

## THE GENERAL ASSEMBLY OF PENNSYLVANIA

## SENATE BILL

No. 711 Session of  
2005

INTRODUCED BY GORDNER, WONDERLING, C. WILLIAMS, RAFFERTY, COSTA,  
CORMAN, WOZNIAK, PIPPY, PICCOLA, VANCE, LOGAN, ERICKSON,  
WAUGH, RHOADES, BOSCOLA, TARTAGLIONE, KITCHEN, THOMPSON,  
O'PAKE, GREENLEAF, STACK AND ROBBINS, JUNE 3, 2005

SENATOR WONDERLING, COMMUNICATIONS AND TECHNOLOGY, AS AMENDED,  
JUNE 13, 2005

## AN ACT

1 Providing for the protection of consumers from having spyware  
2 deceptively installed on their computers, ~~for enforcement and~~ <—  
3 ~~for civil relief.~~ AND FOR CRIMINAL AND CIVIL ENFORCEMENT. <—

## 4 TABLE OF CONTENTS

- 5 Section 1. Short title.  
6 Section 2. Definitions.  
7 Section 3. Computer spyware prohibitions.  
8 Section 4. Control or modification.  
9 Section 5. Misrepresentation and deception.  
10 Section 6. Nonapplicability.  
11 Section 7. Enforcement.  
12 Section 8. Civil relief.  
13 Section 9. Effective date.

14 The General Assembly of the Commonwealth of Pennsylvania  
15 hereby enacts as follows:

16 Section 1. Short title.

17 This act shall be known and may be cited as the Consumer

1 Protection Against Computer Spyware Act.

2 Section 2. Definitions.

3 The following words and phrases when used in this act shall  
4 have the meanings given to them in this section unless the  
5 context clearly indicates otherwise:

6 ~~"Advertisement." A communication, the primary purpose of~~ <—  
7 ~~which is the commercial promotion of a commercial product or~~  
8 ~~service, including content on an Internet website operated for a~~  
9 ~~commercial purpose.~~

10 "Authorized user." With respect to a computer, a person who  
11 owns or is authorized by the owner or lessee to use the  
12 computer.

13 "Cause to be copied." To distribute ~~or transfer~~, TRANSFER OR <—  
14 PROCURE THE COPYING OF computer software or any component  
15 thereof. The term shall not include the following:

16 (1) Transmission, routing, provision of intermediate  
17 temporary storage or caching of software.

18 (2) A storage or hosting medium, such as a compact disc,  
19 Internet website or computer server, through which the  
20 software was distributed by a third party.

21 (3) An information location tool, such as a directory,  
22 index, reference, pointer or hypertext link, through which  
23 the user of the computer located the software.

24 "Communications provider." Entity providing communications  
25 networks or services that enable consumers to access the  
26 Internet or destinations on the public switched telephone  
27 network via a computer modem. This term shall include cable  
28 service providers that also provide telephone services and  
29 providers of Voice over Internet Protocol services.

30 "Computer software." A sequence of instructions written in

1 any programming language that is executed on a computer. The  
2 term shall not include a text or data file, an Internet website  
3 or a data component of an Internet website that is not  
4 executable independently of the Internet website.

5 "Computer virus." A computer program or other set of  
6 instructions that is designed to degrade the performance of or  
7 disable a computer or computer network and is designed to have  
8 the ability to replicate itself on other computers or computer  
9 networks without the authorization of the owners of those  
10 computers or computer networks.

11 "Damage." Any significant impairment to the integrity,  
12 functionality or availability of data, software, a computer, a  
13 system or information.

14 "Execute." With respect to computer software, the  
15 performance of the functions or the carrying out of the  
16 instructions of the computer software.

17 "Intentionally deceptive." Includes, but is not limited to:

18 (1) An intentionally and materially false or fraudulent  
19 statement.

20 (2) A statement or description that intentionally omits  
21 or misrepresents material information in order to deceive the  
22 authorized user.

23 (3) An intentional and material failure to provide any  
24 notice to an authorized user regarding the download or  
25 installation of software in order to deceive the authorized  
26 user.

