Glenn Grothman
STATE SENATOR
20TH SENATE DISTRICT

Office:
Post Office Box 7882 • Madison, Wisconsin 53707-7882
(608) 266-7513 • Toll-Free: (800) 662-1227
Sen.Grothman@legis.wisconsin.gov
www.legis.wisconsin.gov/senate/sen20/sen20.html

Home:
111 South 6th Avenue
West Bend, Wisconsin 53095
(262) 338-8061

August 20, 2013

To: Members of the Senate Committee on Judiciary and Labor
From: Senator Glenn Grothman
Re: Senate Bill 223

Senate Bill 223 is legislation to prohibit an employer, educational institution, or landlord from accessing or observing the personal internet accounts of employees, students, or tenants.

Under current law, these groups can require individuals to provide their log-in information including passwords and usernames in order to access their personal social media and online accounts that were designed for the sole purpose of personal communication: a clear violation of privacy rights. This legislation would update our current laws to meet the growing issues that arise as a result of rapidly expanding access to digital technology, and it would protect individual rights and prevent an act of reprimand towards those who refuse to surrender their personal account information.

Numerous states have proposed or enacted similar legislation in recent years to prevent this encroachment of privacy in response to various nationwide instances in which this problem has occurred. In this bill, employers are still granted the right to obtain personal information as long as it has already been shared publicly by the individual. Likewise, in a scenario that a legal issue would present itself, an employer or educational institution can require access to information if the mode of communication belongs to the employer or the educational institution or specifically violates rules laid out by an employer.

It is clear that both the rights of the students, employees, and tenants have been properly balanced with those of an employer, landlord, or educational institution in this bill. It is essential that we pass this bill to secure our citizens' privacy, please support this legislation to assure that our citizens' rights are protected.

WISCONSIN STATE ASSEMBLY

STATE REPRESENTATIVE
MELISSA SARGENT
48th DISTRICT

August 20, 2013

Rep. Melissa Sargent's Testimony Regarding Senate Bill 223

Thank you Mr. Chairman and committee members for allowing me to testify before you today.

SB 223 or 'the social media protection bill' is a bill that reflects the changing world we live in.

Increasing numbers of Americans use social media both on and off the job.

Across the country some employers have asked employees to turn over their usernames and passwords for their personal accounts. This same scenario has occurred on college campuses with athletic teams requiring students to turn over the passwords so that their accounts could be monitored.

Requiring access to personal, social media accounts is an invasion of privacy, yet as the bill states 'current law does not regulate employer access to, or observation of, the personal Internet accounts of employees and applicants for employment'.

I believe there must be a reasonable expectation of privacy for our social media accounts which are personal in nature.

Because it is still a relatively new communication source, social media websites and their use is largely unregulated by state or federal law. However, many states have already taken proactive steps to fix this. 14 states have passed laws similar to SB 223, and legislation pending in 36 states.

Every state in the country has realized the need for a bill such as this and has acted accordingly.

Social media legislation in other states has not known party lines. It has been passed in Republican leaning states like Utah and Arkansas, and Democratic states like Illinois.

The bill is fairly straight forward: SB 223 makes it illegal to require an employee, job applicant, student, prospective student, tenant or prospective tenant to turn over their username and password to any social media website. That's it. In the LRB's analysis there is an extensive list of what employers, universities, and landlords are still allowed to do.

- They can still monitor what is done on a company owned computer.
- They can still restrict what websites are visited on a company owned computer.

State Capitol: P.O. Box 8953, Madison, WI 53708
(608) 266-0960 ☆ E-mail: rep.sargent@legis.wi.gov ☆ Website: http://sargent.assembly.wi.gov

- They can monitor anything done publicly on a Facebook or Twitter page.
- They can conduct an investigation or require an employee to cooperate in an investigation of any alleged unauthorized transfer of confidential information via social media.

The list of allowed activity goes on and on in the bill draft.

This bill protects an individual's privacy while still giving employers the flexibility they need to run their business. It also gives employers and universities the clarity they need when deciding on a cohesive social media policy. They will now know explicitly what they are allowed to do and what they are not allowed to do under the law.

