HB1788,HD1

DEPARTMENT OF THE PROSECUTING ATTORNEY

CITY AND COUNTY OF HONOLULU

ALII PLACE
1060 RICHARDS STREET • HONOLULU, HAWAII 96813
PHONE: (808) 547-7400 • FAX: (808) 547-7515

KEITH M. KANESHIRO
PROSECUTING ATTORNEY

ARMINA A. CHING
FIRST DEPUTY PROSECUTING ATTORNEY

THE HONORABLE CLAYTON HEE, CHAIR
SENATE COMMITTEE ON JUDICIARY AND LABOR
Twenty-sixth State Legislature
Regular Session of 2012
State of Hawai`i

March 27, 2012

RE: H.B. 1788, H.D. 1; RELATING TO COMPUTER CRIME.

Chair Hee, Vice Chair Shimabukuro and members of the Senate Committee on Judiciary and Labor, the Department of the Prosecuting Attorney, City and County of Honolulu, submits the following testimony in support of House Bill 1788, House Draft 1. Attached, please see the Department's Proposed Senate Draft 1, for your reference and consideration.

The Department agrees with the crux of H.B. 1788, H.D. 1, which would update Hawai'i's computer fraud statutes by adding language similar to Hawai'i's identity theft statutes. Such updates would better address the realities of modern cybercrime, and serve as a more effective tool for enforcement and prosecution of computer fraud offenses.

As currently written, Hawai'i's computer fraud statutes are too narrow to address most activities that are typically thought of as "computer fraud." For example, first-degree computer fraud requires proof that an offender accessed a computer without authorization to obtain or exert control over the property of another. However, most (would-be) computer fraud offenders use their own computer (i.e. with authorization) to carry out offenses, such as online auction fraud, advance fee scams, counterfeit check scams, phishing and e-mail scams. The language in H.B. 1788, H.D. 1, would fill this gap in the law, using familiar terms from our identity theft statutes.

Similarly, second-degree computer fraud is currently too narrow to effectively prevent or prosecute most types of computer fraud, as it is limited to the misuse of passwords – and that's it. This does not reflect current patterns and schemes used by online fraudsters. The proposed amendments in H.B. 1788, H.D. 1, regarding second- and third-degree computer fraud, would be much more effective, and more accurately reflect the realities of modern-day cybercrime.

In addition, Hawai'i's statutes regarding unauthorized access to computer, which are also addressed in H.B. 1788, H.D. 1, do not currently reflect the dangers posed by this type of crime.

All of us are familiar with the widespread and far-reaching effects that unauthorized computer access can have our society. In 2010, a computer security breach of the University of Hawaii parking garage system affected more than 53,000 people, potentially exposing approximately 41,000 social security numbers and 200 credit card numbers to misuse. Across the country, even larger organizations, such as the Sony Play Station Group, Citigroup, the United States Senate, the C.I.A., and the Arizona State government, have found themselves similarly compromised.

As society becomes increasingly reliant on the Internet for the storage and transfer of our most valuable and confidential information, it becomes increasingly tempting for would-be "hackers" to access our computer networks and information systems without authorization. Moreover, growing Internet connectivity and the proliferation of mobile devices such as tablets and smartphones--combined with the modern ease of creating or obtaining malware--make it possible for practically anyone, anywhere, to engage in online criminal activity at any time.

Even more alarming, we also know that organized criminal groups are increasingly turning to the Internet to commit crimes. They have figured out that the Internet provides anonymity, making it difficult for law enforcement to trace or attribute activity to a particular suspect; they also know that there are a lot of rich targets on the Internet.

Stricter penalties for unauthorized computer access will not only present a stronger deterrent for unauthorized computer access, but also emphasize to the public and would-be offenders that these types of activities will be treated with tougher penalties.

For the reasons noted above, the Department of the Prosecuting Attorney of the City and County of Honolulu supports H.B. 1788, H.D. 1, with proposed amendments in the attached Proposed S.D. 1. Thank for you the opportunity to testify on this matter.

HOUSE OF REPRESENTATIVES
TWENTY-SIXTH LEGISLATURE, 2012
STATE OF HAWAII

H.B. NO. 1788 H.D. 1 Proposed S.D. 1

A BILL FOR AN ACT

RELATING TO COMPUTER CRIME.

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

SECTION 1. Chapter 708, Hawaii Revised Statutes, is amended by adding a new section to part IX to be appropriately designated and to read as follows:

"**§708- Computer fraud in the third degree.** (1) A person commits the offense of computer fraud in the third degree if the person knowingly accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the third or fourth degree.

(2) Computer fraud in the third degree is a class C felony."

