Stricken language would be deleted from and underlined language would be added to the law as it existed prior to this session of the General Assembly.

State of Arkansas
85th General Assembly
Regular Session, 2005

A Bill

HOUSE BILL 2904

By: Representatives D. Evans, Pace, Dobbins

For An Act To Be Entitled

AN ACT TO PROTECT CONSUMERS FROM THE IMPROPER USE OF COMPUTER SPYWARE; AND FOR OTHER PURPOSES.

Subtitle

TO PROTECT CONSUMERS FROM THE IMPROPER USE OF COMPUTER SPYWARE.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:

SECTION 1. Arkansas Code Title 4 is amended to add an additional chapter to read as follows:

Chapter 110 -- INFORMATION TECHNOLOGY

Subchapter 1 -- Consumer Protection Against Computer Spyware Act

4-110-101. Short title.

This subchapter shall be known and cited as the "Consumer Protection Against Computer Spyware Act".

4-110-102. Definitions.

As used in this subchapter:

(1) "Advertisement" means 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;

(2)(A) "Authorized user", with respect to a computer, means a person that owns or is authorized by the owner or lessee to use the computer.

(B) 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;

(3) "Bundled software" means software that is acquired through the installation of a large number of separate programs in a single installation when the programs are not all relevant to or reasonably associated with the purpose of the installation;

(4) "Computer software" means a sequence of instructions written in any programming language that is executed on a computer;

(5) "Computer virus" means a computer program or other set of instructions that is designed to do the following acts without the authorization of the owner or owners of a computer or computer network:

(A) Degrade the performance of or disable a computer or computer network; and

(B) Have the ability to replicate itself on another computer or computer network;

(6) "Damage" means any significant impairment to the integrity, confidentiality, or availability of data, software, a system, or information, including, but not limited to, the:

(A) Significant degradation of the performance of or disabling a computer or computer network;

(B) Inability to uninstall computer data due to an intentionally deceptive uninstall process;

(C) Unauthorized loss of or change to data; and

(D) Unauthorized loss of or change to security settings, copyrighted software, or authorized computer settings;

(7) "Distributed denial of service" or "DDoS attack" means techniques or actions involving the use of one (1) or more damaged computers to damage another computer or a targeted computer system in order to shut the computer or computer system down and deny the service of the damaged computer or computer system to legitimate users;

(8) "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;

(9) "Hardware" means a comprehensive term for all of the discrete physical parts of a computer as distinguished from:

(A) The data the computer contains or that enables it to operate; and

(B) The software that provides instructions for the

hardware to accomplish tasks;

(10) "Intentionally deceptive" means with the intent to deceive an authorized user in order to either damage a computer or computer system or wrongfully obtain personally identifiable information without authority:

(A) To make an intentional and materially false or fraudulent statement;

(B) To make a statement or description that intentionally omits or misrepresents material information; or

(C) An intentional and material failure to provide any notice to an authorized user regarding the download or installation of software;

(11) "Internet" means:

(A) The international computer network of both federal and nonfederal interoperable packet switched data networks; or

(B) The global information system that:

(i) Is logically linked together by a globally unique address space based on the Internet Protocol (IP), or its subsequent extensions;

(ii) 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

(iii) Provides, uses, or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described in this subdivision (11);

(12) "Internet site" means a specific location on the Internet accessible through an Internet domain name, universal resource locator, or IP address;

(13) “Malicious code” means a computer program or other set of instructions that is designed to damage a computer without the authorization of the owner or owners of the computer by any of the following acts:

(A) Give an unauthorized group or individual unrestricted access to the data stored on a computer for the purpose of transmitting personally identifiable information;

(B) Replicate itself or generate other similar software that can run independently on a computer and travel across Internet or local network connections attempting to install on other computers;

(C) Attach to or modify a system process, network setting, file, or boot sector;

(D) Cause the denial to an authorized user of a computer or multiple computers access to data on the computer of the authorized user;

(E) Log each key stroke on a keyboard or capture images displayed on the computer hardware;

