PRINTER'S NO. 858

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 AND STACK, JUNE 3, 2005

REFERRED TO COMMUNICATIONS AND TECHNOLOGY, JUNE 3, 2005

AN ACT

Providing for the protection of consumers from having spyware deceptively installed on their computers, for enforcement and for civil relief.

TABLE OF CONTENTS

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

Section 1. Short title.

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

Protection Against Computer Spyware Act.

Section 2. Definitions.

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

"Advertisement." A communication, the primary purpose of which is the commercial promotion of a commercial product or service, including content on an Internet website operated for a commercial purpose.

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

"Cause to be copied." To distribute or transfer computer software or any component thereof. The term shall not include the following:

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

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

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

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

"Computer software." A sequence of instructions written in

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

"Computer virus." 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.

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

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

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

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

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

(3) 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 authorized user.

"Internet." 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 act.

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

"Personally identifiable information." The term shall include 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 other than a password, personal identification number or other identification number transmitted by an authorized user to the issuer of the account or its agent.

(4) Social Security number.

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

(i) Account balances.

(ii) Overdraft history.

(iii) Payment history.

(iv) A history of Internet websites visited.

(v) Home address.

(vi) Work address.

(vii) A record of a purchase or purchases.

Section 3. Computer spyware prohibitions.

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 an authorized user in this Commonwealth 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:

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

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

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

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

(i) 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.

(ii) It includes all or substantially all of the Internet websites visited by an authorized user, other than Internet websites 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.

(iii) It is a data element described in paragraph

(2), (3), (4) or (5)(i) or (ii) of the definition of "personally identifiable information" that is extracted from the authorized user'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.

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

Section 4. Control or modification.

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 an authorized user in this Commonwealth and use the software to do any of the following:

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

(i) Transmitting or relaying commercial electronic mail or a computer virus from the authorized user'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.

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

(iii) Using the authorized user'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.

(iv) Opening a series of stand-alone advertisements in the authorized user's computer 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 Internet application.

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

(i) 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.

(ii) 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:

(i) 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.

(ii) Falsely representing that software has been disabled.

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

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

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

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

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

Section 5. Misrepresentation and deception.

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

(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.

(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.

Section 6. Nonapplicability.

Nothing in section 4 or 5 shall apply to any monitoring of or interaction with a user's Internet or other network connection or service, or a protected computer, by a 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, network management or maintenance, 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.

Section 7. Enforcement.

Any person that violates the provisions of sections 3(2) and 4(1)(i), (ii) and (iii) and (2)(i) and (ii) shall be guilty of a felony and, upon conviction thereof, shall be sentenced to imprisonment for not less than one nor more than ten years or a fine of not more than $3,000,000, or both.

Section 8. Civil relief.

(a) General rule.--The following persons may bring a civil

action against a person who violates this act:

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

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

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

(4) The Attorney General.

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

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

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

(i) Actual damages arising from the violation.

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

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

(c) Increase by court.--The court may increase an award of actual damages in an action brought under this section to an amount not to exceed three times the actual damages sustained if the court finds that the violations have occurred with a frequency as to constitute a pattern or practice.

(d) Fees and costs.--A plaintiff who prevails in an action filed under this section is entitled to recover reasonable attorney fees and court costs.

(e) Communications provider relief.--In the case of a

violation of section 4(1)(ii) that causes a communications provider to incur costs for the origination, transport or termination of a call triggered using the modem of a customer of the communications provider as a result of a violation, the communications provider may bring a civil action against the violator to recover any or all of the following:

(1) The charges the carrier 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.

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

(3) Costs and a reasonable attorney fee.

(4) An order to enjoin the violation.

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

Section 9. Effective date.

This act shall take effect in 60 days.