I believe that this bill is a good example of how we can work with one another in a bi-partisan manner. I reached out to Representative Bies after I read about Illinois and Michigan passing social media protection laws. He was interested in the concept and we have been able to forge a group of Democrats and Republicans to sign on as co-sponsors of this simple yet very necessary legislation.

Republicans and Democrats alike have shown support for this bill for various reasons. I have worked hard to gather a broad consensus by reaching out to consumer advocates, students, and employees as well as members of the business community. I believe that through this work, AB 218 respects the privacy rights of social media users with the needs of Wisconsin businesses.

WMC, an unlikely ally for me, has sent around a memo to our colleagues in the legislature stating "the authors (of AB 218) have made a serious attempt to balance privacy concerns related to social media with the needs of employers."

We, as legislators, must keep up with the pace of technology. As times evolve, so must our laws.

It was not until the early 1900's that it was made illegal to open someone else's mail, or snail mail as we call it today.

It was not until 1986 that it was made illegal to look at another individual's email.

AB 218 is another step in a progression to protect an individual's privacy when a new means of breaching that privacy becomes available.

I'd also like to quickly point out, that along with Representative Bies, we have introduced a substitute amendment to the Assembly version of this bill. This sub takes into account the various interests who have weighed in on the bill.

Attached to my testimony you will see the provisions that have changed. For the most part they are technical in nature and clarify some aspects that were not explicit in the first draft of the bill.

Thank you again Mr. Chairman.

Substitute Amendment to AB 218

Within the substitute amendment are provisions that address technical changes and clarifications as to the bill's intent. The following are the substantive changes in language:

1. **Definition of "personal Internet account":** Clarifies the definition of a 'Personal Internet Account' to "an Internet-based account that is created and used by an individual exclusively for purposes of personal communications". (Section 5 (d)). This change was made after looking at other states definitions regarding these accounts. This new definition is more concise and less ambiguous than the previous definition.
2. **Restrictions on employer access:** The substitute amendment retains the prohibitions on granting access and allowing observation. Adds in language that an employer may not request **or require** an employee or applicant to disclose access information. (Section 5 (2)). Also adds one sentence that states an employer may not "refuse to hire an applicant for employment because the applicant refused to disclose access information, for, grant access too, or allow observation of the applicant's personal Internet account." These changes to the bills prohibitions strengthen the bill and make it more consistent with social media privacy bills in other states.
3. **Clarification on employer owned devices:** Adds '**supplied** for by employer' to the language (section 5, line 22). This change would cover any electronic communications device supplied by the employer (in addition to subsidized device programs, as originally included in the bill).
4. **Conducting an Investigation:** Change in language stating that in conducting an investigation an employer can require an employee to grant access to or allow observation of the account, but cannot require disclosure of access information for the account.
5. **Employer Monitoring:** Notes that if through monitoring of an employer owned computer or device (allowed under the bill), an employer inadvertently receives an employee's username and password, the employer is not liable for having this information, but may not use this information to access an employee's personal online account. (Section 5, (7) (d))This change came from a coalition of employers and civil liberties advocates in other states, such as Washington and Oregon, who have passed similar language.
6. **State and Federal Law Addition:** Per the request of the Life Insurers, a clarifying change has been added that an employer is not prohibited from "complying with a duty to screen applicants for employment prior to hiring or duty to monitor or retain employee communications that is established under **state or federal laws, rules, or regulations or the rules of a self-regulatory organization.** (Section 5, (7) (c))
7. **Employee rule / handbook provision:** At the request of the business community, we have added a section that employers have the right to observe social media accounts as the result of a 'violation of an employer's rule as specified in an employee handbook'.

STATE REPRESENTATIVE
Garey Bies
1ST ASSEMBLY DISTRICT

Testimony of Representative Garey Bies
Senate Committee on Judiciary and Labor
Senate Bill 223 –Access to Social Media Accounts

Chairman Grothman, committee members. Thank you for the opportunity to submit testimony on Senate Bill 223 relating to access to an individual's social media accounts.

Everyday someone new registers a social media account. Earlier this year, Facebook had over 1 billion users. Twitter has over 500 million registered users and LinkedIn has over 225 users. And this is just a quick sampling of what we consider the more popular social media sites.

As more and more people rely on these sites as a means to connect with family, friends, and business associates, we need our current privacy laws to reflect the trends of today's modern society. Throughout the country we hear incidents of employers and educational institutions asking applicants and students to give their usernames and passwords to personal social media accounts. This is a clear violation of an individuals' right to privacy and the privacy of those they're "friends" with on these sites. If an employer/school/landlord has the ability to see an applicant's site, they also gain access to the private sites of individuals who haven't consented.

Six states have enacted legislation and more than 50 bills are pending in 28 states. This is clearly an issue states understand needs to be addressed to protect the rights of both parties involved.

We were careful to make certain exceptions in this bill to protect the rights of employers/schools/landlords because we understand there are situations that could open them up for liability. For instance, they are permitted to block access to certain sites and they can access and monitor data that is stored on an electronic device paid for in whole or part by the employer.

I'd like to add that I'm thankful to members of different industries within the business community that came to us with sensible and reasonable recommendations for changes. Following the public hearing in the Assembly, we had a substitute amendment drafted to further address some minor issues that were brought to our attention. The bill before you today is a stronger bill, which balances the rights of employees with the necessary protections for employers.

Once again thank you for the opportunity to testify on Senate Bill 223. I am happy to answer any questions you may have.

First for Wisconsin!

Capitol: P.O. 8952, Madison, WI 53708-8952 • (608) 266-5350 • Fax: (608) 282-3601
Toll-Free: (888) 482-0001 • Rep.Bies@legis.wi.gov
www.legis.state.wi.us/assembly/asm01/news/

Home: 2520 Settlement Road, Sister Bay, WI 54234 • (920) 854-2811

WISCONSIN ASSOCIATION OF SCHOOL BOARDS

122 W. Washington Avenue, Madison, WI 53703
Phone: 608-257-2622·Fax: 608-257-8386

John H. Ashley, Executive Director

TO: Members of the Senate Committee on Judiciary and Labor

FROM: Dan Rossmiller, Government Relations Director

RE: Testimony on Senate Bill 223, relating to employer access to, and observation of, the personal Internet accounts of employees and applicants for employment; educational institution access to, and observation of, the personal Internet accounts of students and prospective students; landlord access to, and observation of, the personal Internet accounts of tenants and prospective tenants; and providing a penalty

DATE: August 20, 2013

Good afternoon Senator Grothman and members of the Senate Committee on Judiciary and Labor. Thank you for this opportunity to testify on Senate Bill 223. My name is Dan Rossmiller and I am the Government Relations Director for the Wisconsin Association of School Boards.

Digital electronic technology is evolving rapidly and becoming ever more present in our private lives, our work lives and in education. As a result, it is becoming harder to define appropriate boundaries separating information that one would wish to keep truly private from information that may be accessible to others.

As you debate these issues, we have a number of concerns about where and how Senate Bill 223 draws certain of these boundaries with respect to our state's public K-12 schools, where the protection of minor children is of paramount concern.

Public schools are both "employers" and "educational institutions" under this bill.

Generally speaking, we believe Senate Bill 223 makes sense as applied to applicants for employment and students applying/enrolling to a school.

Our primary concern, and the reason for my appearance here today, is that the bill, as introduced, could hamper schools' ability to investigate certain types of **student** misconduct (such as cyberbullying) and **employee** misconduct (such as inappropriate relationships between school staff and students).

The problematic provisions in our view are found at page 7 of the bill, lines 1 through 6. These provisions would make it a violation for an educational institution to "request a student or prospective student to grant access to, allow observation of, or disclose information that allows access to or observation of the personal Internet account of the student or prospective student." Each violation by a school official could result in a $1,000 forfeiture.

Currently, the first thing school officials often do as part of their investigation—when misconduct such as cyberbullying is alleged—is to request the student's consent to view the allegedly offensive or abusive content, and such consent is often given by the victim of the behavior, and it is sometimes given by the alleged bully/aggressor.