27 "Internet." The global information system that is logically  
28 linked together by a globally unique address space based on the  
29 Internet Protocol (IP), or its subsequent extensions, and that  
30 is able to support communications using the Transmission Control

1 Protocol/Internet Protocol (TCP/IP) suite, or its subsequent  
2 extensions, or other IP-compatible protocols, and that provides,  
3 uses or makes accessible, either publicly or privately, high-  
4 level services layered on the communications and related  
5 infrastructure described in this act.

6 "MESSAGE." A GRAPHICAL OR TEXT COMMUNICATION PRESENTED TO AN <—  
7 AUTHORIZED USER OF A COMPUTER OTHER THAN COMMUNICATIONS  
8 ORIGINATED AND SENT BY THE COMPUTER'S OPERATING SYSTEM OR  
9 COMMUNICATIONS PRESENTED FOR ANY OF THE PURPOSES DESCRIBED IN  
10 SECTION 6.

11 "Person." Any individual, partnership, corporation, limited  
12 liability company or other organization, or any combination  
13 thereof.

14 "Personally identifiable information." The term shall  
15 include any of the following:

16 (1) First name or first initial in combination with last  
17 name.

18 (2) Credit or debit card numbers or other financial  
19 account numbers.

20 (3) A password or personal identification number  
21 required to access an identified financial account other than  
22 a password, personal identification number or other  
23 identification number transmitted by an authorized user to  
24 the issuer of the account or its agent.

25 (4) Social Security number.

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

28 (i) Account balances.

29 (ii) Overdraft history.

30 (iii) Payment history.

- 1 (iv) A history of Internet websites visited.
- 2 (v) Home address.
- 3 (vi) Work address.
- 4 (vii) A record of a purchase or purchases.

5 "PROCURE THE COPYING." TO INTENTIONALLY PAY OR PROVIDE OTHER <—  
6 CONSIDERATION TO, OR INDUCE ANOTHER PERSON TO CAUSE SOFTWARE TO  
7 BE COPIED ONTO A COMPUTER.

### 8 Section 3. Computer spyware prohibitions.

9 A person or entity that is not an authorized user shall not,  
10 with actual knowledge, with conscious avoidance of actual  
11 knowledge, or willfully, cause computer software to be copied OR <—  
12 PROCURE THE COPYING onto the computer of an authorized user in  
13 this Commonwealth and use the software to do any of the  
14 following:

15 (1) Modify through intentionally deceptive means any of  
16 the following settings related to the computer's access to or  
17 use of the Internet:

18 (i) The page that appears when an authorized user  
19 launches an Internet browser or similar software program  
20 used to access and navigate the Internet.

21 (ii) The default provider or Internet website proxy  
22 the authorized user uses to access or search the  
23 Internet.

24 (iii) The authorized user's list of bookmarks used  
25 to access Internet website pages.

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

29 (i) It is collected through the use of a keystroke-  
30 logging function that records all keystrokes made by an

1 authorized user who uses the computer and transfers that  
2 information from the computer to another person.

3 (ii) It includes all or substantially all of the  
4 Internet websites visited by an authorized user, other  
5 than Internet websites of the provider of the software,  
6 if the computer software was installed in a manner  
7 designed to conceal from all authorized users of the  
8 computer the fact that the software is being installed.

9 (iii) It is a data element described in paragraph  
10 (2), (3), (4) or (5)(i) or (ii) of the definition of  
11 "personally identifiable information" that is extracted  
12 from the authorized user's computer hard drive for a  
13 purpose wholly unrelated to any of the purposes of the  
14 software or service described to an authorized user.

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

22 (4) Intentionally misrepresent that software will be  
23 uninstalled or disabled by an authorized user's action with  
24 knowledge that the software will not be so uninstalled or  
25 disabled.

26 (5) Through intentionally deceptive means, remove,  
27 disable or render inoperative security, antispyware or  
28 antivirus software installed on the computer.

29 Section 4. Control or modification.

30 A person or entity that is not an authorized user shall not,

1 with actual knowledge, with conscious avoidance of actual  
2 knowledge, or willfully, cause computer software to be copied  
3 onto the computer of an authorized user in this Commonwealth and  
4 use the software to do any of the following:

5 (1) Take control of the authorized user's computer by  
6 doing any of the following:

7 (i) Transmitting or relaying commercial electronic  
8 mail or a computer virus from the authorized user's  
9 computer, where the transmission or relaying is initiated  
10 by a person other than the authorized user and without  
11 the authorization of an authorized user.

12 (ii) Accessing or using the authorized user's modem  
13 or Internet service for the purpose of causing damage to  
14 the authorized user's computer or of causing an  
15 authorized user to incur financial charges for a service  
16 that is not authorized by an authorized user.

17 (iii) Using the authorized user's computer as part  
18 of an activity performed by a group of computers for the  
19 purpose of causing damage to another computer, including,  
20 but not limited to, launching a denial of service attack.

21 (iv) Opening a series of stand-alone advertisements <—  
22 MESSAGES in the authorized user's computer without the <—  
23 authorization of an authorized user and with knowledge  
24 that a reasonable computer user cannot close the  
25 advertisements without turning off the computer or  
26 closing the Internet application.

27 (2) Modify any of the following settings related to the  
28 computer's access to or use of the Internet:

29 (i) An authorized user's security or other settings  
30 that protect information about the authorized user for

1 the purpose of stealing personal information of an  
2 authorized user.

3 (ii) The security settings of the computer for the  
4 purpose of causing damage to one or more computers.

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

9 (i) Presenting the authorized user with an option to  
10 decline installation of software with knowledge that,  
11 when the option is selected by the authorized user, the  
12 installation nevertheless proceeds.

13 (ii) Falsely representing that software has been  
14 disabled.

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

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

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

28 (vi) Causing the installation of software in a  
29 particular computer directory or computer memory for the  
30 purpose of evading authorized users' attempts to remove



1 the software from the computer.

2 (vii) Requiring, without the authority of the owner  
3 of the computer, that an authorized user obtain a special  
4 code or download software from a third party to uninstall  
5 the software.

6 Section 5. Misrepresentation and deception.

7 A person or entity who is not an authorized user shall not do  
8 any of the following with regard to the computer of an  
9 authorized user in this Commonwealth:

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

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

19 Section 6. Nonapplicability.

20 ~~Nothing in section 4 or 5 shall apply to any monitoring of or~~ <—

21 (1) NOTHING IN SECTION 4 OR 5 SHALL APPLY TO ANY <—  
22 MONITORING OF OR interaction with a user's Internet or other  
23 network connection or service, or a protected computer, by a  
24 cable operator, computer hardware or software provider or  
25 provider of information service or interactive computer  
26 service for network or computer security purposes,  
27 diagnostics, technical support, repair, authorized updates of  
28 software or system firmware, network management or  
29 maintenance, authorized remote system management or detection  
30 or prevention of the unauthorized use of or fraudulent or

1 other illegal activities in connection with a network,  
2 service or computer software, including scanning for and  
3 removing software proscribed under this act.

4 (2) NOTHING IN THIS ACT SHALL LIMIT THE RIGHTS OF <—  
5 PROVIDERS OF WIRE AND ELECTRONIC COMMUNICATIONS UNDER 18  
6 U.S.C. § 2511 (RELATING TO INTERCEPTION AND DISCLOSURE OF  
7 WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS PROHIBITED).

8 SECTION 7. CRIMINAL ENFORCEMENT.

9 (A) DISTRICT ATTORNEYS.--THE DISTRICT ATTORNEYS OF THE  
10 SEVERAL COUNTIES SHALL HAVE AUTHORITY TO INVESTIGATE AND TO  
11 INSTITUTE CRIMINAL PROCEEDINGS FOR ANY VIOLATIONS OF THIS ACT.

