

HAWAI‘I CIVIL RIGHTS COMMISSION

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

February 19, 2016
Rm. 325, 3:00 p.m.

To: The Honorable Karl Rhoads, Chair
Members of the House Committee on Judiciary

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

Re: H.B. No. 1739, H.D.1

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.

H.B. No. 1739, H.D.1, if enacted, will prohibit employers from requiring or requesting employees and potential employees to grant access to personal account usernames and passwords.

The HCRC supports the intent of H.B. No. 1739, with the H.D.1 amendment that provides, in a new HRS subsection 378-__ (d), that nothing in the new section shall diminish the authority and obligation of an employer to investigate complaints, allegations, or the occurrence of sexual, racial, or other prohibited harassment under chapter 378, part I.

The HCRC requests that the new statutory protection established by H.B. No. 1739, H.D.1, be placed in a new part of chapter 378, providing for both civil penalties for violations and a direct civil cause of action for injunctive relief and damages, rather than in part I of chapter 378, because the privacy rights protected by the new statute are different in kind from the protected bases (race, sex, ancestry, religion, sexual orientation, etc.) that fall under HCRC jurisdiction. Employment discrimination based on information obtained online (e.g., an applicant’s or employee’s race, ancestry, religion, marital status) is already prohibited under chapter 378, part I.



February 16, 2016

House's Committee on Judiciary
Hawaii State Capitol
415 South Beretania Street, Room 325
Honolulu, HI 96813

Hearing: Friday, February 19, 2016 – 3:00 p.m.

RE: **STRONG SUPPORT for House Bill 1739 HD 1 – RELATING TO EMPLOYMENT**

Aloha Chairperson Rhoads, Vice Chair San Buenaventura and fellow committee members,

I am writing in STRONG SUPPORT to House Bill 1739 HD 1 on behalf of the LGBT Caucus of the Democratic Party of Hawai'i. HB 1739 HD 1 will prohibit, subject to certain exemptions, employers from requiring, requesting, or coercing employees or potential employees to provide access to their personal social media accounts.

The right to keep one's personal and professional life separate is necessity for any civilized society. This is especially true for members of the LGBT community that may have decided for a variety of reasons to not come out at work. The decision to come out is a personal one and should not be a requirement for employment. Without this bill LGBT citizens have the fear of being outed by their employer since they would have full access to all their emails as well as their social media life that they may have only shared with their selected friends.

The reason the LGBT Caucus finds this bill and imperative is because of the fact that 90% of transgender employees and 35% of lesbian, gay and bisexual report experiencing harassment and/or discrimination by their employer and/or fellow employees. To force LGBT citizens to face this kind of harassment by giving their employer unfettered access to their email and social media accounts is unacceptable.

We ask that you support this bill to help protect all workers from unnecessary search and seizure by their employer.

Mahalo nui loa,

Michael Golojuch, Jr.
Chair



KOBAYASHI SUGITA & GODA, LLP
Attorneys at Law

Bert T. Kobayashi, Jr.*
Alan M. Goda*

John R. Aube*
Wendell H. Fujii*
Charles W. Gall*
Neal T. Gota
Clifford K. Higa*
Robert K. Ichikawa*
Christopher T. Kobayashi*
Jan M. L. Y. Kutsunar*

David M. Louie*
Jonathan S. Moore
Bruce A. Nakamura*
Kenneth M. Nakasone*
Gregory M. Sato*
Jesse W. Schiel*
Craig K. Shikuma*
Lex R. Smith*
Joseph A. Stewart*
David B. Tongg*
Thao T. Tran

*A Law Corporation

Yuko Funaki
Caycie K. Gusman
Charles D. Hunter
Nicholas R. Monlux
Aaron Mun
Gabriele V. Provenza
Anthony Suetsugu
Brian D. Tongg
Maria Y.Y. Wang

Of Counsel:
Kenneth Y. Sugita*
Burt T. Lau*
John F. Lezak*
Larry L. Myers*

February 18, 2016

Honorable Karl Rhoads
Chair
Members of the Judiciary Committee
House of Representatives
State Capitol Building, Room 302
Honolulu, Hawaii 96813

Re: Testimony Regarding House Bill 1739, HD 1
Requesting Amendment

Dear Chair Rhoads and Members of the Judiciary Committee:

Thank you for this opportunity to testify on House Bill 1739, HD 1. Our office represents Facebook. While our client supports the intent of House Bill 1739, House Draft 1, we have some concerns with some of the proposed language used.

