Testimony of Becky Straus, Legislative Director
In Support of SB 344 with Dash 1 Amendment
Senate General Government, Consumer and Small Business Protection
February 13, 2013

Chair Shields and Members of the Committee:

SB 344 would prohibit employers from compelling access to employees' personal social media accounts and, with amendments, would prohibit institutions of higher education from doing the same of their students. Thank you for the opportunity to testify in support of the bill. I plan to describe briefly the problem addressed by SB 344 and explain the proposed solution, including the details of the Dash 1 amendment. We urge you to adopt the Dash 1 amendment and send the bill on to the House floor for a vote.

Social media passwords vulnerable to privacy violation

A growing number of employers and schools are demanding that job applicants, employees 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 an employer or 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. They should not expect the right to do the electronic equivalent.

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

Employment

- Robert Collins of Maryland was required to provide his Facebook login to his employer, the Maryland Division of Corrections, as part of a reinstatement interview after a leave of absence.[1]
- Justin Bassett, a statistician from New York, was asked for his Facebook password during a job interview. (He withdrew his application saying he didn't want to work for an organization that would seek such personal information.)[2]
- The Norman, Oklahoma Police Department asks applicants to turn over their Facebook passwords as part of background checks.[3]

---

[1] Curtis, Meredith. "Want a Job? Password, Please!" *ACLU Blog of Rights*. 18 February 2011. http://www.aclu.org/blog/technology-and-liberty/want-job-password-please

[2] Valdes, Manuel. "Job seekers getting asked for Facebook passwords." *AP*. 20 March 2012. http://finance.yahoo.com/news/job-seekers-getting-asked-facebook-080920368.html

- Until 2011, when there was public outcry, the city of Bozeman, Montana instructed all job applicants to provide passwords for all social media accounts.[4]
- As of January 1, 2012, anyone seeking to become a Virginia state trooper is required to reveal the contents of all of his/her social media accounts as part of the interview process.[5]
- A North Carolina police department asks job applicants for social media user names and passwords as part of its application for clerical positions.[6]

Schools

- 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.[7]
- 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.[8]

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.[9]

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.

---

[3] Charette, Robert. "Should you have to turn over your Facebook password to get a job?" *IEEE Spectrum*. 24 February 2011. http://spectrum.ieee.org/riskfactor/computing/it/should-you-have-to-turn-over-your-facebook-password-to-get-a-job

[4] Gouras, Matt. "City drops request for internet passwords." *AP*. 19 June 2009. http://www.msnbc.msn.com/id/31446037/ns/technology_and_science-security/t/city-drops-request-internet-passwords/#

[5] Bowes, Mark. "Sharing Facebook profile part of Va. Trooper application." *Richmond Times-Dispatch*. 22 March 2012. http://www2.timesdispatch.com/news/news/2012/mar/22/tdmain01-trooper-applicants-must-share-websites-ar-1784527/#fbcomments

[6] Wehner, Mike. "Could employers begin asking for Facebook passwords on applications?" *Tecca*. 30 November 2011. http://www.tecca.com/news/2011/11/30/facebook-password-jobs

[7] 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

[8] 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)

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

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."[10] 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 a job applicant – such as age, religion, ethnicity, pregnancy – about which an employer is forbidden to ask. That information can expose an applicant to unlawful discrimination. Learning such information may also expose an employer to lawsuits from rejected job candidates claiming such discrimination.

SB 344 with the Dash 1 Amendment

SB 344 takes a reasoned approach to this issue, applying offline privacy principles to an online medium while respecting the rights of employers and schools to access information that is public.

The Dash 1 amendment provides more detail and clarification than the bill as introduced in order to close any loopholes that the original language may have exposed. SB 344, as introduced, does not include a section to address compelled access to electronic accounts in the context of higher education and the Dash 1 amendment adds provisions to cover this area.[11] If the Committee choses to adopt the Dash 1 amendment, SB 344-1 will then be identical to HB 2654 and SB 499.

Section 1: Incorporates Section 2 into ORS 659A.

Section 2: Makes it an unlawful employment practice for an employer to:

- Ask an employee/applicant for his/her username or password to his/her social media account,
- Compel an employee/applicant to add the employer to his/her contacts on social media,
- Penalize an employee for refusing to disclose account info or add employer to contacts,
- Refuse to hire an applicant because he/she refused to disclose account info or add employer to contacts.

Clarifies that the protections do not apply to non-personal accounts that provide access to employment-related information systems.
Defines "social media."

Section 3: Prohibits public and private community colleges and public universities from:

- Ask a student/applicant for his/her username or password to his/her social media account,
- Compel a student/applicant to add a school-related official to his/her contacts on social media,

[10] https://www.facebook.com/terms#!/legal/terms
[11] Should the Committee decide not exclude higher education from this bill, the Dash 2 amendment is written to fix the drafting in the employment context but not add higher education sections.

- Penalize a student/applicant for refusing to disclose account info or add school to contacts,
- Refuse to admit an applicant for refusal to disclose account info or add school to contacts.

Defines "educational institution" and "social media."

Section 4: Private cause of action for violation by schools. Attorney fees available to prevailing plaintiff; attorney fees and expert witness fees available to prevailing defendant if plaintiff had no objectively reasonable basis for asserting a claim or appealing an adverse decision of a trial court.

Oregon Should Join List of States Enacting Protections

To date, legislatures in Maryland, Illinois, Michigan and California have passed laws prohibiting employers from compelling access to social media accounts and legislatures in Delaware, Michigan, New Jersey and California have done so in the education context. Legislation is pending in at least 25 states to address these issues in the 2013 session.[12]

We urge you to adopt the Dash 1 amendment and move SB 344 to the House floor. Thank you for the opportunity to provide testimony. Please be in touch at any time with comments or questions.

[12] http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx