PRINTER'S NO. 2924

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 2005 Session of 2005

INTRODUCED BY FLICK, PRESTON, RAMALEY, REICHLEY, ADOLPH, ARGALL, ARMSTRONG, BAKER, BALDWIN, BELARDI, BENNINGHOFF, BOYD, BUNT, BUXTON, CALTAGIRONE, CAPPELLI, CIVERA, CLYMER, COHEN, CRAHALLA, DALEY, DALLY, DENLINGER, DeWEESE, FABRIZIO, FAIRCHILD, FICHTER, GEIST, GEORGE, GOODMAN, HARHAI, HARRIS, HENNESSEY, HERMAN, JOSEPHS, KOTIK, LEDERER, LEH, MANN, MARKOSEK, R. MILLER, MUNDY, PETRARCA, PHILLIPS, PICKETT, READSHAW, RUBLEY, SEMMEL, SHANER, SHAPIRO, B. SMITH, SOLOBAY, R. STEVENSON, E. Z. TAYLOR, THOMAS, TIGUE, WANSACZ, WILT, WOJNAROSKI, WRIGHT AND YOUNGBLOOD, OCTOBER 25, 2005

REFERRED TO COMMITTEE ON CONSUMER AFFAIRS, OCTOBER 25, 2005

AN ACT

Prohibiting the installation, transmission and use of computer software that collects personally identifiable information; authorizing the Attorney General and district attorneys to bring civil actions against persons who violate this act; and providing for damages.

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 Computer Spyware Protection Act.

Section 2. Legislative intent.

It is the intent of the General Assembly to protect owners and operators of computers in this Commonwealth from the use of spyware and malicious software, commonly referred to as malware, that is deceptively or surreptitiously installed on the owner's or the operator's computer.

Section 3. 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:

"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, web site 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.

"Computer software." A sequence of instructions written in any programming language that is executed on a computer. The term does not include a data component of a web page that is not executable independently of the web page.

"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 or availability of data, software, a system or information.

"Execute." When used with respect to computer software, the term means the performance of the functions or the carrying out of the instructions of the computer software.

"Intentionally deceptive." Any of the following:

(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 an owner or operator of a computer.

(3) An intentional and material failure to provide a notice to an owner or operator regarding the installation or execution of computer software for the purpose of deceiving the owner or operator.

"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 section.

"Message." A graphical or text communication presented to an authorized user of a computer.

"Owner or operator." The owner or lessee of a computer or a person using such computer with the owner or lessee's authorization. The term does not include a person who owned a computer prior to the first retail sale of the computer.

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

"Personally identifiable information." Any of the following information if it allows the entity holding the information to identify the owner or operator of a computer:

(1) The first name or first initial in combination with the last name.

(2) A home or other physical address, including street name.

(3) Personal identification code in conjunction with a password required to access an identified 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, tax identification number, driver's license number, passport number or any other government-issued identification number.

(5) Account balance, overdraft history or payment history that personally identifies an owner or operator of a computer.

Section 4. Prohibitions; use of software.

It is unlawful for a person who is not an owner or operator of a computer to cause computer software to be copied on such computer knowingly or with conscious avoidance of actual knowledge or willfully use such software to do any of the following:

(1) Modify, through intentionally deceptive means, settings of a computer that control any of the following:

(i) The web page that appears when an owner or operator launches an Internet browser or similar computer software used to access and navigate the Internet.

(ii) The default provider or web proxy that an owner or operator uses to access or search the Internet.

(iii) An owner's or an operator's list of bookmarks used to access web pages.

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

(i) The use of a keystroke-logging function that records all or substantially all keystrokes made by an owner or operator of a computer and transfers that information from the computer to another person.

(ii) In a manner that correlates personally identifiable information with data regarding all or substantially all of the Internet sites visited by an owner or operator, other than Internet sites operated by the person providing such 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) By extracting from the hard drive of an owner's or an operator's computer, an owner's or an operator's Social Security number, tax identification number, driver's license number, passport number, any other government-issued identification number, account balances or overdraft history for a purpose unrelated to any of the purposes of the software or service described to an authorized user.

(3) Prevent, through intentionally deceptive means, an owner's or an operator's reasonable efforts to block the installation of or execution of or to disable computer software by causing computer software that the owner or operator has properly removed or disabled to automatically

reinstall or reactivate on the computer without the authorization of an authorized user.

(4) Intentionally misrepresent that computer software will be uninstalled or disabled by an owner's or an operator's action.

(5) Through intentionally deceptive means, remove, disable or render inoperative security, antispyware or antivirus computer software installed on an owner's or an operator's computer.

(6) Enable use of an owner's or an operator's computer to do any of the following:

(i) Accessing or using a modem or Internet service for the purpose of causing damage to an owner's or an operator's computer or causing an owner or operator or a third party affected by such conduct to incur financial charges for a service that the owner or operator did not authorize.