(F) Be installed alongside bundled software or through controls on the Internet without disclosure for the purpose of gathering personally identifiable information or showing the user advertising materials;

(G) Give an unauthorized group or individual unrestricted access to remotely control the computer for the purpose of storing or sharing copyrighted material or releasing malicious code; and

(H) Degrade or render inoperable normally functioning hardware or software;

(14) "Person" means one (1) or more individuals, partnerships, corporations, limited liability companies, or other organizations;

(15) "Personally identifiable information" includes, but is not limited to:

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

(B) Credit or debit card numbers or other financial account numbers;

(C) A password;

(D) A personal identification number or other identification required to access an identified account;

(E) A social security number; or

(F) 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 websites visited;

(v) Home address;

(vi) Work address; or

(vii) A record of a purchase or purchases;

(16) "Phishing", "brand spoofing", or "carding" means the use of electronic mail or other means to imitate a legitimate company or business in order to entice the user into divulging passwords, credit card numbers, or other sensitive information for the purpose of committing theft or fraud;

(17) "Software" means the computer programs and instructions that make hardware work, including system software or operating systems that control the workings of the computer, and applications such as word processing programs, spreadsheets, and databases; and

(18) "Trojan horse" means:

(A) A destructive program that masquerades as a benign application; or

(B) A program containing hidden code allowing the unauthorized collection, falsification, or destruction of data, or the execution of outside control of a computer system.

4-110-103. Unlawful acts — Exceptions.

(a) A person 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 any computer in this state and use the software to:

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

(A) Which page 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; or

(C) The authorized user's list of bookmarks used to access web pages;

(2) Collect, through intentionally deceptive means, personally identifiable information about the authorized user that:

(A) Is collected through the use of malicious code;

(B) Includes all or substantially all of the Internet addresses visited by an authorized user, other than Internet addresses of the provider of the software, if the computer software was installed in an

intentionally deceptive manner to conceal from all authorized users of the computer the fact that the software is being installed; or

(C) Is a data element described in § 4-110-102(15) that is extracted from a computer hard drive for a purpose wholly unrelated to any of the purposes of the software or service as described to the authorized user;

(3) Prevent without authorization from the authorized user through intentionally deceptive means an authorized user's reasonable efforts to block the installation of or 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 uninstalled or disabled; and

(5) Through intentionally deceptive means:

(A) Remove, disable, or render inoperative security, antispyware, or antivirus software installed on the computer;

(B) Install or cause to be installed any software without:

(i) Notification to and consent from the authorized user immediately prior to the installation process; and

(ii) Providing a separate end user license agreement with notification of the items installed and their functions and purposes;

(C) Exploit security vulnerabilities or security settings as consent to install software without notice;

(D) Install any applications that are not removable;

(E) Request personal information to install software unless essential to the program function or for the purpose of authentication or validation;

(F) Share or otherwise use any authorized user data in any way that compromises the authorized user's privacy without the authorized user's permission;

(G) Use any authorized user data for marketing purposes or enroll an authorized user in any deal, offer, newsletter, or any similar material from the distributor or other parties, except with the authorized user's explicit consent through a check box or other user initiated means; or

(H) Through means of a trojan horse or other remote access

software installed through clandestine means, remove control of the computer's functions from the authorized user in order to use it for spamming, disabling other computer systems, searching for other vulnerable computer systems, or other illegal or unauthorized purposes.

(b) A person 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 any computer in this state and use the software to:

(1) Take control of a computer by:

(A) Transmitting or relaying without the authorization of an authorized user commercial electronic mail or a computer virus from the consumer's computer;

(B) Accessing or using the authorized user's modem or Internet service for the purpose of causing:

(i) Damage to the authorized user's computer; or

(ii) An authorized user to incur financial charges for a service that is not authorized by the 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; or

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

(B) The security settings of the computer for the purpose of causing damage to one (1) or more computers;

(3) Prevent without the authorization of an authorized user an authorized user's reasonable efforts to block the installation of or disable software by:

(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; or

(B) Falsely representing that software has been disabled; or

(4) Interfere with uninstalling the software by:

(A) Requiring Internet access to uninstall software;

(B) Requesting unnecessary information in order to uninstall software including, but not limited to, electronic mail addresses, names, physical addresses, other physical information or surveys;

(C) Leaving behind hidden elements of the software that is designed to and will reinstall itself or portions of itself;

(D) Leaving by design active portions of the program that originated with the install resident in memory without explicit notification and consent from the user; or

(E) Intentionally causing damage to or removing any vital component of the operating system.