Our first concern, is that while the intent is to prevent coercion of employees by “employers,” as currently drafted this bill casts too wide of a net and may apply to people in the employer organization, not intended to be covered by this bill. The language of the bill prohibits an employer from “requesting” an “employee or potential employee” to be added to their list of contacts associated with a personal account. Unfortunately the definition section of Section 378-1 H.R.S. provides that “Employer” means **any person**, including the State or any of its political subdivisions **and any agent** of such person, having one or more employees, but shall not include the United States.” While an “agent” is not defined in the statute, it could mean a co-employee or other person acting on behalf of the employer. It could mean a “line-supervisor” or other intermediate supervisor, who is closer to being a fellow employee with all other employees, and yet, under the broad definition currently in place, these employees with supervisory control can be construed as “agents” of the employer. The mere fact that these two essentially co-employees use social media to communicate, may unintentionally trigger “employer” liability, when the event would have been entirely innocent and even unknown to the “employer.”

More importantly, in today’s world, the use of “social media” is not just about people communicating and connecting with other people. Many business and commercial ventures have social media pages to inform customers, to advertise, to market new products. In fact many of these business, have sections within their company, which deal with the company’s (i.e. the employer) presence on the internet.

Many of these companies, and even state legislators maintain Facebook and other social media websites, and have ongoing relationships and contacts with employees for a variety of legitimate reasons. By the same token employees of that employer may be on the same social media site on which the employer maintains a presence. Again, the mere communication between someone employed by the “employer” with another co-employee, asking about the co-employee’s social site, would constitute a violation and trigger liability for “employers,” even when there is no hint of an intent or act to coerce that employee.

The intent is to prevent coercion of employees by “employers” which is an important and legitimate concern. However, the mere fact that such a request may have been made, without any underlying malice or intent to coerce or intrude on the employee’s social media presence, should not automatically trigger liability.

There are many reasons why an employer, acting through other employees, might innocently and with good motive make a Facebook “friend” request to an employee. Perhaps a supervisory employee or similar employee in a company has an ongoing social relationship with another employee and follows existing social media practices and sends a “friend” request. That would trigger a violation.

We are concerned that such innocent requests, which have no element of coercion or compelled action, would now be prohibited under the current language of the bill. If the requested employee does not want to acknowledge the “friend” request, they can decline or refuse, and there are laws, currently in place intended to protect employees against workplace intimidation, if the evidence of such circumstances exist.

We certainly would support the prohibition upon coercing or compelling any such requests. Attached as **Exhibit “A”** is a proposed amendment to the current version of HB 1739, HD 1, reflecting a proposed amendment intended to address this concern. We would respectfully request that this section be amended or modified as reflected in the attached Exhibit “A”.

We believe that such a change would eliminate the possible prohibition and establishment of penalties for innocent behavior in simply making a “friend” request.

Thank you for this opportunity to present testimony on this bill and to propose a slight change to the draft of the bill as it presently exists.

Karl Rhoads, Chair
and Members
Judiciary Committee
February 18, 2016
Page 3

Should you have any questions, please do not hesitate to contact the undersigned.

Very truly yours,

A handwritten signature in black ink, appearing to read "David M. Louie", written in a cursive style.

DAVID M. LOUIE

A handwritten signature in black ink, appearing to read "Burt T. Lau", written in a cursive style.

BURT T. LAU

for
KOBAYASHI, SUGITA & GODA

Enclosure: Exhibit "A": Proposed Amendment to HB 1739, HD1

EXHIBIT "A"

PROPOSED AMENDMENT TO HOUSE BILL 1739, HD 1

Section 378-_____ Employer access to employee or potential employee personal accounts prohibited. (a) An employer shall not [~~require, request, or coerce an employee or potential employee to do any of the following~~]:

(1) Require, request, or coerce an employee or potential employee to [D]disclose the username, password, or any other information for the purpose of accessing the employee or potential employee's personal account;

(2) Require, request or coerce an employee or potential employee to [A]access the employee or potential employee's personal account in the presence of the employer;
or

(3) Compel or coerce an employee or potential employee to [A]add anyone, including the employer, to their list of contacts associated with a personal account.



Written Statement of
Robbie Melton
Executive Director & CEO
High Technology Development Corporation
before the
House Committee on Judiciary
Friday, February 19, 2016
3:00 p.m.
State Capitol, Conference Room 325

In consideration of
HB1739 HD1
RELATING TO EMPLOYMENT.

