

I Mina'Trentai Dos Na Liheslaturan Received
Bill Log Sheet

BILL NO.	SPONSOR	TITLE	DATE INTRODUCED	DATE REFERRED	CMTE REFERRED	PUBLIC HEARING DATE	DATE COMMITTEE REPORT FILED	FISCAL NOTES
319-32 (LS)	T.A. Morrison	AN ACT TO ADD A NEW ARTICLE 3 TO CHAPTER 46, TITLE 9, GUAM CODE ANNOTATED RELATIVE TO CREATING THE "COMPUTER SPYWARE PROTECTION ACT,"	04/14/14 12:32 p.m.	04/14/14	Committee on the Guam U. S. Military Relocation, Homeland Security, Veteran's Affairs, and Judiciary			



COMMITTEE ON RULES

I Mina'trentai Dos na Liheslaturan Guåhan • The 32nd Guam Legislature
155 Hesler Place, Hagåtña, Guam 96910 • www.guamlegislature.com
E-mail: roryforguam@gmail.com • Tel: (671)472-7679 • Fax: (671)472-3547

Senator
Rory J. Respicio
CHAIRPERSON
MAJORITY LEADER

Senator
Thomas C. Ada
VICE CHAIRPERSON
ASSISTANT MAJORITY LEADER

Senator
Vicente (Ben) C. Pangelinan
Member

Speaker
Judith T.P. Won Pat, Ed.D.
Member

Senator
Dennis G. Rodriguez, Jr.
Member

Vice-Speaker
Benjamin J.F. Cruz
Member

Legislative Secretary
Tina Rose Muña Barnes
Member

Senator
Frank Blas Aguon, Jr.
Member

Senator
Michael F.Q. San Nicolas
Member

Senator
V. Anthony Ada
Member
MINORITY LEADER


Senator
Aline Yamashita
Member

April 14, 2014

MEMORANDUM

To: Rennae Meno
Clerk of the Legislature

Attorney Therese M. Terlaje
Legislative Legal Counsel

From: Senator Rory J. Respicio 
Chairperson of the Committee on Rules

Subject: Referral of Bill No. 319-32(LS)

As the Chairperson of the Committee on Rules, I am forwarding my referral of **Bill No. 319-32(LS)**.

Please ensure that the subject bill is referred, in my name, to the respective committee, as shown on the attachment. I also request that the same be forwarded to all members of *I Mina'trentai Dos na Liheslaturan Guåhan*.

Should you have any questions, please feel free to contact our office at 472-7679.


Si Yu'os Ma'åse!

Attachment

I MINA' TRENTAI DOS NA LIHESLATURAN GUÅHAN
2014 (SECOND) Regular Session

Bill No. 319-32 (LS)

Introduced by:

T. A. Morrison 

**AN ACT TO ADD A NEW ARTICLE 3 TO CHAPTER 46,
TITLE 9, GUAM CODE ANNOTATED RELATIVE TO
CREATING THE “COMPUTER SPYWARE PROTECTION
ACT,”**

1 **BE IT ENACTED BY THE PEOPLE OF GUAM:**

2

3 **Section 1.** A new Article 3 is *added* to Chapter 46 of 9GCA to read:

4

5

“Article 3

6

COMPUTER SPYWARE PROTECTION ACT

7

8 **§46.301. Title.** This Act may be cited as the “Computer Spyware Protection Act.”

9

10 **§46.302. Legislative Intent.** *I Liheslaturan Guåhan* finds that spyware is a problem that
11 adversely affects nearly every computer connected to the internet. Spyware is a catch-all
12 term for computer programs that can track computer users' movements online. There are
13 hundreds of programs that range from innocuous “ad-ware,” which generates pop-up
14 advertisements, to more dangerous programs that can record a user’s keystrokes to gather
15 personal information such as credit card numbers and passwords without their knowledge
16 and forward this information to another entity without the consumer’s consent. Spyware is
17 a serious problem that can create substantial privacy risks, increase the risk of identity

2014 APR 14 PM 12:32



1 theft, and cause serious degradation to personal and business computers that can cost
2 millions of dollars in lost productivity.

3
4 It is the intent of the Legislature to protect owners and operators of computers in Guam from
5 the use of spyware and malware that is deceptively or surreptitiously installed on the
6 owner's or the operator's computer.

7
8 **§46.303. Definitions**

9
10 (1) "Cause to be copied" means to distribute or transfer computer software, or any
11 component thereof. Such term shall not include providing:

12
13 (a) a transmission, routing, provision of intermediate temporary storage, or
14 caching of software;

15
16 (b) a storage or hosting medium, such as a compact disk, web site, or
17 computer server through which the software was distributed by a third party;
18 or

19
20 (c). an information location tool, such as a directory, index, reference,
21 pointer, or hypertext link, through which the user of the computer located
22 the software.

23
24 (2) "Computer software" means a sequence of instructions written in any programming
25 language that is executed on a computer. "Computer software" does not include a data
26 component of a web page that is not executable independently of the web page.

1 (3) "Computer virus" means a computer program or other set of instructions that is
2 designed to degrade the performance of or disable a computer or computer network and is
3 designed to have the ability to replicate itself on other computers or computer networks
4 without the authorization of the owners of those computers or computer networks.
5

6 (4) "Damage" means any significant impairment to the integrity or availability of data,
7 software, a system, or information.
8

9 (5) "Execute," when used with respect to computer software, means the performance of
10 the functions or the carrying out of the instructions of the computer software.
11

12 (6) "Intentionally deceptive" means any of the following:
13

14 a. An intentionally and materially false or fraudulent statement.
15

16 b. A statement or description that intentionally omits or misrepresents
17 material information in order to deceive an owner or operator of a computer.
18

19 c. An intentional and material failure to provide a notice to an owner or
20 operator regarding the installation or execution of computer software for the
21 purpose of deceiving the owner or operator.
22

23 (7) "Internet" means the global information system that is logically linked together by a
24 globally unique address space based on the internet protocol (IP), or its subsequent
25 extensions, and that is able to support communications using the transmission control
26 protocol/internet protocol (TCP/IP) suite, or its subsequent extensions, or other IP-
27 compatible protocols, and that provides, uses, or makes accessible, either publicly or

1 privately, high-level services layered on the communications and related infrastructure
2 described in this subsection.

3
4 (8) "Owner or operator" means the owner or lessee of a computer, or a person using such
5 computer with the owner or lessee's authorization, but does not include a person who
6 owned a computer prior to the first retail sale of the computer.

7
8 (9) "Message" means a graphical or text communication presented to an authorized user of
9 a computer.

10
11 (10) "Person" means any individual, partnership, corporation, limited liability company,
12 or other organization, or any combination thereof.

13
14 (11) "Personally identifiable information" means any of the following information if it
15 allows the entity holding the information to identify the owner or operator of a computer:

16
17 a. The first name or first initial in combination with the last name.

18
19 b. A home or other physical address including street name.

20
21 c. Personal identification code in conjunction with a password required to
22 access an identified account, other than a password, personal identification
23 number or other identification number transmitted by an authorized user to
24 the issuer of the account or its agent.

25
26 d. Social security number, tax identification number, driver's license number,
27 passport number, or any other government-issued identification number.

1 e. Account balance, overdraft history, or payment history that personally
2 identifies an owner or operator of a computer.
3

4 **§46.304. Prohibitions, Use of Software**

5 It is unlawful for a person who is not an owner or operator of a computer to cause
6 computer software to be copied on such computer knowingly or with conscious avoidance
7 of actual knowledge or willfully, and to use such software to do any of the following:
8

9 (1) Modify, through intentionally deceptive means, settings of a computer that control any
10 of the following:
11

12 a. The web page that appears when an owner or operator launches an Internet
13 browser or similar computer software used to access and navigate the
14 Internet.
15

16 b. The default provider or web proxy that an owner or operator uses to access
17 or search the Internet.
18

19 c. An owner's or an operator's list of bookmarks used to access web pages.
20

21 (2) Collect, through intentionally deceptive means, personally identifiable information
22 through any of the following means:
23

24 a. The use of a keystroke-logging function that records all or substantially all
25 keystrokes made by an owner or operator of a computer and transfers that
26 information from the computer to another person.
27

1 b. In a manner that correlates personally identifiable information with data
2 regarding all or substantially all of the Web sites visited by an owner or
3 operator, other than Web sites operated by the person providing such
4 software, if the computer software was installed in a manner designed to
5 conceal from all authorized users of the computer the fact that the software is
6 being installed..

