LATE

The Judiciary, State of Hawaii

Testimony to the Committee on Technology and the Arts
Senator Glenn Wakai, Chair
Senator Clarence K. Nishihara, Vice Chair

Tuesday, February 5, 2013, 1:15pm
State Capitol, Conference Room 414

Kevin G. Thornton
Information Technology and Systems Department Head
The Judiciary, State of Hawaii

Bill No. and Title: Senate Bill No. 729, Relating to the Internet Privacy

Purpose: Requires operators of commercial websites or online services that collect personally identifiable information through the Internet about consumers in the State who use the websites or online services to conspicuously post their privacy policies on their websites or through any other reasonably accessible means.

Judiciary's Position:

The Judiciary supports the intent of the bill to protect personal information, but wishes to point out that the definition of "personally identifiable information" is inconsistent with the definition used in other statutes. To the extent possible, it is helpful if a single definition is used so as to minimize confusion. Also, we would suggest that the bill does not address requirements for operators of mobile application and that inclusion should be considered.

"Personal Information" is defined in Hawaii Revised Statutes (HRS) §487N-1, and by reference in HRS §487J-1) as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver's license number or Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

The definition provided in Senate Bill No. 729 is "individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: (1) A first and last name; (2) A home or other physical address, including street name and name of a city or town; (3) An e-mail address; (4) A telephone number; (5) A social security number; (6) Any other identifier that permits the physical or online contacting of a specific individual; or (7) Information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this part."

The Judiciary recommends, for purposes of clarity, that a single definition of "personally identifiable information" be used and that the definition be expanded possibly to include a person's date of birth.

We further wish to point out that although this bill addresses "webpages," mobile applications function in a similar manner to web pages in that operators of these applications also collect "personally identifiable information". The Judiciary recommends that the bill be expanded to require operators of mobile applications to provide a menu option to access the developer's privacy policy. This would ensure that the bill's intent (promoting privacy) would be optimally achieved.

Thank you for the opportunity to testify on Senate Bill No. 729.

LATE

NEIL ABERCROMBIE
GOVERNOR

SHAN S. TSUTSUI
LT. GOVERNOR

STATE OF HAWAII
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
335 MERCHANT STREET, ROOM 310
P.O. Box 541
HONOLULU, HAWAII 96809
Phone Number: 586-2850
Fax Number: 586-2856
www.hawaii.gov/dcca

KEALI'I S. LOPEZ
DIRECTOR

JO ANN M. UCHIDA TAKEUCHI
DEPUTY DIRECTOR

PRESENTATION OF THE
OFFICE OF CONSUMER PROTECTION

TO THE SENATE COMMITTEE ON TECHNOLOGY AND THE ARTS

THE TWENTY-SEVENTH LEGISLATURE
REGULAR SESSION OF 2013

TUESDAY, FEBRUARY 5, 2013
1:15 P.M.

TESTIMONY ON SENATE BILL NO. 729, RELATING TO THE INTERNET PRIVACY.

TO THE HONORABLE GLENN WAKAI, CHAIR,
AND TO THE HONORABLE CLARENCE K. NISHIHARA, VICE CHAIR,
AND MEMBERS OF THE COMMITTEE:

The Department of Commerce and Consumer Affairs ("DCCA"), Office of Consumer Protection ("OCP") appreciates the opportunity to appear today and testify on Senate Bill No. 729, Relating to Internet Privacy. My name is Bruce B. Kim and I am the Executive Director of OCP. **OCP takes no position but offering the following comments**.

This bill raises serious questions on an important subject. However, the potential for unintended consequences is great. Federal laws already exist which may preempt the field regarding privacy in financial transactions (Gramm Leach Bliley - 1999); health

care privacy (HIPAA); and Children's Online Privacy Act (1998).

The State of California passed a comprehensive act in 2004 which requires disclosures of online privacy policies. The California Online Privacy Protection Act[1] ("OPPA"). To the extent that the Federal government has not preempted the field, California's OPPA law functions as a national standard of sorts, as operators cannot identify if the website visitor is a resident of California. Therefore, the California law forces commercial websites to disclose their privacy protection policy to all website users without regard to their state of residency to avoid violating the OPPA law.

The Federal Trade Commission has yet to draft rules on this issue and instead focuses on enforcement of privacy policy violations or violations of existing federal law. Congress has offered legislation to establish a national policy but so far none has passed. If Hawaii enacts legislation in this area, it could conflict with existing federal laws (see above), the California OPPA statute and federal laws which could be enacted in the future.

OCP believes that this issue is important given the proliferation of personal identification information today. However, any legislation to address this issue must be carefully studied and crafted, so as to avoid a patchwork of conflicting state laws or running afoul of Federal preemption.

Thank you for allowing me to testify regarding S.B. 729. If the committee has any questions, I will be happy to answer them.

[1] http://leginfo.ca.gov/pub/03-04/bill/asm/ab_0051-0100/ab_68_bill_20031012_chaptered.pdf

wakai1 - Danille

From: mailinglist@capitol.hawaii.gov
Sent: Tuesday, February 05, 2013 1:18 PM
To: TECTestimony
Cc: anakama@wik.com
Subject: Submitted testimony for SB207 on Feb 5, 2013 13:15PM
Attachments: sb207.pdf

LATE

SB207
Submitted on: 2/5/2013
Testimony for TEC on Feb 5, 2013 13:15PM in Conference Room 414

Submitted By	Organization	Testifier Position	Present at Hearing
Allison	State Privacy & Security Coalition	Oppose	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

TESTIMONY ON
S.B. 207, RELATING TO SOCIAL MEDIA
BY
JEANNINE SOUKI
ON BEHALF OF THE
STATE PRIVACY AND SECURITY COALITION

Sen. Glenn Wakai
Chair, Senate Committee on Technology and the Arts
Hawaii State Capitol, Room 216
Honolulu, HI 96813
Tuesday, February 5, 2013, 1:15 PM

- 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 SB 207. 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.

THE SENATE
TWENTY-SEVENTH LEGISLATURE, 2013
STATE OF HAWAII

S.B. NO. 207

A BILL FOR AN ACT

RELATING TO SOCIAL MEDIA.

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

SECTION 1. The legislature finds that existing law generally regulates the conduct of employers in the State.

The purpose of this Act is to prohibit an employer 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. This Act also prohibits an employer from discharging, disciplining, or otherwise penalizing or threatening to discharge, discipline, or otherwise penalize an employee solely for an employee's refusal to comply with a request or demand by the employer that violates these provisions.

SECTION 2. 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:

Deleted: for employment
Deleted: or
Deleted: for the purpose of
Deleted: ing
Deleted: social media
Deleted: s
Deleted: or
Deleted: retaliating
Deleted: against
Deleted: or applicant
Deleted: not
Deleted: ing
Deleted: Employer access to employee social media p

(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; .

(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

Deleted: r

Deleted: for employment to do any of the following:¶ (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).

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.

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

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

(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.

Deleted: r

Deleted: personal social media

Deleted: the social media

Deleted: c

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

Deleted: ing

Deleted: ing

Deleted: the purpose of

Deleted: a

Deleted: employer-issued

Deleted: .

(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.

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

(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

(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.

Deleted: d

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

Deleted: t

Deleted: ing

Deleted: ing

Deleted: e

Deleted: .

(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.

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

SECTION 4. New statutory material is underscored.

SECTION 5. 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.

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

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