Chair Rhoads, Vice Chair San Buenaventura, and Members of the Committee on the Judiciary.

The High Technology Development Corporation (HTDC) **supports the intent of** HB1739 HD1 which relates to employment. This bill clarifies that personal online accounts used exclusively for personal communications unrelated to any business purposes of the employer should remain private. With the ubiquitousness of online accounts, adding some privacy guidelines is very appropriate.

Thank you for the opportunity to offer these comments.

From: mailinglist@capitol.hawaii.gov
Sent: Thursday, February 18, 2016 12:21 PM
To: JUDtestimony
Cc: otc@chikamotolaw.com
Subject: *Submitted testimony for HB1739 on Feb 19, 2016 15:00PM*

HB1739

Submitted on: 2/18/2016

Testimony for JUD on Feb 19, 2016 15:00PM in Conference Room 325

Submitted By	Organization	Testifier Position	Present at Hearing
Oren T. Chikamoto	American Council of Life Insurers	Oppose	Yes

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

TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS
IN OPPOSITION TO HOUSE BILL HB 1739, HD 1, RELATING TO EMPLOYMENT

February 19, 2016

Via e mail: capitol.hawaii.gov/submittestimony.aspx

Honorable Representative Karl Rhoads, Chair
Committee on Judiciary
State House of Representatives
Hawaii State Capitol, Conference Room 325
415 South Beretania Street
Honolulu, Hawaii 96813

Dear Chair Rhoads and Committee Members:

Thank you for the opportunity to testify in opposition to HB 1739, HD 1, relating to Employment.

Our firm represents the American Council of Life Insurers (“ACLI”), a Washington, D.C., based trade association with approximately 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 sixteen (216) ACLI member companies currently do business in the State of Hawaii; and they represent 93% of the life insurance premiums and 88% 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.

Federal and state securities laws and regulations as well as self-regulatory organization rules require broker-dealers and Registered Investment Advisors (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 Authority¹ (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 has issued a National Examination Risk Alert 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.

Life insurers want to accommodate the use of new technologies by their representatives to the extent practical. At the same time, companies must have in place compliance procedures that ensure compliance with federal and state laws and regulations as well as FINRA rules and guidance.

ACLI submits that to enable a life insurer to more effectively monitor and supervise its captive producers' in their communications with the public as required by law but at the same time protect the legitimate privacy of its captive producers and representatives in their personal communications more clarity in the language of the bill is required.

ACLI suggests that Paragraph (b)(2) of the new Section of the proposed new Part to be included in Chapter 378, which is in Section 1 of the Bill (beginning at line 3, page 2 of the bill) be amended as set forth below:

(b) Nothing in this Section shall prevent an employer from:

...

(2) Complying with applicable laws, rules, or regulations the requirements of State or federal statutes, rules or regulations, case law or rules of self-regulatory organizations;

In addition, as HB 1739, HD 1, as currently drafted does not affirmatively authorize a life insurer to adopt policies and procedures that will enable the insurer to comply with these legal and regulatory requirements ACLI respectfully requests that HB 1739, HD 1, be amended to include the following new provision:

Nothing in this Part shall prevent an employer from implementing and enforcing a policy pertaining to the use of employer issued electronic communications device or to the use of an employee-owned electronic communications device that will be used for business purposes.

¹ “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”.

Again, thank you for the opportunity to testify in opposition to HB 1739, HD 1, relating to Employment.

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
E mail: otc@chikamotolaw.com

Testimony before the House Committee on Judiciary

H.B. 1739, H.D. 1 -- Relating to Employment

**Friday, February 19, 2016
3:00 PM, Conference Room 325**

**By Kelly McCanlies
Director, Privacy Programs
Hawaiian Electric Company, Inc.**

Chair Rhoads, Vice-Chair San Buenaventura, and Members of the Committee:

My name is Kelly McCanlies. I am the Director of Privacy Programs for Hawaiian Electric Company. I am testifying on behalf of Hawaiian Electric Company and its subsidiary utilities, Maui Electric Company and Hawaii Electric Light Company (hereinafter collectively referred to as “the Companies”).

We support the intent of H.B. 1739, H.D. 1, which seeks to protect employees’ privacy in their online social interactions during the hiring process and throughout their employment. However, we request amendments to the bill to ensure that employers’ cybersecurity is not compromised.