7
8 c. By extracting from the hard drive of an owner's or an operator's computer,
9 an owner's or an operator's social security number, tax identification number,
10 driver's license number, passport number, any other government-issued
11 identification number, account balances, or overdraft history for a purpose
12 unrelated to any of the purposes of the software or service described to an
13 authorized user.

14
15 (3) Prevent, through intentionally deceptive means, an owner's or an operator's reasonable
16 efforts to block the installation of or execution of, or to disable, computer software by
17 causing computer software that the owner or operator has properly removed or disabled to
18 automatically reinstall or reactivate on the computer without the authorization of an
19 authorized user.

20
21 (4) Intentionally misrepresent that computer software will be uninstalled or disabled by an
22 owner's or an operator's action.

23
24 (5) Through intentionally deceptive means, remove, disable, or render inoperative
25 security, antispyware, or antivirus computer software installed on an owner's or an
26 operator's computer.

27
28 (6) Enable use of an owner's or an operator's computer to do any of the following:

1
2 a. Accessing or using a modem or Internet service for the purpose of causing
3 damage to an owner's or an operator's computer or causing an owner or
4 operator , or a third party affected by such conduct to incur financial charges
5 for a service that the owner or operator did not authorize.

6
7 b. Opening multiple, sequential, stand-alone messages in an owner's or an
8 operator's computer without the authorization of an owner or operator and
9 with knowledge that a reasonable computer user could not close the messages
10 without turning off the computer or closing the software application in which
11 the messages appear; provided that this paragraph shall not apply to
12 communications originated by the computer's operating system, originated
13 by a software application that the user chooses to activate, originated by a
14 service provider that the user chooses to use, or presented for any of the
15 purposes described in §46.306.

16
17 c. Transmitting or relaying commercial electronic mail or a computer virus
18 from the computer, where the transmission or relaying is initiated by a person
19 other than the authorized user and without the authorization of an authorized
20 user.

21
22 (7) Modify any of the following settings related the computer's access to, or use of, the
23 Internet:

24
25 a. Settings that protect information about an owner or operator for the
26 purpose of taking personally identifiable information of the owner or
27 operator.
28

1 b. Security settings for the purpose of causing damage to a computer.

2
3 c. Settings that protect the computer from the uses identified in subsection (6)
4 of this section.

5
6 (8) Prevent, without the authorization of an owner or operator, an owner's or an operator's
7 reasonable efforts to block the installation of, or to disable, computer software by doing
8 any of the following:

9
10 a. Presenting the owner or operator with an option to decline installation of
11 computer software with knowledge that, when the option is selected by the
12 authorized user, the installation nevertheless proceeds.

13
14 b. Falsely representing that computer software has been disabled.

15
16 c. Requiring in an intentionally deceptive manner the user to access the
17 Internet to remove the software with knowledge or reckless disregard of the
18 fact that the software frequently operates in a manner that prevents the user
19 from accessing the Internet.

20
21 d. Changing the name, location or other designation information of the
22 software for the purpose of preventing an authorized user from locating the
23 software to remove it.

24
25 e. Using randomized or intentionally deceptive filenames, directory folders,
26 formats, or registry entries for the purpose of avoiding detection and removal
27 of the software by an authorized user.

1 f. Causing the installation of software in a particular computer directory or
2 computer memory for the purpose of evading authorized users' attempts to
3 remove the software from the computer;

4
5 g. Requiring, without the authority of the owner of the computer, that an
6 authorized user obtain a special code or download software from a third party
7 to uninstall the software.

