

POLICE DEPARTMENT  
**CITY AND COUNTY OF HONOLULU**

801 SOUTH BERETANIA STREET · HONOLULU, HAWAII 96813  
TELEPHONE: (808) 529-3111 · INTERNET: www.honolulu.org



KIRK W. CALDWELL  
MAYOR

LOUIS M. KEALOHA  
CHIEF

DAVE M. KAJIHIRO  
MARIE A. McCAULEY  
DEPUTY CHIEFS

OUR REFERENCE RN-JK

February 8, 2013

The Honorable Mark M. Nakashima, Chair  
and Members  
Committee on Labor and Public Employment  
State House of Representatives  
Hawaii State Capitol  
415 South Beretania Street  
Honolulu, Hawaii 96813

Dear Chair Nakashima and Members:

Subject: House Bill No. 713, Relating to Social Media

I am Alan K. Bluemke, Major of the Human Resources Division of the Honolulu Police Department (HPD), City and County of Honolulu.

The HPD opposes the passage of House Bill No. 713, Relating to Social Media. The HPD relies on many different sources to check the background and suitability of a recruit or civilian applicant, including social media on the internet. Vital information regarding the ethical and moral character of an applicant can be found through the social media. The passing of this bill will not only delay the background check process, but it will limit the HPD's ability to thoroughly screen recruit and civilian applicants with the highest levels of integrity to serve the City and County of Honolulu.

The HPD urges you to oppose House Bill No. 713.

Thank you for the opportunity to testify.

Sincerely,

A handwritten signature in black ink, appearing to read "Alan K. Bluemke".

ALAN K. BLUEMKE, Major  
Human Resources Division

Approved:

A handwritten signature in black ink, appearing to read "Louis M. Kealoa".

LOUIS M. KEALOHA  
Chief of Police

*Serving and Protecting With Aloha*

**TESTIMONY ON  
HB 713, RELATING TO SOCIAL MEDIA  
BY JEANNINE SOUKI  
ON BEHALF OF THE  
STATE PRIVACY AND SECURITY COALITION**

**Rep. Mark M. Nakashima, Chair  
House Committee on Labor & Public Employment  
Hawaii State Capitol, Room 309  
Honolulu, HI 96813  
Friday, February 8, 2013, 9:00 AM**

- The State Privacy and Security Coalition – a coalition of leading communications, technology and media companies and trade associations – writes to express our serious concerns with HB 713. We appreciate the intent of the bill but believe that it is very important that the bill be narrowed slightly and balanced with additional exceptions if it is to become law.
- The bill would, among other things, prohibit an employer from requiring or requesting an employee or applicant to disclose a username or password for the purpose of obtaining access to the employee's or applicant's social media accounts. As drafted, this would prohibit employers from friending any of their employees on Facebook, or asking an employee for his or her home email address, because this is often the “user name” for social media accounts.
- There have been reports of employers asking job-seekers for access to job-seekers’ personal social media accounts. We agree that there is no valid reason for employers in almost all sectors to request that job applicants relinquish log-in credentials for personal social media accounts.
- It is likewise true that obtaining private account log-in credentials for an employee can be a significant privacy intrusion, and should occur only for very narrow and specific purposes.
- At the same time, none of these concerns apply to employee use of work accounts provided by an employer, or to online accounts that an employee uses for business purposes. It is critical that social media privacy bills not prevent employers from supervising work-related employee activities – for example, following an employee’s job-related posts on Twitter through an account that the employee has set up (in fact, this is sometimes required by federal securities laws). It is likewise critical that employers be able to access these accounts as employers can be held legally responsible for employee actions using these accounts, and because they are the employer’s property.
- Furthermore, it is essential that employers be able to investigate specific allegations of illegal activity or work-related misconduct by employees involving an employee personal account. For example, if an employee is harassing another employee from a personal online account, responsible employers need to be able to investigate the allegation to maintain a safe working environment.

- Similarly, if an employee is alleged to have engaged in insider trading or bribery from a personal online account, employers have a responsibility to investigate. Furthermore, when employees download confidential information – for instance, business plans or sensitive personal information that could be used for identity theft – from work computers to a personal online account, it is important that the employer be able to investigate.
- While the bill contains an exception for employers “*to request an employee to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable law,*” this should be broadened to help employers protect their employees from a dangerous working environment and to help employers protect their trade secrets.
- The economic impact of the failure to expand this exception could be very significant. Increasingly, foreign companies are bribing employees of U.S. companies to steal intellectual property/trade secret information that foreign companies are unable to license in the marketplace. In fact, there have been several successful federal prosecutions of this behavior. Failure to broaden exceptions for legitimate employer investigations would assist in creating a “safe zone” for employees who want to steal valuable IP assets of companies in your state by transferring them to the employee’s social media account.
- For these reasons, we strongly support narrow exemptions to augment an employer’s ability to ask an employee – not a job applicant – to share the contents of a personal online account in response to a specific allegation of work-related misconduct involving that personal online account. However, these exemptions would not cover asking the employee to divulge the employee’s log-in credentials to any such personal online account.
- Likewise, this bill should not prevent employers from protecting company networks, blocking access to restricted websites, or complying with legal requirements.
- Without these narrow and entirely reasonable exceptions, this very well-intentioned bill could be used as a shield by employees to hide illegal conduct or undermine the security of company networks and devices. With them, the bill would address an important privacy issue in a thoughtful and balanced way.
- Finally, to the extent that employers are prohibited from requesting job applicants’ or employees’ log-in credentials, employers should not be subject to any claim for negligent hiring for failing to make that prohibited request.
- We respectfully urge the Committee to oppose this bill, unless it is amended to address the issues above. For your convenience, we have attached a potential amendment to the bill and would be happy to work with you further on this. Thank you for the opportunity to testify, and we appreciate your consideration of our concerns.

## A BILL FOR AN ACT

RELATING TO SOCIAL MEDIA.

### BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. Chapter 378, Hawaii Revised Statutes, is amended by adding a new section to Part I to be appropriately designated and to read as follows:

"§378- Prohibited Acts. (a) An employer shall not:

(1) Require or request that an employee or applicant disclose any user name and password, password, or other means of authentication for accessing the employee's or applicant's personal online account or personal online service;

(2) Discharge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee solely for an employee's refusal to disclose any information specified in subsection (a)(1) of this section;

(3) Fail or refuse to hire any applicant as a result of the applicant's refusal to disclose any information specified in subsection (a)(1) of this section;

~~Deleted: Employer access to employee social media p~~

~~Deleted: r~~

~~Deleted: for employment to do any of the following: f  
(1) D~~

~~Deleted: or~~

~~Deleted: the purpose of~~

~~Deleted: social media~~

~~Deleted: Access the employee's or applicant's personal social media in the presence of the employer~~

~~Deleted: or~~

~~Deleted: Divulge any personal social media, except as provided in subsection (b).~~

(4) Be held liable for failure to request or require that an applicant or employee disclose any information specified in subsection (a)(1) of this section.

(b) An employee may not transfer employer proprietary or confidential information or financial data to an employee's personal online account or personal online service without the employer's authorization.

(c) Nothing in this section shall affect an employer's existing rights and obligations to:

(1) Conduct an investigation:

(i) For the purpose of ensuring compliance with applicable laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on a personal online account or personal online service by an employee or other source;

(ii) Of an employee's actions based on the receipt of specific information about the unauthorized transfer of an employer's proprietary information, confidential information or financial data to a personal online account or personal online service by an employee or other source; or

(iii) Conducting an investigation as specified in paragraphs (i) and (ii) includes requiring the employee's cooperation to share the content that has been reported in order to make a factual determination.

(2) Request an employee to divulge any information reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable law; provided that such information is used solely for purposes of that investigation or a related proceeding.

Deleted: r

Deleted: personal social media

Deleted: the social media

(3) Require or request an employee to disclose any user name or password, or other means of authentication for accessing:

Deleted: c

Deleted: Nothing in this section shall preclude an employer from r

Deleted: ing

Deleted: ing

Deleted: the purpose of

(i) Any electronic communications device supplied or paid for in whole or in part by the employer; or

Deleted: a

Deleted: employer-issued

Deleted: .

(ii) Any accounts or services provided by the employer or by virtue of the employee's employment relationship with the employer or that the employee uses for business purposes.

(4) Discipline or discharge an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal online account without the employer's authorization.

Deleted: d

(5) Terminate or take an adverse action against an employee or applicant if otherwise permitted by law.

Deleted: An employer shall not discharge, discipline, threaten to discharge or discipline, or retaliate against an employee or applicant for not complying with a request or demand by the employer that violates this section; provided that this section shall not prohibit an employer from

(6) Restrict or prohibit an employee's access to certain websites while using an electronic communications device paid for in whole or in part by the employer or while using an employer's network or resources, in compliance with state and federal law; or

Deleted: t

Deleted: ing

Deleted: ing

(7) Monitor, review, access, or block electronic data stored on an electronic communications device paid for in whole or in part by the employer, or traveling through or stored on an employer's network, in compliance with state and federal law.