As currently written, this bill would limit sharing of cybersecurity data for analysis purposes with subject-matter experts, law enforcement, and cybersecurity vendors. This will impact routine monitoring functions and impair cybersecurity investigatory efforts.

The Companies utilize industry-standard cybersecurity tools to strengthen and protect the Companies’ networks from cyberattack. These tools (which extend beyond firewalls and anti-virus) perform routine monitoring functions. The logs and other collected data is shared with third-party services for round-the-clock monitoring and for cybersecurity-specific analysis.

If employees voluntarily choose to access their “Personal accounts” from within an employers’ network, current tools may inadvertently capture information on “Personal accounts” (as defined in HB 1739, HD 1) in log files and as other data, including packet data of internet traffic across the Companies’ network. This data is sometimes retained for investigatory use in case of cybersecurity incidents.

We have the following concerns:

1. Username is often transmitted in clear text over the internet. Inadvertent capture is unavoidable.
2. Network protection and monitoring tools are more extensive than just firewalls and anti-virus. By calling out these two technologies, the bill artificially limits the scope of the bill.
3. It is an industry standard best practice to NOT allow alteration of computer log files. Bad actors in breach situations might attempt to erase or alter such logs as part of a cyberattack; so log alteration is a strong indicator of a compromised IT system. Therefore, these files are heavily protected to ensure authenticity. Any alterations, such as deleting of “Personal account” information would affect the data’s use in a forensic capacity and as evidence in any criminal proceeding of a cyberattack.

The following changes are recommended to keep the intent of the legislation without endangering employers’ networks.

Page 2 - 3

20 (c) If an employer inadvertently received the username, and
21 password, or any other information that would enable the
1 employer to gain access to the employee or potential employee’s
2 personal account through the use of ~~an otherwise lawful virus~~
3 ~~scan or network monitoring tools~~ or firewalls on an that monitors the employer’s network or
4 employer-provided devices, then the employer is not liable for
5 having that information, unless the employer:
6 (1) Shares that information with anyone who uses that information to access the
employee or potential employee’s personal account; or
7 (2) Uses that information to access the employee or
8 potential employee’s personal account; ~~or~~
9 ~~(3) Does not delete the information as soon as reasonably~~
10 ~~practicable.”~~

And stated earlier, we support the intent of the legislation in protecting employee privacy. We feel that the changes recommended above will satisfy the intent of the legislation, while not limiting cybersecurity protections or cybersecurity information sharing.

Thank you for the opportunity to testify.



LATE

Committee: Committee on Judiciary
Hearing Date/Time: Friday, February 19, 2016, 3:00 p.m.
Place: Conference Room 325
Re: Testimony from the ACLU of Hawaii in Support of H.B. 1739, H.D.1, Relating to Employment

Dear Chair Rhoads and Members of the Committee on Judiciary:

The American Civil Liberties Union of Hawaii (“ACLU of Hawaii”) writes in support of H.B. 1739, H.D.1, which prohibits employers from demanding access to employees’/applicants’ personal social media accounts (such as Facebook and Instagram).

A growing number of employers are demanding that job applicants and employees give employers their passwords to their private social networking accounts such as Facebook. This practice constitutes a significant invasion of privacy and may have a chilling effect on free expression. Social networking sites like Facebook allow for private messages between individuals; just as an employer should never be permitted to go to an employee’s house and look through her personal letters, diary, and/or photographs, employers have no legitimate business interest in accessing an individual’s communications sent electronically. Such a practice violates the employee’s/applicant’s privacy and the privacy of everyone with whom the individual has communicated, and chills the free expression of ideas.

Accessing an applicant’s social media account using the applicant’s password – rather than merely collecting publicly available information – may expose information about a job applicant (such as age, religion, ethnicity, or pregnancy) which an employer is forbidden to ask about. That can expose an applicant to unlawful discrimination and can subject an employer to lawsuits from rejected job candidates claiming such discrimination.

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.

American Civil Liberties Union of Hawaii
P.O. Box 3410
Honolulu, Hawaii 96801
T: 808-522-5900
F: 808-522-5909
E: office@acluhawaii.org
www.acluhawaii.org

Chair Rhoads and Members of the Committee
February 19, 2016
Page 2 of 2

H.B. 1739, H.D.1 does not change current law regarding background checks: prospective employers, including law enforcement officials, can still use the Internet to access public profiles of job candidates; this law merely prohibits access to private materials and communications.

