

FOURTEENTH CONGRESS OF THE )  
REPUBLIC OF THE PHILIPPINES )  
Second Regular Session )

9 JAN 28 110:40

SENATE

RECEIVED BY: *[Signature]*

S. NO. 3023

---

Introduced by Senator Antonio "Sonny" F. Trillanes IV

---

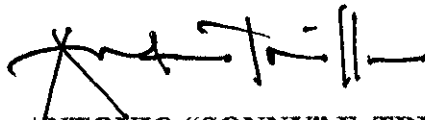
**EXPLANATORY NOTE**

It is the duty of the State to protect its citizens from falling prey to unscrupulous individuals who employ technology through deceitful and unfair ways. This bill aims to protect consumers from the use of spyware and malware that are deceptively or surreptitiously installed on their computers.

No existing law provides for the regulation of computer spyware. This bill would prohibit a person or entity other than the authorized user of a computer owned by a person with actual knowledge, conscious avoidance of actual knowledge, or willfully, causing computer software to be copied onto the computer and using the software to: (1) take control of the computer, as specified; (2) modify certain settings relating to the computer's access to or use of the Internet, as specified; (3) collect, through intentionally deceptive means, personally identifiable information, as defined; (4) prevent, without authorization, an authorized user's reasonable efforts to block the installation of or disable software, as specified; (5) intentionally misrepresent that the software will be uninstalled or disabled by an authorized user's action, or (6) through intentionally deceptive means, remove, disable, or render inoperative security, anti-spyware, or antivirus software installed on the computer.

Furthermore, this measure would also prohibit a person or entity who is not an authorized user from inducing an authorized user to install a software component by intentionally misrepresenting that it is necessary for security or privacy or in order to open, view, or play a particular type of content. It would prohibit a person or entity who is not an authorized user from deceptively causing the copying and execution on the computer of software components with the intent of causing an authorized user to use the components in a way that violates any of these prohibitions.

In view of the foregoing, the passage of this bill is earnestly sought.



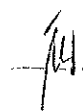
ANTONIO "SONNY" F. TRILLANES IV  
Senator

FOURTEENTH CONGRESS OF THE )  
REPUBLIC OF THE PHILIPPINES )  
Second Regular Session )

9 JAN 28 AM 10:40

SENATE

S. NO. 3023

RECEIVED BY: 

---

Introduced by Senator Antonio "Sonny" F. Trillanes IV

---

AN ACT  
PROTECTING CONSUMERS BY REGULATING THE UNAUTHORIZED AND  
DECEPTIVE INSTALLATION OF SPYWARE IN COMPUTERS, PROVIDING  
PENALTIES THEREFOR, AND FOR OTHER PURPOSES

*Be it enacted by the Senate and the House of Representatives of the Philippines in Congress assembled:*

1           **SECTION 1. *Short Title.*** – This Act shall be known as the "*Consumer Protection*  
2 *Against Computer Spyware Act of 2009*".

3  
4           **SEC. 2. *Purpose.*** – It is the intent of this Act to protect consumers from the use of  
5 spyware and malware that are deceptively or surreptitiously installed on their computers.

6  
7           **SEC. 3. *Definition of Terms.*** – For the purposes of this Act, the following terms have the  
8 following meaning:

9           a. "*Advertisement*" means a communication, the primary purpose of which is the commercial  
10 promotion of a commercial product or service, including content on an Internet Web site  
11 operated for a commercial purpose;

12           b. "*Authorized user,*" with respect to a computer, means a person who owns or is authorized by  
13 the owner or on to use the computer. An "authorized user" does not include a person or  
14 entity that has obtained authorization to use the computer solely through the use of an end  
15 user license agreement;

16           c. "*Computer software*" means a sequence of instructions written in any programming language  
17 that is executed on a computer;

18           d. "*Computer virus*" means a computer program or other set of instructions that is designed to  
19 degrade the performance of or disable a computer or computer network and is designed to