(d) This Act does not prohibit or restrict an employer from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without the information specified in subsection (a)(1) of this section or that is available in the public domain.

(e) Nothing in this Act shall be construed to prevent an employer from complying with the requirements of state or federal statutes, rules or regulations, case law or rules of self-regulatory organizations.

(f) As used in this section:

(1) "Applicant" means an applicant for employment.

(2) (i) "Electronic communications device" means any device that uses electronic signals to create, transmit, and receive information.

(ii) "Electronic communications device" includes computers, telephones, personal digital assistants, and other similar devices.

(3) "Employer" means a person, including a unit of state or local government, engaged in a business, industry, profession, trade, or other enterprise in this state, and includes an agent, representative, and designee of the employer.

Deleted: e  
Deleted: L

(4) "Personal online account" means an online account that is used by an employee or applicant exclusively for personal communications unrelated to any business purposes of the employer. This definition shall not include any account created, maintained, used or accessed by an employee or applicant for business related communications or for a business purpose of the employer.

**Deleted:** "social media" means an electronic service or account or electronic content, including videos, photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or internet website profiles or locations."

SECTION 2. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 3. New statutory material is underscored.

SECTION 4. This Act shall take effect upon its approval.

INTRODUCED BY: \_\_\_\_\_

**Report Title:**

Social Media; Password; Username; Privacy; Employer; Employee; Employment

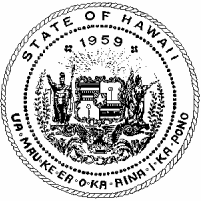
**Description:**

Prohibits employers from requiring or requesting an employee or applicant to disclose any user name, and password, password, or other means of authentication to obtain access to the employee's or applicant's personal online account or personal online service.

- Deleted: s
- Deleted: and
- Deleted: s for employment
- Deleted: from
- Deleted: ing
- Deleted: social media
- Deleted: s
- Deleted: or
- Deleted: s

*The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.*





# HAWAI‘I CIVIL RIGHTS COMMISSION

830 PUNCHBOWL STREET, ROOM 411 HONOLULU, HI 96813 · PHONE: 586-8636 FAX: 586-8655 TDD: 568-8692

February 8, 2013  
Rm. 309, 9:00 a.m.

To: The Honorable Mark M. Nakashima, Chair  
Members of the House Committee on Labor and Public Employment

From: Linda Hamilton Krieger, Chair  
and Commissioners of the Hawai‘i Civil Rights Commission

Re: H.B. No. 713

The Hawai‘i Civil Rights Commission (HCRC) has enforcement jurisdiction over Hawai‘i’s laws prohibiting discrimination in employment, housing, public accommodations, and access to state and state-funded services. The HCRC carries out the Hawai‘i constitutional mandate that no person shall be discriminated against in the exercise of their civil rights. Art. I, Sec. 5.

The HCRC supports the intent of H.B. No. 713, but does not support the placement of this employment practice provision in HRS Chapter 378, Part I, under HCRC jurisdiction. H.B. No. 713 would prohibit employers from requiring applicants and employees from disclosing the usernames or passwords to their social media accounts. The HCRC has jurisdiction over only Part I of Chapter 378, which is our state fair employment law prohibiting discrimination in employment on the bases of race, sex, including gender identity or expression, sexual orientation, age, religion color, ancestry, disability, marital status, arrest and court record, domestic violence or sexual violence victim status, retaliation, National Guard participation, assignment of income for child support, breastfeeding, or credit history or credit report. The HCRC does not have jurisdiction over the other parts of Chapter 378: Part II (Lie Detector Tests); Part III (Unlawful Suspension or Discharge; Part IV (Fair Representation); Part V (Whistleblower Protection Act); or Part VI (Victims Protection).

If added to Chapter 378, this prohibited practice would protect a right and expectation of privacy for applicants and employees with regard to their personal social media accounts. This protection is different in kind from the anti-discrimination focus of the civil rights laws that the HCRC enforces. It is more akin to the protections found in the parts of Chapter 378 that the HCRC does not enforce – more like the employment practices protections regarding lie detector tests and whistleblowers. Of course, under current law if an employer uses access to social media, whether authorized by an applicant/employee or not, to screen out or discriminate on the basis of race, sex, sexual orientation, age, religion, ancestry, or any other protected basis, that would be a prohibited practice under Chapter 378, Part I. The proposed new protection applies to any requirement or request for a user name or password for an applicant or employee, even if used in a non-discriminatory manner. It does not belong in Chapter 378, Part I, under HCRC jurisdiction.