Thank you for this opportunity to testify.

A handwritten signature in black ink that reads "Mandy Finlay". The signature is written in a cursive, flowing style.

Mandy Finlay
Advocacy Coordinator
ACLU of Hawaii

The mission of the ACLU of Hawaii is to protect the fundamental freedoms enshrined in the U.S. and State Constitutions. The ACLU of Hawaii fulfills this through legislative, litigation, and public education programs statewide. The ACLU of Hawaii is a non-partisan and private non-profit organization that provides its services at no cost to the public and does not accept government funds. The ACLU of Hawaii has been serving Hawaii for 50 years.

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
www.acluhawaii.org



**Testimony to the House Committee on Judiciary
Friday, February 19, 2016 at 3:00 P.M.
Conference Room 325, State Capitol**

RE: HOUSE BILL 1739 HD 1 RELATING TO EMPLOYMENT

Chair Rhoads, Vice Chair San Buenaventura, and Members of the Committee:

The Chamber of Commerce Hawaii ("The Chamber") would like to **express concerns regarding** HB 1739 HD 1, which prohibits employers from requiring, requesting, or coercing employees or potential employees to provide access to their personal accounts.

The Chamber is Hawaii's leading statewide business advocacy organization, representing about 1,000 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 members and the entire business community to improve the state's economic climate and to foster positive action on issues of common concern.

While we understand the reasoning behind the proposed bill, we have also seen instances where unnecessary laws create unintended consequences. The Chamber hasn't seen any empirical evidence that private employers routinely request access to applicant and employee personal social media.

There are legitimate exceptions at times to request and receive access to employees' personal social media pages. For example, law enforcement agencies have a public safety need to know who their representatives or potential employees are affiliating themselves with. And private companies may need to be able to investigate inter-office harassment claims that may stem from social media conversations. So, in terms of best practices, maybe a broad exception for workplace investigations to provide content in a personal account that is relevant to that investigation.

Thank you for the opportunity to testify.

LATE TESTIMONY

House Committee on Judiciary
Hawaii State Capitol, Room 325
February 19, 2016; 3:00 PM
415 South Beretania St.
Honolulu, HI 96813

Written Testimony of Jim Halpert

on behalf of the

State Privacy and Security Coalition, Inc.

Dear Chair Rhoads, Vice Chair San Buenaventura, and Members of the Committee:

Thank you very much for the opportunity to testify on House Bill 1739 HD1 Relating to Employment.

The State Privacy & Security Coalition is comprised of 25 major technology and media companies and 6 trade associations representing companies in the technology, media and advertising sectors.

Our coalition is recommending the attached amendments to HB 1739 HD1, which would clearly define the rules governing employer access to employee or potential employee personal accounts. The amendments are based on a model social media privacy law, which our Coalition developed with the national ACLU.

HB 1739 HD1, as amended, would prohibit employers from *coercing* employees or applicants to add the employer to a social media contact list, but would allow *requests* to do so. This is a valuable change in light of the way businesses communicate with employees, customers, and the general public today. Many businesses post updates and offers or specials on social media, for example, and it is reasonable that the employer would invite employees to add the employer to their list of contacts. Our coalition supports this change.

Second, in addition to requiring employees to disclose a username and password to access an employer-issued electronic device (or account or service provided by the employer), as amended the bill would allow employers to require disclosure of "similar authentication information." In many circumstances a username and password are not the only means of accessing a device, account, or service. The amendment would allow employers to obtain alternatives when necessary to access their own devices and networks.

Moreover, employers must be able to ensure compliance with all applicable laws and regulatory requirements, in addition to prohibitions against work-related employee misconduct. The bill, as amended, would allow for that. It would allow employers to request that an employee share specific content regarding a personal account for these purposes.

February 19, 2016


Page 2

Finally, the bill as amended would allow “the use of technology that monitors the employer’s network or employer provided devices for service quality or security purposes,” subject to the conditions already in the bill on the use of the technology. This amendment is an improvement over the previous version of the bill, which limited the network monitoring to an overly specific “virus scan or firewall.” It would allow employers to retain critical information needed to investigate a suspected breach without an invasion of privacy.

These changes are important to help this bill strike the appropriate balance of protecting employee privacy while leaving room for employer practices to protect employers’ networks, systems, and proprietary information.

