ENGROSSED HOUSE
BILL NO. 2083

By: Liebmann, Shelton, Duncan and Bingman of the House

and

Jolley of the Senate

(technology – Computer Spyware Protection Act – Internet service providers – plaintiff – codification – noncodification – effective date)

BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

SECTION 1. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 776.11 of Title 15, unless there is created a duplication in numbering, reads as follows:

This act shall be known and may be cited as the "Computer Spyware Protection Act".

SECTION 2. NEW LAW A new section of law not to be codified in the Oklahoma Statutes reads as follows:

It is the intent of the Legislature to protect owners and operators of computers in this state from the use of spyware and malware that is deceptively or surreptitiously installed on the computer of an owner or operator.

SECTION 3. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 776.12 of Title 15, unless there is created a duplication in numbering, reads as follows:

As used in the Computer Spyware Protection Act:

1. "Cause to be copied" means to distribute or transfer computer software, or any component thereof. Such term shall not include providing:

a. transmission, routing, provision of intermediate temporary storage, or caching of software,

b. a storage or hosting medium, such as a compact disk, web site, or computer server through which the software was distributed by a third party, or

c. an information location tool, such as a directory, index, reference, pointer, or hypertext link, through which the user of the computer located the software;

2. “Computer software” means a sequence of instructions written in any programming language that is executed on a computer. Computer software does not include a data component of a web page that is not executable independently of the web page;

3. “Computer virus” means 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;

4. “Damage” means any significant impairment to the integrity or availability of data, software, a system, or information;

5. “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;

6. “Intentionally deceptive” means any of the following:

a. an intentionally and materially false or fraudulent statement,

b. a statement or description that intentionally omits or misrepresents material information in order to deceive an owner or operator of a computer, and

c. 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;

7. “Internet” means 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 paragraph;

8. “Owner or operator” means the owner or lessee of a computer, or a person using such computer with authorization of the owner or lessee, but does not include a person who owned a computer prior to the first retail sale of the computer;

9. “Message” means a graphical or text communication presented to an authorized user of a computer;

10. “Person” means any individual, partnership, corporation, limited liability company, or other organization, or any combination thereof; and

11. “Personally identifiable information” means any of the following information if it allows the entity holding the information to identify the owner or operator of a computer:

a. the first name or first initial in combination with the last name,

b. a home or other physical address including street name,

c. 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,

d. social security number, tax identification number, driver license number, passport number, or any other government-issued identification number,

e. account balance, overdraft history, or payment history that personally identifies an owner or operator of a computer, or

f. biometric information.

SECTION 4. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 776.13 of Title 15, unless there is created a duplication in numbering, reads as follows:

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

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

a. 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 or a private network,

b. the default provider or web proxy that an owner or operator uses to access or search the Internet, or

c. a list of bookmarks used by an owner or operator to access web pages;

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

a. 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,

b. in a manner that correlates personally identifiable information with data regarding all or substantially all of the web sites visited by an owner or operator, other than web 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, or

c. by extracting from the Random Access Memory (RAM) or storage media of a computer of an owner or operator, the social security number, tax identification number, driver license number, passport number, any other government-issued identification number, account balances, or overdraft history of an owner or operator 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, the reasonable efforts of an owner or operator 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 the action of an owner or operator;

5. Through intentionally deceptive means, remove, disable, or render inoperative security, antispyware, or antivirus computer software installed on the computer of an owner or operator;

6. Enable use of the computer of an owner or operator to do any of the following:

a. accessing or using a modem or Internet service for the purpose of causing damage to the computer of an owner or operator 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,

b. opening multiple, sequential, stand-alone messages in the computer of an owner or operator 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. This subparagraph shall not apply to communications originated by the operating system of the computer, 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 of this act, or

c. 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 access of the computer, or use of, the Internet:

a. settings that protect information about an owner or operator for the purpose of taking personally identifiable information of the owner or operator,

b. security settings for the purpose of causing damage to a computer, or

c. settings that protect the computer from the uses identified in paragraph 6 of this section; and

8. Prevent, without the authorization of an owner or operator, the reasonable efforts of an owner or operator to block the

installation of, or to disable, computer software by doing any of the following:

a. 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,

b. falsely representing that computer software has been disabled,

c. 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,

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 attempts by authorized users to remove the software from the computer, or

g. 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. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 776.14 of Title 15, unless there is created a duplication in numbering, reads as follows:

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 computer of the owner or operator 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; or

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 provisions of the Computer Spyware Protection Act.

SECTION 6. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 776.15 of Title 15, unless there is created a duplication in numbering, reads as follows:

Sections 4 and 5 of the Computer Spyware Protection Act shall not apply to the monitoring of, or interaction with, the Internet or other network connection, service, or computer of an owner or operator, 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. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 776.16 of Title 15, unless there is created a duplication in numbering, reads as follows:

A. The Attorney General for the State of Oklahoma, an Internet service provider or software company that expends resources in good faith assisting authorized users harmed by a violation of the Computer Spyware Protection 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 One Thousand Dollars ($1,000.00) per violation of the act, not to exceed One Million Dollars ($1,000,000.00) for a pattern or practice of such violations, attorney fees, and costs.

B. The court may increase a damage award to an amount equal to not more than three times the amount otherwise recoverable under subsection A of this section if the court determines that the defendant committed the violation willfully and knowingly.

C. The court may reduce liquidated damages recoverable under subsection A of this section, to a minimum of One Hundred Dollars ($100.00), not to exceed One Hundred Thousand Dollars ($100,000.00) 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. In the case of a violation of subparagraph a of paragraph 6 of Section 4 of this act 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 the 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; and

4. An order to enjoin the violation.

E. For purposes of a civil action under subsection A, B or C of this section, any single action or conduct that violates more than one provision of this act shall be considered multiple violations based on the number of provisions violated.

F. No liability protection shall be afforded under this section against a claim brought by a computer software or interactive computer service against a competitor of such service or similar goods in the relevant market, where the defendant in the action fails to prove beyond a reasonable doubt that it acted with due diligence:

1. In establishing, implementing, and enforcing internal practices and procedures, impartially applied and reasonably calculated and based on human review, evaluation, and investigation of the relevant facts, that identify, prevent installation or execution of, remove or disable a computer program that violates this act; and

2. In establishing, implementing, and enforcing a process for managing and within thirty (30) days responding to disputes and inquiries regarding misclassification or false positive identifications of computer programs, and removing false positives and correcting such misclassifications. If warranted, the defendant must adjust its future process upon finding false positives. If after internal review the defendant believes that the product or application in question violates the act, the defendant shall state

with particularity the facts underlying its belief that the software violates the act.

In an action, the plaintiff shall carry the burden of proving that it is a competitor of the defendant with regard to a good, service, or application that is the subject of the disputed misclassification or false positive.

SECTION 8. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 776.17 of Title 15, unless there is created a duplication in numbering, reads as follows:

A. 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 such provider;

2. Reasonably believes the computer program exhibits behavior that violates the Computer Spyware Protection Act; and

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

B. A provider of computer software or interactive computer service is entitled to protection under this section only if the 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; and

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

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

SECTION 9. This act shall become effective November 1, 2006.

Passed the House of Representatives the 28th day of February, 2006.

_____
Presiding Officer of the House of Representatives

Passed the Senate the ____ day of _____, 2006.

_____
Presiding Officer of the Senate