If the Committee decides to move and recommend passage of H.B. No. 713, the HCRC respectfully requests that it be in the form of an amended H.D.1, removing the new employment practices prohibition from HRS Chapter 378, Part I, to a new part of the same chapter.

Thank you for considering the HCRC's concerns.

**Testimony to the House Committee on Labor and Public Employment  
Friday, February 8, 2013 at 9:00 A.M.  
Conference Room 309, State Capitol**

**RE: HOUSE BILL 713 RELATING TO SOCIAL MEDIA**

Chair Nakashima, Vice Chair Hashem, and Members of the Committee:

The Chamber of Commerce of Hawaii ("The Chamber") **has serious concerns on HB 713 Relating to Social Media.**

The Chamber is the largest business organization in Hawaii, representing more than 1,100 businesses. Approximately 80% of our members are small businesses with less than 20 employees. As the "Voice of Business" in Hawaii, the organization works on behalf of its members, which employ more than 200,000 individuals, to improve the state's economic climate and to foster positive action on issues of common concern.

The Chamber appreciates the intent of the bill. We understand that several high profile cases that happened on the mainland brought this issue forward. However, we do not believe that this is a prevalent problem in Hawaii.

We appreciate the intent of the bill but we believe that it needs more discussion before moving forward.

Thank you for this opportunity to express our views.

**TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS  
IN OPPOSITION TO HB 713, RELATING TO SOCIAL MEDIA**

February 8, 2013

Hon. Representative Mark M. Nakashima, Chair  
Committee on Labor and Public Employment  
State House of Representatives  
Hawaii State Capitol, Conference Room 309  
415 South Beretania Street  
Honolulu, Hawaii 96813

Dear Chair Nakashima and Committee Members:

Thank you for the opportunity to testify in opposition to HB 713, relating to Social Media.

Our firm represents the American Council of Life Insurers (“ACLI”), a Washington, D.C., based trade association with more than 300 member companies operating in the United States and abroad. ACLI advocates in federal, state, and international forums for public policy that supports the industry marketplace and the 75 million American families that rely on life insurers’ products for financial and retirement security. ACLI members offer life insurance, annuities, retirement plans, long-term care and disability income insurance, and reinsurance, representing more than 90 percent of industry assets and premiums. Two hundred thirty-two (232) ACLI member companies currently do business in the State of Hawaii; and they represent 94% of the life insurance premiums and 92% of the annuity considerations in this State.

Today, many individuals use social media accounts and personal devices for both business and personal purposes.

ACLI and its member companies believe that an individual’s personal information should remain private and should not be subject to inspection by an employer or prospective employer.

However, legislation which seeks to protect strictly personal social media account information must simultaneously accommodate legal and regulatory requirements imposed upon life insurers that certain communications be reviewed and retained to comply with recordkeeping requirements.

Life insurance companies have legal obligations with respect to business communications made by their captive insurance producers and registered representatives of their affiliated broker-dealers or registered investment advisers (RIAs).

State insurance laws and regulations require insurers to supervise, monitor and review their captive producers’ communications with the public in the marketing and sale of life insurance products.

The following are but a few examples of a life insurer’s oversight obligations:

Hawaii's law relating annuities require a life insurer to “. . . establish and maintain a supervision system that is reasonably designed to achieve the insurer's and its producer's compliance . . .” with the suitability rules relating to the sale of annuities to seniors. §§431:10D-623(a) and (f), HRS.

A life insurer is obligated to monitor, review and supervise its captive producers in the replacement of a consumer's life insurance policy. §§431:10D-504, 431:10D-505(a), HRS.

Hawaii law requires a life insurer to establish marketing and auditable procedures to assure that the sale of long term care insurance is suitable for the consumer given the consumer's coverage under any existing policy and the consumer's financial resources, goals or needs with respect to long term care. §§431:10H-229.

If a life insurer fails to fulfill its oversight obligations, as described above, the life insurer is subject to monetary fines and other penalties imposed under Hawaii's Insurance Code.

The National Association of Insurance Commissioners (NAIC) has issued a White Paper titled “The Use of Social Media in Insurance.” This Paper provides an overview of insurance regulatory and compliance issues associated with the use of social media, and guidance for addressing identified regulatory and compliance issues. Insurance regulators have emphasized the requirement that “[a]n insurer's policies, procedures and controls relative to social media communications must comport with existing regulations, which include, but are not limited to, statutes and rules related to advertising and marketing, record retention, consumer privacy and consumer complaints.” To comply with these requirements, insurers must have the ability to properly supervise their producers' social media communications, if such content is attributable to the insurer or the insurer's products or services.