We are concerned that a parent could, for example, come to school officials asking that they look into cyberbullying or other alleged student misconduct that is occurring at school and harming their child but that also involves personal devices and personal Internet accounts. Under the bill as currently drafted, school officials would not only be prohibited from looking at the Internet account in which the abusive or offensive material was contained, they could not even ask to see the account.

And as we read the bill, school officials, could not even request the **victim** of the cyberbullying in this example to consent to allow access to the content that constitutes the bullying if it is located on a private site because merely making such a request would be prohibited.

We see little reason to prohibit school officials from asking alleged victims for access to content from their account in order to attempt to right the wrong done to them. We believe that at a minimum, consent should be a valid basis for asking for and obtaining content—provided that the consent isn't being requested from the student who may be disciplined, suspended or expelled as a result. And even in this context, we see little reason to prohibit school officials from allowing students accused of misconduct to give consent in order to clear their name.

The WASB is not looking to give school officials blanket permission to access student's social media or email accounts or for any authority to conduct searches of personal devices or accounts that are not supported by individualized and reasonable suspicion of misconduct. Further, WASB agrees that neither employers nor schools should be permitted to require any individual to allow access to his/her private accounts so that the employer or school can go an intrusive "fishing expedition" within those accounts.

We do ask committee members to recognize that an entire body of law already exists surrounding the extent to which a public entity may seek to "search" a public school student or public employee or their personal property That body of law, which has generally served the interests of school safety well, while protecting students' and employees' privacy rights, holds that the search of a student's personal electronic device without consent or a reasonable basis for a suspected violation of law or school rules violates the student's constitutional rights.

The bill, however, appears to provide no exception for school officials to obtain consent or to obtain access to content in cases where school officials have reasonable cause to believe that a violation of school policy or law has occurred. Academic cheating, cyberbullying, coordinated school violence, and "sexting" are all instances where the prohibition in this bill could be significant. Ironically, the prohibitions in the bill could also hurt the interests of students when it comes to defending against potentially false allegations of violations of school rules.

Finally, to the extent the bill would limit the ability of schools to passively or actively monitor certain Internet-based activities that involve the use of district-owned technology resources, it could also hamper a school district's efforts to comply with federal laws surrounding Internet safety which expressly require schools to monitor such activities.

If the bill were passed in its present form, we believe it could have several unintended consequences, including that it:

- could result in school officials making significant decisions regarding student and employee conduct without access to the "best evidence" available—the information contained in the personal Internet accounts. (If so, this will increase school's reliance on circumstantial evidence and witness testimony instead of the "best evidence" available.);

- may increase the incentive for school officials to involve other agencies with broader investigative powers (such as law enforcement or social service agencies);

- could cause schools to backtrack on the extent to which they permit students to possess and use "smart phones" and other personal electronic devices while at school. (Many school districts have been trending toward policy positions that generally allow possession of such devices and that focus on teaching safe/responsible use, but those policies were adopted with the backdrop of consent-based access, the "reasonable suspicion" standard, and the possibility of school discipline based on the information that is found in connection with the school's investigation of alleged misconduct.)

In summary, while the bill sensibly attempts to curb and prevent certain abuses of personal privacy, the WASB is advocating for a more incremental and nuanced approach to regulation that:

- better differentiates among the interests of applicants, current employees, and current students;

- gives additional consideration to the unique responsibilities of public schools and school officials; and

- accounts for the developed body of law that already places relevant restrictions on public entities.

In closing, we also want to point out what to our reading appears to be a discrepancy in the bill. It isn't clear from our reading whether or how this bill applies to text messages, pictures, videos, etc., stored **as files** on a device that isn't password protected and is not an Internet account.

It appears that so long as students run their content through an Internet-based account, they have more protection from a search than students who use "standard" text/file storage on a device. We're not sure this was intended.

Thank you for this opportunity to speak before you. We would be happy to work with you to address the concerns we raised in this testimony, and I would be happy to answer any questions you may have.