12 (B) ATTORNEY GENERAL.--IN ADDITION TO THE AUTHORITY  
13 CONFERRED UPON THE ATTORNEY GENERAL UNDER THE ACT OF OCTOBER 15,  
14 1980 (P.L.950, NO.164), KNOWN AS THE COMMONWEALTH ATTORNEYS ACT,  
15 THE ATTORNEY GENERAL SHALL HAVE THE AUTHORITY TO INVESTIGATE AND  
16 INSTITUTE CRIMINAL PROCEEDINGS FOR ANY VIOLATION OF THIS ACT. A  
17 PERSON CHARGED WITH A VIOLATION OF THIS ACT BY THE ATTORNEY  
18 GENERAL SHALL NOT HAVE STANDING TO CHALLENGE THE AUTHORITY OF  
19 THE ATTORNEY GENERAL TO INVESTIGATE OR PROSECUTE THE CASE, AND,  
20 IF ANY SUCH CHALLENGE IS MADE, THE CHALLENGE SHALL BE DISMISSED  
21 AND NO RELIEF SHALL BE AVAILABLE IN THE COURTS OF THIS  
22 COMMONWEALTH TO THE PERSON MAKING THE CHALLENGE.

23 ~~Section 7. Enforcement.~~ <—

24 SECTION 8. PENALTY. <—

25 Any person that violates the provisions of sections 3(2) and  
26 4(1)(i), (ii) and (iii) and (2)(i) and (ii) shall be guilty of a  
27 felony OF THE SECOND DEGREE and, upon conviction thereof, shall <—  
28 be sentenced to imprisonment for not less than one nor more than  
29 ten years or a fine, NOTWITHSTANDING 18 PA.C.S. § 1101 (RELATING <—  
30 TO FINES), of not more than \$3,000,000, or both.

1 Section 9. Civil relief.

2 (a) General rule.--The following persons may bring a civil  
3 action against a person who violates this act:

4 (1) A provider of computer software who is adversely  
5 affected by the violation.

6 (2) An Internet Service Provider who is adversely  
7 affected by the violation.

8 (3) A trademark owner whose trademark is used without  
9 the authorization of the owner to deceive users in the course  
10 of any of the deceptive practices prohibited by this section.

11 (4) The Attorney General.

12 (b) Additional remedies.--In addition to any other remedy  
13 provided by law, a person bringing an action under this section  
14 may:

15 (1) Seek injunctive relief to restrain the violator from  
16 continuing the violation.

17 (2) Recover damages in an amount equal to the greater  
18 of:

19 (i) Actual damages arising from the violation.

20 (ii) Up to \$100,000 for each violation, as the court  
21 considers just.

22 (3) Seek both injunctive relief and recovery of damages  
23 as provided by this subsection.

24 (c) Increase by court.--The court may increase an award of  
25 actual damages in an action brought under this section to an  
26 amount not to exceed three times the actual damages sustained if  
27 the court finds that the violations have occurred with a  
28 frequency WITH RESPECT TO A GROUP OF VICTIMS as to constitute a <—  
29 pattern or practice.

30 (d) Fees and costs.--A plaintiff who prevails in an action

1 filed under this section is entitled to recover reasonable  
2 attorney fees and court costs.

3 (e) Communications provider relief.--In the case of a  
4 violation of section 4(1)(ii) that causes a communications  
5 provider to incur costs for the origination, transport or  
6 termination of a call triggered using the modem of a customer of  
7 the communications provider as a result of a violation, the  
8 communications provider may bring a civil action against the  
9 violator to recover any or all of the following:

10 (1) The charges the carrier is obligated to pay to  
11 another carrier or to an information service provider as a  
12 result of the violation, including, but not limited to,  
13 charges for the origination, transport or termination of the  
14 call.

15 (2) Costs of handling customer inquiries or complaints  
16 with respect to amounts billed for calls.

17 (3) Costs and a reasonable attorney fee.

18 (4) An order to enjoin the violation.

19 (f) Multiple violations.--For purposes of this section,  
20 multiple violations of this section resulting from any single  
21 action or conduct shall constitute one violation. In addition,  
22 any single action or conduct that violates more than one  
23 subsection of this section shall be considered multiple  
24 violations based on the number of subsections violated.

25 Section 9 10. Effective date.

<—

26 This act shall take effect in 60 days.