In addition, federal and state securities laws and regulations as well as self-regulatory organization rules require broker-dealers and RIAs to comply with specific requirements related to its communications with the public in order to protect investors and consumers. For example, the Financial Industry Regulatory Authority<sup>1</sup> (FINRA) rules require prior review of certain advertisements and other specified communications. In addition, strict recordkeeping requirements apply to business communications of registered representatives.

Further, the Securities Exchange Commission issued National Examination Risk Alert earlier this year which details regulatory requirements related to the use of social media by RIAs and their investment advisory representatives (IARs). As part of an effective compliance program, the SEC staff stressed a firm's obligation to maintain an effective compliance program to ensure compliance with securities laws and rules related to their use of social media. Key components of an effective compliance program includes policies and procedures which establish usage guidelines, content standards, sufficient monitoring, approval of content, training, and recordkeeping responsibilities.

---

<sup>1</sup> “The Financial Industry Regulatory Authority (FINRA) is the largest independent regulator for all securities firms doing business in the US. Its mission is to protect America's investors by making sure the securities industry operates fairly and honestly.” FINR website – “About FINRA”.

In large part these regulatory notices and guidelines affirm that existing approval, supervision, and recordkeeping requirements are applicable regardless of the delivery mechanism. Supervising employers have an obligation to monitor personal social media accounts utilized for business purposes, and must have in place mechanisms to capture and store relevant communications.

HB 713 would prevent a life insurer from accessing the personal social media of its captive insurance producers, RIAs and their IARs to insure their compliance with these legal and regulatory requirements.

HB 713 in relevant part provides:

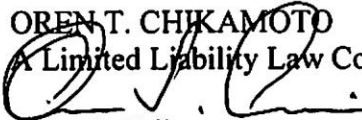
An employer shall not require or request an employee . . . to do any of the following:

- (1) Disclose a username or password for the purpose of accessing the employee's . . . personal social media;
- (2) Access the employee's . . . personal social media in the presence of the employer;
- (3) Divulge any personal social media . . . .

HB 713 would, therefore, make it unlawful for a life insurer to access the personal social media account of its captive insurance producers, RIAs and their IARs.

Accordingly, ACLI respectfully requests that HB 713 be amended as set forth in its accompanying Proposed HD 1.

Again, thank you for the opportunity to testify in opposition to HB 713, relating to social media.

LAW OFFICES OF  
OREN T. CHIKAMOTO  
A Limited Liability Law Company  
  
Oren T. Chikamoto  
1001 Bishop Street, Suite 1750  
Honolulu, Hawaii 96813  
Telephone: (808) 531-1500  
Facsimile: (808) 531-1600

STATE OF HAWAII

---

---

1      **A BILL FOR AN ACT**

RELATING TO SOCIAL MEDIA.

**BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:**

SECTION 1. Chapter 378, Hawaii Revised Statutes, is amended by adding a new section to Part I to be appropriately designated and to read as follows:

"§378- Employer access to employee ~~social media~~ personal account prohibited. (a) An employer shall not require or request an employee or applicant for employment to do any of the following:

(1) Disclose a username or password for the purpose of accessing the employee's or applicant's personal account ~~social media~~;

(2) Access the employee's or applicant's personal account ~~social media~~ in the presence of the employer;  
or

(3) Divulge any information in a personal account ~~social media~~, except as provided in subsection (b).

(b) Nothing in this section shall affect an employer's existing rights and obligations to ~~require~~ request an employee to divulge information in a personal account ~~social media~~ reasonably believed to be relevant to an investigation of allegations of

employee misconduct or an employee's violation of applicable law; provided that such informationthe social media is used solely for purposes of that investigation or a related proceeding.

(c) Nothing in this section shall be construed to prevent an employer from complying with the requirements of State or federal statutes, rules or regulations, case law or rules of self-regulatory organizations.

~~(e)~~(d) Nothing in this section shall preclude an employer from requiring or requesting an employee to disclose a username or password for the purpose of accessing an employer-issued electronic device.

~~(d)~~(e) An employer shall not discharge, discipline, threaten to discharge or discipline, or retaliate against an employee or applicant for not complying with a request or demand by the employer that violates this section; provided that this section shall not prohibit an employer from terminating or taking an adverse action against an employee or applicant if otherwise permitted by law.

~~(e)~~(f) As used in this section, "social media" means an electronic service or account or electronic content, including videos, photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or internet website profiles or locations." "personal account" means an



account, service or profile on a social networking website that is used by a current or prospective employee exclusively for personal communications unrelated to any business purposes of the employer. This definition shall not apply to any account, service or profile created, maintained, used or accessed by a current or prospective employee for business purposes of the employer or to engage in business related communications.

