

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

8 APR 17 P 3 11

SENATE  
S. No. 2176

RECEIVED BY: HA

---

Introduced by Senator Miriam Defensor Santiago

---

EXPLANATORY NOTE

Grayware (or greyware) is a general classification for applications that behave in a manner that is annoying or undesirable. Grayware encompasses spyware, adware, dialers, joke programs, remote access tools, and any other unwelcome files and programs apart from viruses that can harm the performance of computers on your network. The term has been in use since at least as early as September 2004.

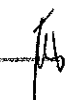
Grayware refers to applications or files that are not classified as viruses or trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization. Often grayware performs a variety of undesired and threatening actions such as irritating users with pop-up windows, logging user key strokes, and exposing computer vulnerabilities to attack. This bill aims to address the growing problem of grayware among computer users in the Philippines.

*Miriam Defensor Santiago*  
MIRIAM DEFENSOR SANTIAGO

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

3 APR 17 2015

SENATE  
S. No. 2176

RECEIVED BY: 

---

Introduced by Senator Miriam Defensor Santiago

---

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21

AN ACT  
PROTECTING CONSUMERS FROM COMPUTER GRAYWARE

*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 Grayware Act of 2008.”

SECTION 2. *Definition of terms.* – As used in this Act, the term–

(A) "Advertisement" is any 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, is a person who owns or leases a computer or is authorized by the owner or lessee to use the computer. Authorized user shall 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" is a sequence of instructions written in any programming language that is executed on a computer;

(D) "Computer virus" or malware is 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" is an individual who uses a computer for whatever purpose;

1 (F) "Grayware" refers to applications or files that are not classified as viruses or trojan  
2 horse programs, but can still negatively affect the performance of the computers on your network  
3 and introduce significant security risks, it includes spyware and adware;

4 (1) "Spyware" refers to software that installs components on a computer for the  
5 purpose of recording Web surfing habits (primarily for marketing purposes). Spyware  
6 sends this information to its author or to other interested parties when the computer is  
7 online;

8 (2) "Adware" is software that displays advertising banners on Web browsers such  
9 as Internet Explorer and Mozilla. While not categorized as malware, many users consider  
10 adware invasive. Adware programs often create unwanted effects on a system, such as  
11 annoying popup ads and the general degradation in either network connection or system  
12 performance. Adware programs are typically installed as separate programs that are  
13 bundled with certain free software.

14 (G) "Execute," when used with respect to computer software, means the performance of  
15 the functions or the carrying out of the instructions of the computer software;

16 (H) "Intentionally deceptive" is any of the following:

17 (1) By means of an intentionally and materially false or fraudulent statement;

18 (2) By means of a statement or description that intentionally omits or  
19 misrepresents material information in order to deceive the consumer;

20 (3) By means of an intentional and material failure to provide any notice to an  
21 authorized user regarding the download or installation of software in order to deceive the  
22 consumer;

23 (I) "Internet" is the global information system that is linked together by a globally unique  
24 address space based on the Internet protocol, or its subsequent extensions, and that is able to  
25 support communications using the Transmission Control Protocol/Internet Protocol suite, or its  
26 subsequent extensions, or other Internet protocol-compatible protocols, and that provides, uses,  
27 or makes accessible, either publicly or privately, high level services layered on the  
28 communications and related infrastructure described in this subdivision;

1 (J) "Person" refers to any individual, partnership, corporation, or any kind of  
2 organization, or any combination thereof;

3 (K) "Damage" refers to any significant impairment to the integrity, functionality or  
4 availability of data, software, a computer, or a system;

5 (L) "Personally identifiable information" is any of the following:

6 (1) A first name or first initial in combination with last name;

7 (2) Any credit or debit card numbers or other financial account numbers;

8 (3) A password or personal identification number required to access an identified  
9 financial account;

10 (4) A Social Security number;

11 (5) Any of the following information in a form that personally identifies an  
12 authorized user:

13 (a) Account balance;

14 (b) Overdraft history;

15 (c) Payment history;

16 (d) History of web sites visited;

17 (e) Home address;

18 (f) Work address;

19 (g) Record of a purchase or purchases.

20 SECTION 3. *Prohibited Acts.* – A person or entity that is not an authorized user shall not,  
21 with actual knowledge, with conscious avoidance of actual knowledge, or willfully, cause  
22 computer software to be copied onto the computer of a consumer and use the software to do any  
23 of the following:

24 (A) Modify, through intentionally deceptive means, any of the settings related to the  
25 computer's access to, or use of, the Internet;

26 (B) Collect, through intentionally deceptive means, personally identifiable information  
27 that meets any of the following criteria:

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

4 (2) It includes all or substantially all of the web sites visited by an authorized user,  
5 other than web sites of the provider of the software, if the computer software was  
6 installed in a manner designed to conceal from all authorized users of the computer the  
7 fact that the software is being installed;

8 (3) It is a data element described in paragraph K of Section 2, that is extracted  
9 from the consumer's computer hard drive for a purpose wholly unrelated to any of the  
10 purposes of the software or service described to an authorized user.

11 (C) Prevent, without the authorization of an authorized user, through intentionally  
12 deceptive means, an authorized user's reasonable efforts to block the installation of, or to disable,  
13 software, by causing software that the authorized user has properly removed or disabled to  
14 automatically reinstall or reactivate on the computer without the authorization of an authorized  
15 user;

16 (D) Intentionally misrepresent that software will be uninstalled or disabled by an  
17 authorized user's action, with knowledge that the software will not be so uninstalled or disabled;

18 (E) Through intentionally deceptive means, remove, disable, or render inoperative  
19 security, antispyware, or antivirus software installed on the computer.

20 (F) Take control of the consumer's computer by doing any of the following:

21 (1) Transmitting or relaying commercial electronic mail or a computer virus from  
22 the consumer's computer, where the transmission or relaying is initiated by a person other  
23 than the authorized user and without the authorization of an authorized user;

24 (2) Accessing or using the consumer's modem or Internet service for the purpose  
25 of causing damage to the consumer's computer or of causing an authorized user to incur  
26 financial charges for a service that is not authorized by an authorized user;

27 (3) Using the consumer's computer as part of an activity performed by a group of  
28 computers for the purpose of causing damage to another computer, including, but not  
29 limited to, launching a denial of service attack;

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

5           (G) Modify any of the following settings related to the computer's access to, or use of, the  
6 Internet:

7           (1) An authorized user's security or other settings that protect information about  
8 the authorized user for the purpose of obtaining personally identifiable information of an  
9 authorized user;

10           (2) The security settings of the computer for the purpose of causing damage to  
11 one or more computers;

12           (H) Prevent, without the authorization of an authorized user, an authorized user's  
13 reasonable efforts to block the installation of, or to disable, software, by doing any of the  
14 following:

15           (1) Presenting the authorized user with an option to decline installation of  
16 software with knowledge that, when the option is selected by the authorized user, the  
17 installation nevertheless proceeds;

18           (2) Falsely representing that software has been disabled;

19           (3) Causing the installation of computer software in an intentionally deceptive  
20 manner so as to evade an authorized user's attempts to remove the computer software  
21 from the computer;

22           (I) Remove, disable, or render inoperative, through intentionally deceptive means,  
23 security, antispymware, or antivirus software installed on the computer;

24           (J) Induce an authorized user to install a software component onto the computer by  
25 misrepresenting that installing software is necessary for security or privacy reasons or in order to  
26 open, view, or play a particular type of content;

27           (K) Deceptively causing the copying and execution on the computer of a computer  
28 software component with the intent of causing an authorized user or computer to use the  
29 component in a way that violates any other provision of this section;

1           SECTION 4. *Exceptions.* – Nothing in the preceding section shall apply to any  
2 monitoring of, or interaction with, an authorized user's Internet or other network connection or  
3 service, or a protected computer, by a telecommunications carrier, cable operator, computer  
4 hardware or software provider, or provider of information service or interactive computer  
5 authorized service for authorized network or computer security purposes, authorized diagnostics,  
6 technical support, network management, authorized maintenance or repair, authorized updates of  
7 software or system firmware, authorized remote system management, or authorized detection or  
8 prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a  
9 network, service, or computer software, including scanning for and removing software  
10 proscribed under this Act.

11           SECTION 5. *Separability Clause.* – If any provision, or part hereof is held invalid or  
12 unconstitutional, the remainder of the law or the provision not otherwise affected shall remain  
13 valid and subsisting.

14           SECTION 6. *Repealing Clause.* – Any law, presidential decree or issuance, executive  
15 order, letter of instruction, administrative order, rule or regulation contrary to or inconsistent  
16 with, the provisions of this Act is hereby repealed, modified, or amended accordingly.

17           SECTION 7. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its  
18 publication in at least two (2) newspapers of general circulation.

19           Approved,