SECTION 2. Section 708-891, Hawaii Revised Statutes, is amended to read as follows:

"**[~~§~~]§708-891[~~§~~] Computer fraud in the first degree.** (1) A person commits the offense of computer fraud in the first degree if the person knowingly[~~, and with intent to defraud, accesses a computer without authorization and, by means of such conduct, obtains or exerts control over the property of another.~~

~~(2) In a prosecution for computer fraud in the first degree, it is a defense that the object of the fraud and the property obtained consists only of the use of the computer and the value of such use is not more than $300 in any one-year period.~~] accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the first degree.

[~~(3)~~] (2) Computer fraud in the first degree is a class [~~B~~] A felony."

SECTION 3. Section 708-891.5, Hawaii Revised Statutes, is amended to read as follows:

"**[~~[~~]§708-891.5[~~]~~] Computer fraud in the second degree.** (1) A person commits the offense of computer fraud in the second degree if the person knowingly[~~, and with the intent to defraud, transfers, or otherwise disposes of, to another, or obtains control of, with the intent to transfer or dispose of, any password or similar information through which a computer, computer system, or computer network may accessed.~~] accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the second degree.

(2) Computer fraud in the second degree is a class [~~C~~] B felony."

SECTION 4. Section 708-895.5, Hawaii Revised Statutes, is amended to read as follows:

"**[~~§~~]§708-895.5[~~:~~] Unauthorized computer access in the first degree.** (1) A person commits the offense of unauthorized computer access in the first degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information, and:

(a) The offense was committed for the purpose of commercial or private financial gain;

(b) The offense was committed in furtherance of any other crime;

(c) The value of the information obtained exceeds [~~$5,000;~~] $20,000; or

(d) The information has been determined by statute or rule of court to require protection against unauthorized disclosure.

(2) Unauthorized computer access in the first degree is a class [~~B~~] A felony."

SECTION 5. Section 708-895.6, Hawaii Revised Statutes, is amended to read as follows:

"**[~~§~~]§708-895.6[~~:~~] Unauthorized computer access in the second degree.** (1) A person commits the offense of unauthorized computer access in the second degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information.

(2) Unauthorized computer access in the second degree is a class [~~C~~] B felony."

SECTION 6. Section 708-895.7, Hawaii Revised Statutes, is amended to read as follows:

"**[~~[~~]§708-895.7[~~]~~] Unauthorized computer access in the third degree.** (1) A person commits the offense of unauthorized computer access in the third degree if the person knowingly accesses a computer, computer system, or computer network without authorization.

(2) Unauthorized computer access in the third degree is a [~~misdemeanor.~~] class C felony."

SECTION 7. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

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

SECTION 9. This Act shall take effect upon its approval.

Report Title:
Computer Crime

Description:
Creates a third degree of computer fraud. Clarifies and increases penalties for computer fraud in the second degree and first degree. Increases penalties for third, second and first degree unauthorized computer access, and increases the monetary threshold for first degree unauthorized computer access to $20,000. Effective January 7, 2059. (Proposed SD1)

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

TESTIMONY ON
H.B. 1788 HD1, RELATING TO COMPUTER CRIME
BY
JEANNINE SOUKI
ON BEHALF OF THE
STATE PRIVACY AND SECURITY COALITION

Sen. Clayton Hee
Chair, Senate Committee on Judiciary and Labor
Tuesday, March 27, 2012 - 10:30 AM
Hawaii State Capitol, Room 016
Honolulu, HI 96813

- The State Privacy and Security Coalition – a coalition of leading technology companies and technology trade associations – and its members strongly support the goals H.B. 1788 HD1, but are very concerned that the bill's definition of "spyware" is overly broad, inconsistent with other state laws and unless amended, would result in significant unintended consequences.

- We urge the Committee either to amend the bill's definition of "spyware" to strike the words "**or gather information about an authorized user, without authorization**" in Section 2, or else to amend the bill to add an exception that is in all the other state spyware laws in order to avoid requiring interrupting consumers' online experience by requiring that they consent to routine software functions that consumers do not care about or that benefit them (for example, by securing consumers against malware and spyware).

- The exception found in the other state spyware laws is as follows:

> Nothing in this section shall apply to any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, repair, authorized updates of software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing software proscribed under this chapter.

- An amendment is necessary because a large range of beneficial software programs collection information about an authorized user without the user's express

authorization. Examples of these beneficial programs include, but are by no means limited to:

- parental control software programs that protect children from objectionable or harmful content,
- programs that secure end user computers and networks from spyware, malware, and botnet attacks,
- programs that authenticate authorized users and/or detect intruders,
- spell check and grammar check programs that detect and fix typing errors,
- remote technical support programs that detect if user computers or networks are functioning normally.

- Either solution would make this well-intentioned bill avoid unintended consequences, and make it consistent with spyware bills adopted in the overwhelming majority of states.
- We respectfully urge the Committee to adopt either one. Thank you for the opportunity to testify, and we appreciate your consideration of our concerns.