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

SENATE

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)

SENATE

S. NO. 3023

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:

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

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

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

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

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

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

d. *"Computer virus"* means a computer program or other set of instructions that is designed to degrade the performance of or disable a computer or computer network and is designed to have the ability to replicate itself on other computers or computer networks without the authorization of the owners of those computers or computer networks;

e. *"Consumer"* means an individual who resides in this state and who uses the computer in question primarily for personal, family, or household purposes;

f.. *"Damage"* means any significant impairment to the integrity or availability of data, software, a system, or information;

g. *"Execute,"* when used with respect to computer software means the performance of the functions or the carrying out of the instructions of the computer software;

h. *"Intentionally deceptive"* means any of the following:

1. By means of an intentionally and materially false or fraudulent statement;
2. By means of a statement or description that intentionally omits or misrepresents material information in order to deceive the consumer; and
3. By means of an intentional and material failure to provide any notice to an authorized user regarding the download or installation of software in order to deceive the consumer;

i. *"Internet"* means the global information system that is logically linked together by a globally unique address space based on the Internet Protocol (IP), or its subsequent extensions, and that is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols, and that provides, uses, or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described in this subdivision;

j. *"Person"* means any individual, partnership, corporation, company, or other organization, or any combination thereof;

k. *"Personally identifiable information"* means any of the following:

1. First name or first initial in combination with last name;
2. Credit or debit card numbers or other financial account numbers;
3. A password or personal identification number required to access an identified financial account;
4. Social Security number; and

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

(A) Account balances;

(B) Overdraft history;

(C) Payment history;

(D) A history of Web sites visited;

(E) Home address;

(F) Work address; and

(G) A record of a purchase or purchases.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

D. Opening multiple, sequential, stand-alone advertisements in the consumer's Internet browser without the authorization of an authorized user and with knowledge that a reasonable computer user cannot close the advertisements without turning off the computer or closing the consumer's Internet browser;

2. Modify any of the following settings related to the computer's access to, or use of, the Internet:

A. An authorized user's security or other settings that protect information about the authorized user for the purpose of stealing personal information of an authorized user; and

B. The security settings of the computer for the purpose of causing damage to one or more computers;

3. Prevent, without the authorization of an authorized user, an authorized user's reasonable efforts to block the installation of, or to disable, software, by doing any of the following:

A. Presenting the authorized user with an option to decline installation of software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds; and

B. Falsely representing that software has been disabled.

c. A person or entity, who is not an authorized user, shall not do any of the following with regard to the computer of a consumer:

1. Induce an authorized user to install a software component onto the computer by intentionally misrepresenting that installing software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content; and

2. Deceptively causing the copying and execution on the computer of a computer software component with the intent of causing an authorized user to use the component in a way that violates any other provision of this section.

d. 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 Act.

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

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

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

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

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

Approved,