SECTION 2. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 3. New statutory material is underscored.

SECTION 4. This Act shall take effect upon its approval.

INTRODUCED BY: \_\_\_\_\_

**Report Title:**

Social Media; Password; Username; Privacy; Employer; Employee; Employment

**Description:**

Prohibits employers from requiring employees and applicants for employment from disclosing social media usernames or passwords.

*The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.*



Committee: Committee on Labor and Public Employment  
Hearing Date/Time: Friday, February 8, 2013, 9:00 a.m.  
Place: Conference Room 309  
Re: Testimony of the ACLU of Hawaii in Support of H.B. 713, Relating to Social Media

Dear Chair Nakashima and Members of the Committee on Labor and Public Employment:

The American Civil Liberties Union of Hawaii (“ACLU of Hawaii”) writes in support of H.B. 713, which will prohibit employers from requiring employees or applicants for employment from discussing social media usernames or passwords.

As this is also a growing problem for students, we ask that the bill be amended to apply to educational institutions as well. You might consider amending the bill to mirror the prohibitions laid out in H.B. 1023, the Internet Privacy Protection Act, which protects both employees and students and was heard by EDN/HED on Wednesday, February 6, 2013 at 2:10 p.m.

#### Employees and Applicants

A growing number of employers are demanding that job applicants and employees hand over the passwords to their private social networking accounts such as Facebook. Such demands constitute a grievous invasion of privacy. Private activities that would never be intruded upon offline should not receive less privacy protection simply because they take place online. It is inconceivable that an employer would be permitted to read an applicant’s diary or postal mail, listen in on the chatter at their private gatherings with friends, or look at their private videos and photo albums. Nor should they expect the right to do the electronic equivalent.

Employer policies that request or require employees or applicants to disclose user names and/or passwords to their private internet or web-based accounts, or require individuals to let employers view their private content, constitute a frightening and illegal invasion of privacy for those applicants and employees -- as well those who communicate with them electronically via social media. We are concerned that employers may begin to require this information from job applicants without clear statutory language against it. While employers may permissibly incorporate some limited review of public internet postings into their background investigation procedures, review of password-protected materials overrides the privacy protections users have erected and thus violates their reasonable expectations of privacy in these communications. As

American Civil Liberties Union of Hawaii  
P.O. Box 3410  
Honolulu, Hawaii'i 96801  
T: 808-522-5900  
F: 808-522-5909  
E: [office@acluhawaii.org](mailto:office@acluhawaii.org)  
[www.acluhawaii.org](http://www.acluhawaii.org)

such, we believe that policies such as this may be illegal under the federal Stored Communications Act (SCA), 18 U.S.C. §§2701-11 and Hawaii's privacy laws.<sup>1</sup> These laws were enacted to ensure the confidentiality of electronic communications, and make it illegal for an employer or anyone else to access stored electronic communications without valid authorization. Additionally, such practices constitute the common law tort of invasion of privacy and arguably chill employee speech and due process rights protected under the First and Fourteenth Amendments to the U.S. Constitution.<sup>2</sup>

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."  
<https://www.facebook.com/terms#!/legal/terms>. Thus, sharing one's password or access to one's account with potential or current employers violates these terms of agreement.

Finally, this bill would benefit employers as well. If employers do start reviewing employees' and applicants' private social media sites, they then run the risk of being held liable if there is criminal activity revealed on these sites that they don't catch and/or report to authorities.

Job applicants and employees should not have to give up their first amendment rights, as well as risk the security of their private information, by being forced to divulge their passwords to accounts in order to gain or maintain employment.

---

<sup>1</sup> Section 2701 of the SCA makes it illegal to intentionally (1) access a facility through which an electronic communication service is provided, without valid authorization; or (2) exceed an authorization to access that facility, thereby obtaining an electronic communication while it is in electronic storage in such a system. 18 U.S.C. §2701(a)(1)-(2).

