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.

Act 2255 of the Regular Session

State of Arkansas *As Engrossed: S4/5/05*
85th General Assembly A Bill
Regular Session, 2005 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) "Authorized user", with respect to a computer, means a person that owns or is authorized by the owner or lessee to use the computer.

(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 wholly unrelated to the purpose of the installation as described to the authorized user;

(4)(A) "Caused to be copied" means to distribute or transfer computer software or any component of computer software.

(B) "Caused to be copied" does not include providing:

(i) Transmission, routing, intermediate temporary storage, or caching of software;

(ii) A compact disk, website, computer server, or other storage medium through which the software was distributed by a third party; or

(iii) A directory, index, reference, pointer, hypertext link, or other information location tool through which the user of the computer located the software;

(5) "Computer software" means a sequence of instructions written in any programming language that is executed on a *computer, but does not include a text or data file, including a cookie;*

(6) "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;

(7) "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 and intentional degradation of the performance of a computer or a computer network; or

(B) Intentional disabling of a computer or computer network;

(8) "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;

(9) "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;

(10) "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;

(11) "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;

(12) "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 (12)*;

(13) "Internet address" means a specific location on the Internet accessible through a universal resource locator or Internet protocol address;

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

(15) "Personally identifiable information" means any of the following if it allows the entity holding the information to identify an authorized user by:

(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 or personal identification number or other identification required to access an identified account other than a password, personal identification number, or other identification transmitted by an authorized user to the issuer of the account or its agent;

(D) A social security number; or

(E) 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; and*

(16) "Phishing" 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.*

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;*

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

(D) Settings in computer software or in a text or data file on the computer that are used to resolve a universal resource locator or other location identifier used to access a public or private network;

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

(A) Is collected through the use of a keystroke-logging function that records all keystrokes made by an authorized user that uses the computer and transmits the information from the computer to another person;

(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;

(C) 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; or*

(D) Is collected by extracting screen shots of an authorized user's use of the computer 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; or*

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

the computer.

(b) A person that is not an authorized user shall not with actual *knowledge, with conscious avoidance of actual knowledge, or willfully:*

(1) Cause computer software to be copied onto any computer in this state and use the software to 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) Without authorization obtain the ability to use one (1) or more computers of other end users on a network to send commercial electronic mail, to damage other computers, or to locate other computers vulnerable to an attack without:

(A) Notice to or knowledge of the owners of the computers or computer networks; or

(B) A prior or existing personal, business, or contractual relationship with the owner or owners of the computer or computer networks;

(3) 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;

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

(5) Intentionally interfere with an authorized user's attempt to uninstall the software by:

(A) Leaving behind without authorization on the authorized user's computer for the purpose of evading an authorized user's attempt to remove the software from the computer hidden elements of the software that are designed to and will reinstall the software or portions of the software;

(B) Intentionally causing damage to or removing any vital component of the operating system;

(C) Falsely representing that software has been disabled;

(D) 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;

(E) 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;

(F) Causing the installation of software in a particular computer directory or computer memory for the purpose of evading an authorized user's attempt to remove the software from the computer;

(G) Requiring completion of a survey to uninstall software unless reasonably related to the uninstallation; or

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

(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; or*

(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.*

(d) No person shall engage in phishing.

(e) 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 to carry out any of the violations described in subsections (a) -- (d) of this section for a purpose wholly unrelated to any of the purposes of the software or service as described to the authorized user if the software is installed in an intentionally deceptive manner that:

(1) Exploits a security vulnerability in the computer; or

(2) Bundles the software with other software without providing prior notice to the authorized user of the name of the software and that the software will be installed on the computer.

(f) Any provision of a consumer contract that permits an intentionally deceptive practice prohibited under this section is not enforceable.

(g) 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;

(G) Network management or maintenance; or

(H) 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.

(i) 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 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. Use of Spyware Monitoring Fund.

(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 to:*

(1) Investigate potential violations and enforce the provisions of this subchapter; and

(2) Establish and maintain a website to:

(A) Provide information concerning:

(i) The availability of computer software to combat spyware; and

(ii) False representations about the effectiveness of specific antispyware software;

(B) Promote consumer awareness about spyware, antispyware, and computer fraud;

(C) Educate consumers about:

(i) Spyware, computer fraud, and the effects of spyware and computer fraud upon consumer privacy and computer systems; and

(ii) How to access or obtain computer software to combat spyware; and

(D) Provide consumers with links to antispyware websites

with helpful information.

(b) The Attorney General is authorized to request an appropriation from the fund to offset his or her salary and administrative expenses directly related to the enforcement of this subchapter and the administration of the website.

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 Fiscal Officer of the State a fund to be known as the "Spyware Monitoring Fund" to be used by the Attorney General to offset his or her salary and administrative expenses directly related to the enforcement of the Consumer Protection Against Computer Spyware Act, § 4-110-101 et seq. and administration of the website required by the act.*

/s/ D. Evans

APPROVED: 4/13/2005

1