We thank you for addressing this important issue and would be happy to assist as the bill moves forward.

Respectfully submitted,



James J. Halpert
General Counsel

500 8th Street NW
Washington, DC 20005
(202) 799-4000
Jim.Halpert@dlapiper.com

A BILL FOR AN ACT

RELATING TO EMPLOYMENT.

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

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

4 "PART EMPLOYEE PERSONAL SOCIAL MEDIA

5 §378- Employer access to employee or potential employee

6 personal accounts prohibited. (a) An employer shall not do any
7 of the following:

8 (1) ~~Request, require or coerce an employee or an~~
9 ~~applicant for employment to disclose a username and~~
10 ~~password, password, or any other authentication~~
11 ~~information that allows access to the employee or~~
12 potential employee's personal account;

Deleted: Disclose the

13 (2) ~~Request, require or coerce an employee or an applicant~~
14 ~~for employment to access the employee or applicant's~~
15 personal account in the presence of the employer; or

Deleted: for the purpose of
accessing

16 (3) ~~Compel an employee or applicant for employment to add~~
17 ~~the employer or an employment agency, to their list of~~

Deleted: Compel

Deleted: A

Deleted: potential employee's

Deleted: A

Deleted: anyone, including

Deleted: ,

1 | contacts that enable the employer or an employment
2 | agency to view or otherwise access a personal account.
3 | (b) Nothing in this section shall prevent an employer
4 | from:
5 | (1) Accessing information about an employee or potential
6 | employee that is publicly available;
7 | (2) Complying with applicable laws, rules, or regulations;
8 | (3) Requiring an employee to disclose a username or
9 | password or similar authentication information for the
10 | purpose of accessing:
11 | (A) An employer-issued electronic device; or
12 | (B) An account or service provided by the employer,
13 | obtained by virtue of the employee's employment
14 | relationship with the employer, or used for the
15 | employer's business purposes;
16 | (4) Conducting an investigation or requiring an employee
17 | to cooperate in an investigation, including by
18 | requiring an employee to share the content that has
19 | been reported to make a factual determination, if the
20 | employer has specific information about an
21 | unauthorized transfer of the employer's proprietary

information, confidential information, or financial data, to an employee's personal account;

(5) Prohibiting an employee or potential employee from using a personal account during employment hours, while on employer time, or for business purposes; or

(6) Requesting an employee to share specific content regarding a personal account for the purposes of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct.

Deleted: conducting an investigation of allegation; employee work-related misconduct that violates employer under this chapter

(c) If an employer inadvertently receives the username, password, or any other information that would enable the employer to gain access to the employee or potential employee's personal account through the use of an otherwise lawful

technology that monitors the employer's network or employer-provided devices for network security or data confidentiality purposes, then the employer is not liable for having that information, unless the employer:

Deleted: virus scan or firewa

(1) Uses that information, or enables a third party to use that information, to access the employee or potential employee's personal account; or

Deleted: (1) .
Deleted: Compiles empl potential employee p/ online user name and or similar authentic informationShares th information with an;

Deleted: 2

1 (2) After the employer becomes aware that such information
2 was received, does not delete the information as soon
3 as is reasonably practicable, unless that information
4 is being retained by the employer in connection with
5 an ongoing investigation of an actual or suspected
6 breach of computer, network, or data security. Where
7 an employer knows or, through reasonable efforts,
8 should be aware that its network monitoring technology
9 is likely to inadvertently to receive such
10 information, the employer shall make reasonable
11 efforts to secure that information.

Deleted: 3
Formatted: Highlight
Formatted: Highlight

12 (d) Nothing in this section shall diminish the authority
13 and obligation of an employer to investigate complaints,
14 allegations, or the occurrence of sexual, racial, or other
15 harassment as provided under this chapter.

Deleted: Does not delete the information as soon as reasonably practicable.

16 (e) As used in this section, "personal account" means an
17 account, service, or profile on a social networking website that
18 is used by an employee or potential employee exclusively for
19 personal communications unrelated to any business purposes of
20 the employer."