- 1 have the ability to replicate itself on other computers or computer networks without the  
2 authorization of the owners of those computers or computer networks;
- 3 e. "*Consumer*" means an individual who resides in this state and who uses the computer in  
4 question primarily for personal, family, or household purposes;
- 5 f. "*Damage*" means any significant impairment to the integrity or availability of data,  
6 software, a system, or information;
- 7 g. "*Execute*," when used with respect to computer software means the performance of the  
8 functions or the carrying out of the instructions of the computer software;
- 9 h. "*Intentionally deceptive*" means any of the following:
- 10 1. By means of an intentionally and materially false or fraudulent statement;
- 11 2. By means of a statement or description that intentionally omits or misrepresents  
12 material information in order to deceive the consumer; and
- 13 3. By means of an intentional and material failure to provide any notice to an authorized  
14 user regarding the download or installation of software in order to deceive the  
15 consumer;
- 16 i. "*Internet*" means the global information system that is logically linked together by a globally  
17 unique address space based on the Internet Protocol (IP), or its subsequent extensions, and  
18 that is able to support communications using the Transmission Control Protocol/Internet  
19 Protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols, and  
20 that provides, uses, or makes accessible, either publicly or privately, high level services  
21 layered on the communications and related infrastructure described in this subdivision;
- 22 j. "*Person*" means any individual, partnership, corporation, company, or other organization, or  
23 any combination thereof;
- 24 k. "*Personally identifiable information*" means any of the following:
- 25 1. First name or first initial in combination with last name;
- 26 2. Credit or debit card numbers or other financial account numbers;
- 27 3. A password or personal identification number required to access an identified financial  
28 account;
- 29 4. Social Security number; and

1 5. Any of the following information in a form that personally identifies an authorized user:

- 2 (A) Account balances;
- 3 (B) Overdraft history;
- 4 (C) Payment history;
- 5 (D) A history of Web sites visited;
- 6 (E) Home address;
- 7 (F) Work address; and
- 8 (G) A record of a purchase or purchases.

9  
10 **SEC. 4. Prohibitions Against Unauthorized Users. –**

11 a. A person or entity that is not an authorized user, shall not, with actual knowledge, with  
12 conscious avoidance of actual knowledge, or willfully, cause computer software to be copied  
13 onto the computer of a consumer in this state and use the software to do any of the following:

14 1. Modify, through intentionally deceptive means, any of the following settings related to  
15 the computer's access to, or use of the Internet:

16 A. The page that appears when an authorized user launches an Internet browser or  
17 similar software program used to access and navigate the Internet;

18 B. The default provider or Web proxy the authorized user uses to access or search the  
19 Internet; and

20 C. The authorized user's list of bookmarks used to access Web pages;

21 2. Collect, through intentionally deceptive means, personally identifiable information that  
22 meets any of the following criteria:

23 A. It is collected through the use of a keystroke-logging function that records all  
24 keystrokes made by an authorized user who uses the computer and transfers that  
25 information from the computer to another person;

26 B. It includes all or substantially all of the Web sites visited by an authorized user,  
27 other than Web sites of the provider of the software, if the computer software was  
28 installed in a manner designed to conceal from all authorized users of the  
29 computer the fact that the software is being installed; and

1 C. It is a data element that is extracted from the consumer's computer hard drive for a  
2 purpose wholly unrelated to any of the purposes of the software or service described  
3 to an authorized user;

4 3. Prevent, without the authorization of an authorized user, through intentionally  
5 deceptive means, an authorized user's reasonable efforts to block the installation of,  
6 or to disable, software, by causing software that the authorized user has properly  
7 removed or disabled to automatically reinstall or reactivate on the computer without  
8 the authorization of an authorized user;

9 4. Intentionally misrepresent that software will be uninstalled or disabled by an  
10 authorized user's action, with knowledge that the software will not be so uninstalled  
11 or disabled; and

12 5. Through intentionally deceptive means, remove, disable, or render inoperative  
13 security, anti-spyware, or antivirus software installed on the computer.