(ii) Opening multiple, sequential, stand-alone messages in an owner's or an operator's computer without the authorization of an owner or operator and with knowledge that a reasonable computer user could not close the messages without turning off the computer or closing the software application in which the messages appear; provided that this paragraph shall not apply to communications originated by the computer's operating system, originated by a software application that the user chooses to activate, originated by a service provider that the user chooses to use or presented for any of the purposes described in section 6.

(iii) Transmitting or relaying commercial electronic mail or a computer virus from the computer, where the transmission or relaying is initiated by a person other than the authorized user and without the authorization of an authorized user.

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

(i) Settings that protect information about an owner or operator for the purpose of taking personally identifiable information of the owner or operator.

(ii) Security settings for the purpose of causing damage to a computer.

(iii) Settings that protect the computer from the uses identified in paragraph (6).

(8) Prevent, without the authorization of an owner or operator, an owner's or an operator's reasonable efforts to block the installation of or to disable computer software by doing any of the following:

(i) Presenting the owner or operator with an option to decline installation of computer software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds.

(ii) Falsely representing that computer 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 filenames, 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. Other prohibitions.

It is unlawful for a person who is not an owner or operator of a computer to do any of the following with regard to the computer:

(1) Induce an owner or operator to install a computer software component onto the owner's or the operator's computer by intentionally misrepresenting that installing computer software is necessary for security or privacy reasons or in order to open, view or play a particular type of content.

(2) Using intentionally deceptive means to cause the execution of a computer software component with the intent of causing the computer to use such component in a manner that violates any other provision of this chapter.

Section 6. Exceptions.

Sections 4 and 5 shall not apply to the monitoring of or interaction with an owner's or an operator's Internet or other network connection, service or 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, maintenance, repair, network management, authorized updates of computer 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 computer software prescribed under this act.

Section 7. Remedies.

(a) Civil actions.--The Attorney General, an Internet service provider or software company that expends resources in good faith assisting authorized users harmed by a violation of this act; or a trademark owner whose mark is used to deceive authorized users in violation of this act, may bring a civil action against a person who violates any provision of this act to recover actual damages, liquidated damages of at least $1,000 per violation of this act, not to exceed $1,000,000 for a pattern or practice of such violations, attorney fees and costs.

(b) Trebel damages.--The court may increase a damage award to an amount equal to not more than three times the amount otherwise recoverable under subsection (a) if the court determines that the defendant committed the violation willfully and knowingly.

(c) Liquidated damages.--The court may reduce liquidated damages recoverable under subsection (a), to a minimum of $100, not to exceed $100,000 for each violation if the court finds that the defendant established and implemented practices and procedures reasonably designed to prevent a violation of this act.

(d) Other damages.--In the case of a violation of section 4(6)(i) that causes a telecommunications carrier or provider of voice over Internet protocol service to incur costs for the origination, transport or termination of a call triggered using the modem or Internet-capable device of a customer of such telecommunications carrier or provider as a result of such violation, the telecommunications carrier may bring a civil action against the violator to recover any or all of the following:

(1) The charges such carrier or provider 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 such calls.

(3) Costs and a reasonable attorney fee.

(4) An order to enjoin the violation.

(e) Multiple violations.--For purposes of a civil action under subsections (a), (b) and (c), any single action or conduct that violates more than one of the provisions of this act shall be considered multiple violations based on the number of provisions violated.

Section 8. Good Samaritan.

(a) Liability.--No provider of computer software or of an interactive computer service may be held liable for identifying, naming, removing, disabling or otherwise affecting a computer program through any action voluntarily undertaken or service provided where the provider:

(1) Intends to identify accurately, prevent the installation or execution of, remove or disable another computer program on a computer of a customer of the provider.

(2) Reasonably believes the computer program exhibits behavior that violates this act.

(3) Notifies the authorized user and obtains clear and conspicuous consent before undertaking such action or providing such service.

(b) Requirements.--A provider of computer software or interactive computer service is entitled to protection under this section only if such provider:

(1) Has established internal practices and procedures to evaluate computer programs reasonably designed to determine whether or not a computer program exhibits behavior that violates this act.

(2) Has established a process for managing disputes and inquiries regarding misclassification or false positive identifications of computer programs.

(c) Attorney General, district attorney.--Nothing in this section is intended to limit the ability of the Attorney General or a district attorney to bring an action against a provider of computer software or of an interactive computer service.

Section 9. Severability.

The provisions of this act are severable. If any provision of this act or its application to any person or circumstance is held invalid, the invalidity shall not affect other provisions or applications of this act which can be given effect without the invalid provision or application.

Section 10. Repeal.

All acts and parts of acts are repealed insofar as they are inconsistent with this act.

Section 11. Effective date.

This act shall take effect in 60 days.