<sup>2</sup> In a different context factually, the National Labor Relations Board (NLRB) made headlines last November by issuing a complaint against a Connecticut company that fired an employee who criticized the company on Facebook, in violation of the company's social media policy. *E.g.*, "Feds: Woman Illegally Fired Over Facebook Remarks," available at: [http://www.myfoxdc.com/dpp/news/offbeat/feds-woman-illegally-fired-over-facebook-remarks-110910?CMP=201011\\_emailshare](http://www.myfoxdc.com/dpp/news/offbeat/feds-woman-illegally-fired-over-facebook-remarks-110910?CMP=201011_emailshare); "Labor Board: Facebook Vent Against Supervisor Not Grounds for Firing," available at: <http://www.cnn.com/2010/TECH/social.media/11/09/facebook.firing/index.html> The NLRB maintains that both the firing and the social media policy itself violate employees' protected speech rights under the National Labor Relations Act. *See* NLRB Press Release, [http://www.nlr.gov/shared\\_files/Press%20Releases/2010/R-2794.pdf](http://www.nlr.gov/shared_files/Press%20Releases/2010/R-2794.pdf). While the Connecticut case involves the employee's right to engage in particular speech protected under the NLRA, it also addresses the limits that federal law places on employers' interference and monitoring of employees' social media use more generally, and thus is worthy of notice.

### Students

Students have the same privacy rights like any American, and school officials should not have the right to fish through their password-protected information. Students do not give up their constitutional rights when they walk onto school grounds.

Schools have an important duty to provide education for all students, and students are responsible for following reasonable school rules so school remains a safe, welcoming place where all students can learn. But students also have free speech and privacy rights that our schools must recognize and respect. Just as an employer requesting the passwords of an applicant or employee is an invasion of privacy, school officials requesting the same from their students is also.

Many universities have recently started requiring student athletes to provide them with access to the private content on their social media accounts. The University of Maryland, for example, currently monitors athletes' social media activity through an internal compliance office. Sometimes this is done by requiring student athletes to install social media spying software onto their personal electronic devices. Other times schools will require that friend them on Facebook or allow them to follow them on their private Twitter account. Some schools hire private companies to do this.

A recent article in the Washington Post reported the following:

*Schools are essentially paying for a software program that scans athletes' Tweets, Facebook posts and other social media activity 24 hours a day. The program zeroes in on keywords (popular ones include expletives, brands of alcohol, drinking games, opponents' names and common misspellings of racial profanities) and sends each athlete and coach or administrator an e-mail alert when a questionable post has been published. Coaches or administrators can log in with a username and password to see a list of student, and each student's "threat level" — green for low, orange for medium and red for high — and a link or screen shot of the comment that set off red flags.*

While students must agree to the terms of use and install applications allowing these companies to do so, if their school requires them to agree to these terms as a condition for playing on a particular team it is hardly done of free will or freely consented to.

Chair Nakashima and LAB Committee Members  
February 8, 2013  
Page 4 of 5

This raises a number of concerning legal questions. By requiring students to friend a third party on Facebook, this may be a violation of the 4<sup>th</sup> amendment as an unreasonable search and seizure since students likely have a reasonable expectation of privacy if they have set their settings such that most information is to be kept private and only available to those they wish to have access.

In addition, monitoring the social media private accounts of students will likely lead to censorship of these accounts and this could violate the students' first amendment rights to freedom of speech. At least one federal circuit court has already held that Universities don't have the right to punish professors for what they state in their own publications. *See Bauer v. Sampson*, 261 F.3d 775 (9<sup>th</sup> Cir. 2001) (ruling that community college professor's self-published newsletter which placed another professor on his "shit list" which was a "two-ton slab of granite" which he hoped to drop one day on the president's head was protected speech under the First Amendment, and that the school could not punish him for it).

An additional problem is that often only high profile teams are required to provide this information. Accordingly, such a policy may violate Title IX due to gender discrimination.

Lastly, schools that require their student athletes or any students or applicants to give them access to their personal social media accounts may be subjecting themselves to significant legal liability. By taking on the responsibility of watching over the accounts, the school may be assuming legal liability for student activities reported on the sites. For example, if a student reports criminal activity or intent to commit such activity, the school may be liable if they don't catch it and report it.

Please pass S.B. 207 with amendments to include protections for students.

Thank you for this opportunity to testify.

Sincerely,  
Laurie A. Temple  
Staff Attorney and Legislative Program Director  
ACLU of Hawaii

*About the American Civil Liberties Union of Hawaii*

*The American Civil Liberties Union of Hawaii ("ACLU") has been the state's guardian of liberty for 47 years, working daily in the courts, legislatures and communities to defend and*

American Civil Liberties Union of Hawai'i  
P.O. Box 3410  
Honolulu, Hawai'i 96801  
T: 808-522-5900  
F: 808-522-5909  
E: [office@acluhawaii.org](mailto:office@acluhawaii.org)  
[www.acluhawaii.org](http://www.acluhawaii.org)

Chair Nakashima and LAB Committee Members  
February 8, 2013  
Page 5 of 5

*preserve the individual rights and liberties equally guaranteed to all by the Constitutions and laws of the United States and Hawaii.*