14 b. A person or entity that is not an authorized user shall not, with actual knowledge, with  
15 conscious avoidance of actual knowledge, or willfully, cause computer software to be  
16 copied onto the computer of a consumer in this state and use the software to do any of the  
17 following:

18 1. Take control of the consumer's computer by doing any of the following:

19 A. Transmitting or relaying commercial electronic mail or a computer virus from the  
20 consumer's computer, where the transmission or relaying is initiated by a person  
21 other than the authorized user and without the authorization of an authorized user;

22 B. Accessing or using the consumer's modem or Internet service for the purpose of  
23 causing damage to the consumer's computer or of causing an authorized user to  
24 incur financial charges for a service that is not authorized by an authorized user;

25 C. Using the consumer's computer as part of an activity performed by a group of  
26 computers for the purpose of causing damage to another computer, including, but  
27 not limited to, launching a denial of service attack; and

28 D. Opening multiple, sequential, stand-alone advertisements in the consumer's  
29 Internet browser without the authorization of an authorized user and with

- 1 knowledge that a reasonable computer user cannot close the advertisements  
2 without turning off the computer or closing the consumer's Internet browser;
- 3 2. Modify any of the following settings related to the computer's access to, or use of, the  
4 Internet:
- 5 A. An authorized user's security or other settings that protect information about the  
6 authorized user for the purpose of stealing personal information of an authorized  
7 user; and
- 8 B. The security settings of the computer for the purpose of causing damage to one  
9 or more computers;
- 10 3. Prevent, without the authorization of an authorized user, an authorized user's  
11 reasonable efforts to block the installation of, or to disable, software, by doing any of  
12 the following:
- 13 A. Presenting the authorized user with an option to decline installation of software  
14 with knowledge that, when the option is selected by the authorized user, the  
15 installation nevertheless proceeds; and
- 16 B. Falsely representing that software has been disabled.
- 17 c. A person or entity, who is not an authorized user, shall not do any of the following with  
18 regard to the computer of a consumer:
- 19 1. Induce an authorized user to install a software component onto the computer by  
20 intentionally misrepresenting that installing software is necessary for security or  
21 privacy reasons or in order to open, view, or play a particular type of content; and
- 22 2. Deceptively causing the copying and execution on the computer of a computer software  
23 component with the intent of causing an authorized user to use the component in a way  
24 that violates any other provision of this section.
- 25 d. Nothing in this section shall apply to any monitoring of, or interaction with, a subscriber's  
26 Internet or other network connection or service, or a protected computer, by a  
27 telecommunications carrier, cable operator, computer hardware or software provider, or  
28 provider of information service or interactive computer service for network or computer  
29 security purposes, diagnostics, technical support, repair, authorized updates of software or

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

5  
6 **SEC. 5. Penal Clause.** – A person who commits any of the prohibited acts enumerated  
7 above shall be punishable with a penalty of imprisonment for a period of not exceeding six (6)  
8 months or a fine of not less than Fifty Thousand Pesos (Php 50,000.00) but not more than One  
9 Hundred Thousand Pesos (Php 100,000.00), or both, at the discretion of the court.

10  
11 **SEC. 6. Implementing Rules and Regulations.** – The DOTC shall, within sixty (60) days  
12 after the approval of this Act, prepare and issue the necessary guidelines to implement the same.

13  
14 **SEC. 7. Separability Clause.** If any provision or part hereof is held invalid or  
15 unconstitutional, the remainder of the law or the provision not otherwise affected shall remain  
16 valid and subsisting.

17  
18 **SEC. 8. Repealing Clause.** Any law, presidential decree or issuance, executive order,  
19 letter of instruction, administrative order, rule or regulation contrary to, or inconsistent with, the  
20 provisions of this Act, is hereby repealed, modified, or amended accordingly.

21  
22 **SEC. 9. Effectivity Clause.** This Act shall take effect fifteen (15) days after its complete  
23 publication in at least two (2) newspapers of general circulation.

Approved,