1 SECTION 2. Section 378-2, Hawaii Revised Statutes, is
2 amended by amending subsection (a) to read as follows:

3 "(a) It shall be an unlawful discriminatory practice:

4 (1) Because of race, sex including gender identity or
5 expression, sexual orientation, age, religion, color,
6 ancestry, disability, marital status, arrest and court
7 record, or domestic or sexual violence victim status
8 if the domestic or sexual violence victim provides
9 notice to the victim's employer of such status or the
10 employer has actual knowledge of such status:

11 (A) For any employer to refuse to hire or employ or
12 to bar or discharge from employment, or otherwise
13 to discriminate against any individual in
14 compensation or in the terms, conditions, or
15 privileges of employment;

16 (B) For any employment agency to fail or refuse to
17 refer for employment, or to classify or otherwise
18 to discriminate against, any individual;

19 (C) For any employer or employment agency to print,
20 circulate, or cause to be printed or circulated
21 any statement, advertisement, or publication or

1 to use any form of application for employment or
2 to make any inquiry in connection with
3 prospective employment, that expresses, directly
4 or indirectly, any limitation, specification, or
5 discrimination;

6 (D) For any labor organization to exclude or expel
7 from its membership any individual or to
8 discriminate in any way against any of its
9 members, employer, or employees; or

10 (E) For any employer or labor organization to refuse
11 to enter into an apprenticeship agreement as
12 defined in section 372-2; provided that no
13 apprentice shall be younger than sixteen years of
14 age;

15 (2) For any employer, labor organization, or employment
16 agency to discharge, expel, or otherwise discriminate
17 against any individual because the individual has
18 opposed any practice forbidden by this part or has
19 filed a complaint, testified, or assisted in any
20 proceeding respecting the discriminatory practices
21 prohibited under this part;

- 1 (3) For any person, whether an employer, employee, or not,
2 to aid, abet, incite, compel, or coerce the doing of
3 any of the discriminatory practices forbidden by this
4 part, or to attempt to do so;
- 5 (4) For any employer to violate the provisions of section
6 121-43 relating to nonforfeiture for absence by
7 members of the national guard;
- 8 (5) For any employer to refuse to hire or employ or to bar
9 or discharge from employment any individual because of
10 assignment of income for the purpose of satisfying the
11 individual's child support obligations as provided for
12 under section 571-52;
- 13 (6) For any employer, labor organization, or employment
14 agency to exclude or otherwise deny equal jobs or
15 benefits to a qualified individual because of the
16 known disability of an individual with whom the
17 qualified individual is known to have a relationship
18 or association;
- 19 (7) For any employer or labor organization to refuse to
20 hire or employ, bar or discharge from employment,
21 withhold pay from, demote, or penalize a lactating

1 employee because the employee breastfeeds or expresses
2 milk at the workplace. For purposes of this
3 paragraph, the term "breastfeeds" means the feeding of
4 a child directly from the breast;

5 (8) For any employer to refuse to hire or employ, bar or
6 discharge from employment, or otherwise to
7 discriminate against any individual in compensation or
8 in the terms, conditions, or privileges of employment
9 of any individual because of the individual's credit
10 history or credit report, unless the information in
11 the individual's credit history or credit report
12 directly relates to a bona fide occupational
13 qualification under section 378-3(2); [~~or~~]

14 (9) For any employer to discriminate against any
15 individual employed as a domestic, in compensation or
16 in terms, conditions, or privileges of employment
17 because of the individual's race, sex including gender
18 identity or expression, sexual orientation, age,
19 religion, color, ancestry, disability, or marital
20 status[-]; or

1 (10) For any employer to refuse to hire or employ, bar or
2 discharge from employment, or otherwise to
3 discriminate against any individual in compensation or
4 in the terms, conditions, or privileges of employment
5 of any individual because of the individual's refusal
6 to disclose any information regarding a personal
7 account according to section 378- (a)."

8 SECTION 3. Statutory material to be repealed is bracketed
9 and stricken. New statutory material is underscored.

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

Report Title:

Personal Account; Privacy; Employment

Description:

Prohibits, subject to certain exemptions, employers from requiring, requesting, or coercing employees or potential employees to provide access to their personal social media accounts. (HB1739 HD1)

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

From: mailinglist@capitol.hawaii.gov
Sent: Tuesday, February 16, 2016 5:36 PM
To: JUDtestimony
Cc: joyamarshall0416@gmail.com
Subject: *Submitted testimony for HB1739 on Feb 19, 2016 15:00PM*

HB1739

Submitted on: 2/16/2016

Testimony for JUD on Feb 19, 2016 15:00PM in Conference Room 325

Submitted By	Organization	Testifier Position	Present at Hearing
Joy Marshall	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