pdf)

[3] One example: Data Facts (http://www.datafacts.com/background-screening/new-products-whats-hot/social-media-screening)

[4] https://www.facebook.com/terms#!/legal/terms