*The ACLU works to ensure that the government does not violate our constitutional rights, including, but not limited to, freedom of speech, association and assembly, freedom of the press, freedom of religion, fair and equal treatment, and privacy.*

*The ACLU network of volunteers and staff works throughout the islands to defend these rights, often advocating on behalf of minority groups that are the target of government discrimination. If the rights of society's most vulnerable members are denied, everyone's rights are imperiled.*

American Civil Liberties Union of Hawai'i  
P.O. Box 3410  
Honolulu, Hawai'i 96801  
T: 808-522-5900  
F: 808-522-5909  
E: [office@acluhawaii.org](mailto:office@acluhawaii.org)  
[www.acluhawaii.org](http://www.acluhawaii.org)

[REDACTED]

---

**From:** mailinglist@capitol.hawaii.gov  
**Sent:** Tuesday, February 05, 2013 9:29 AM  
**To:** LABtestimony  
**Cc:** mendezj@hawaii.edu  
**Subject:** \*Submitted testimony for HB713 on Feb 8, 2013 09:00AM\*

[REDACTED] [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED] [REDACTED]

**HB713**

Submitted on: 2/5/2013

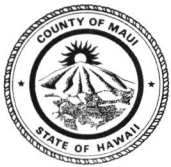
Testimony for LAB on Feb 8, 2013 09:00AM in Conference Room 309

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Present at Hearing</b>
Javier Mendez-Alvarez	Individual	Support	No

Comments:

Please note that testimony submitted less than 24 hours prior to the hearing, improperly identified, or directed to the incorrect office, may not be posted online or distributed to the committee prior to the convening of the public hearing.

Do not reply to this email. This inbox is not monitored. For assistance please email [webmaster@capitol.hawaii.gov](mailto:webmaster@capitol.hawaii.gov)



ALAN M. ARAKAWA  
MAYOR

OUR REFERENCE

YOUR REFERENCE

# POLICE DEPARTMENT

## COUNTY OF MAUI

55 MAHALANI STREET  
WAILUKU, HAWAII 96793  
(808) 244-6400  
FAX (808) 244-6411



GARY A. YABUTA  
CHIEF OF POLICE

CLAYTON N.Y.W. TOM  
DEPUTY CHIEF OF POLICE

February 4, 2013

**LATE TESTIMONY**

The Honorable Mark M. Nakashima, Chair  
And Members of the Committee on Labor & Public Employment  
House of Representatives  
State Capitol  
Honolulu, Hawaii 96813

RE: House Bill No. 713, RELATING TO SOCIAL MEDIA

Dear Chair Nakashima and Members of the Committee:

The Maui Police Department OPPOSES the passage of H.B. No. 713.

The passage of this bill prohibits employers from requiring employees and applicants for employment from disclosing social media usernames or passwords.

In the interest of public safety and the integrity of the law enforcement agencies that this bill could affect, the Maui Police Department is opposing the proposal of this bill. A police applicant's background check should be extensive and thorough, as we the public will be putting our trust in this future officer for the protection of our respective communities.

A check on their social media accounts would reveal a lot about an applicant's personal traits. Again, the purpose of the check would assist the respective department by providing just this one tool in properly screening the applicant for employment as a future police officer.

The Maui Police Department again asks that you OPPOSE the passage of H.B. No. 713.

Thank you for the opportunity to testify.

Sincerely,

GARY A. YABUTA  
Chief of Police



# LATE TESTIMONY

**From:** mailinglist@capitol.hawaii.gov  
**Sent:** Thursday, February 07, 2013 4:27 PM  
**To:** LABtestimony  
**Cc:** Karen@RedwoodGames.com  
**Subject:** Submitted testimony for HB713 on Feb 8, 2013 09:00AM

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

## HB713

Submitted on: 2/7/2013

Testimony for LAB on Feb 8, 2013 09:00AM in Conference Room 309

Submitted By	Organization	Testifier Position	Present at Hearing
Karen Chun	Individual	Support	No

Comments: This is a good bill. People have the expectation and right to keep their private lives private. If they've set their privacy controls so that only people they choose can see their social media accounts, then an employer has no right to see them -- just like an employer has no right to go through their diaries.

Please note that testimony submitted less than 24 hours prior to the hearing, improperly identified, or directed to the incorrect office, may not be posted online or distributed to the committee prior to the convening of the public hearing.

Do not reply to this email. This inbox is not monitored. For assistance please email [webmaster@capitol.hawaii.gov](mailto:webmaster@capitol.hawaii.gov)