8
9 **§46.305. Other Prohibitions**

10 It is unlawful for a person who is not an owner or operator of a computer to do any of the
11 following with regard to the computer:

12
13 (1) Induce an owner or operator to install a computer software component onto the
14 owner's or the operator's computer by intentionally misrepresenting that installing
15 computer software is necessary for security or privacy reasons or in order to open, view,
16 or play a particular type of content.

17
18 (2) Using intentionally deceptive means to cause the execution of a computer software
19 component with the intent of causing the computer to use such component in a manner
20 that violates any other provision of this Article.

21
22 **§46.306. Exceptions**

23 §§46.304 and 46.305 shall not apply to the monitoring of, or interaction with, an owner's
24 or an operator's Internet or other network connection, service, or computer, by a
25 telecommunications carrier, cable operator, computer hardware or software provider, or
26 provider of information service or interactive computer service for network or computer
27 security purposes, diagnostics, technical support, maintenance, repair, network
28 management, authorized updates of computer software or system firmware, authorized

1 remote system management, or detection or prevention of the unauthorized use of or
2 fraudulent or other illegal activities in connection with a network, service, or computer
3 software, including scanning for and removing computer software prescribed under this
4 Article.

5

6 **§46.307. Remedies**

7 (1) The attorney general, an Internet service provider or software company that expends
8 resources in good faith assisting authorized users harmed by a violation of this Article, or
9 a trademark owner whose mark is used to deceive authorized users in violation of this
10 Article, may bring a civil action against a person who violates any provision of this
11 Article to recover actual damages, liquidated damages of at least one thousand dollars per
12 violation of this Article, not to exceed one million dollars for a pattern or practice of such
13 violations, attorney fees, and costs.

14

15 (2) The court may increase a damage award to an amount equal to not more than three
16 times the amount otherwise recoverable under subsection 1 if the court determines that the
17 defendant committed the violation willfully and knowingly.

18

19 (3) The court may reduce liquidated damages recoverable under subsection 1, to a
20 minimum of one hundred dollars, not to exceed one hundred thousand dollars for each
21 violation if the court finds that the defendant established and implemented practices and
22 procedures reasonably designed to prevent a violation of this Article.

23

24 (4) In the case of a violation of §46.304(6)a. that causes a telecommunications carrier or
25 provider of voice over internet protocol service to incur costs for the origination,
26 transport, or termination of a call triggered using the modem or Internet-capable device of
27 a customer of such telecommunications carrier or provider as a result of such violation,

the telecommunications carrier may bring a civil action against the violator to recover any or all of the following—

a. the charges such carrier or provider is obligated to pay to another carrier or to an information service provider as a result of the violation, including but not limited to charges for the origination, transport or termination of the call;

b. costs of handling customer inquiries or complaints with respect to amounts billed for such calls;

c. costs and a reasonable attorneys' fee; and

d. an order to enjoin the violation.

(5) For purposes of a civil action under paragraphs (1), (2) and (3) any single action or conduct that violates more than one paragraph of this Article shall be considered multiple violations based on the number of such paragraphs violated.

§46.308. Good Samaritan

(1) No provider of computer software or of an interactive computer service may be held liable for identifying, naming, removing, disabling, or otherwise affecting a computer program through any action voluntarily undertaken, or service provided, where the provider:

a. Intends to identify accurately, prevent the installation or execution of, remove, or disable another computer program on a computer of a customer of such provider; and

1 b. Reasonably believes the computer program exhibits behavior that violates
2 this act; and

3
4 c. Notifies the authorized user and obtains clear and conspicuous consent
5 before undertaking such action or providing such service.
6

7 (2) A provider of computer software or interactive computer service is entitled to
8 protection under this section only if such provider:
9

10 a. Has established internal practices and procedures to evaluate computer
11 programs reasonably designed to determine whether or not a computer
12 program exhibits behavior that violates this act; and
13

14 b. Has established a process for managing disputes and inquiries regarding
15 misclassification or false positive identifications of computer programs.

16 Nothing in this section is intended to limit the ability of the Attorney General,
17 or a district attorney to bring an action against a provider of computer
18 software or of an interactive computer service.
19