(c) A person that is not an authorized user shall not with regard to any computer in this state:

(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 or software;

(2) Deceptively cause 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; or

(3) Install or cause to be installed any software that is deliberately hidden from detection by the user of a computer and not technically feasible of being revealed.

(d) No person shall engage in phishing, brand spoofing, or carding.

(e) Subsections (b) and (c) of this section shall not apply to any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, in accordance with the relationship or agreement between the owner of the computer or computer system used by the authorized user and a:

(1) Telecommunications or Internet service provider;

(2) Cable Internet provider;

(3) Computer hardware or software provider; or

(4) Provider of information service or interactive computer service for:

(A) Network or computer security purposes;

(B) Diagnostics;

(C) Technical support;

(D) Repair;

(E) Authorized updates of software or system firmware;

(F) Authorized remote system management; or

(G) Detection or prevention of the unauthorized use or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing software proscribed under this subchapter.

(f) Notwithstanding any other provision of this subchapter, the provisions of this subchapter shall not apply to:

(1) The installation of software that falls within the scope of a previous grant of authorization by an authorized user;

(2) The installation of an upgrade to a software program that has already been installed on the computer with the authorization of an authorized user; or

(3) The installation of software before the first retail sale and delivery of the computer.

4-110-104. Penalties.

Any violation of this subchapter is punishable by action of the Attorney General under the Deceptive Trade Practices Act, § 4-88-101 et seq.

4-110-105. Monitoring software.

(a) All fines and penalties collected under § 4-110-104 shall be paid to the Treasurer of State for the benefit of the Spyware Monitoring Fund to be used by the Attorney General and the Department of Information Systems to implement this section.

(b)(1) The Attorney General is authorized to request an appropriation from the fund not to exceed fifty percent (50%) of the fund balance to offset

his or her salary and administration expenses directly related to the enforcement of this subchapter.

(2) The Department of Information Systems is authorized to request an appropriation from the fund not to exceed fifty percent (50%) of the fund balance to purchase and distribute computer monitoring software with the capacity to detect actions and practices in violation of this subchapter.

(c)(1) To the extent that money appropriated to the Department of Information Systems is available from the Spyware Monitoring Fund, the computer monitoring software shall be provided free of charge by the department to any consumer upon request.

(2)(A) The computer monitoring software may be provided to businesses and other entities by the department for a reasonable fee established by the department.

(B) The fee shall be:

(i) Designed to reimburse the department for the cost of obtaining and distributing the software; and

(ii) Paid to the Treasurer of State for the benefit of the Spyware Monitoring Fund.

(d) The Attorney General and Department of Information Systems are authorized to adopt any rules and regulations deemed necessary or desirable to implement this section.

SECTION 2. Title 19, Chapter 6, Subchapter 4, is amended to add an additional section to read as follows:

19-6-499. Spyware Monitoring Fund.

There is established on the books of the Treasurer of State, the Auditor of State, and the Chief Financial Officer of the State a fund to be known as the "Spyware Monitoring Fund" to be used by the Attorney General and the Department of Information Systems as follows:

(1) A maximum of fifty percent (50%) of the fund balance shall be used by the Attorney General to offset his or her salary and administration expenses directly related to the enforcement of the Consumer Protection Against Computer Spyware Act, § 4-110-101 et seq.; and

(2) A maximum of fifty percent (50%) of the fund balance shall be used by the Department of Information Systems to purchase and distribute computer monitoring software with the capacity to detect actions and

practices in violation of the Consumer Protection Against Computer Spyware Act, § 4-110-101 et seq.