

**EHB 2083**

**THE STATE SENATE**  
**Thursday, March 23, 2006**

**ENGROSSED**

**House Bill No. 2083**

**As Amended**

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:

1 As used in the Computer Spyware Protection Act:

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

- 5 a. transmission, routing, provision of intermediate  
6 temporary storage, or caching of software,
- 7 b. a storage or hosting medium, such as a compact disk,  
8 web site, or computer server through which the  
9 software was distributed by a third party, or
- 10 c. an information location tool, such as a directory,  
11 index, reference, pointer, or hypertext link, through  
12 which the user of the computer located the software;

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

17 3. "Computer virus" means a computer program or other set of  
18 instructions that is designed to degrade the performance of or  
19 disable a computer or computer network and is designed to have the  
20 ability to replicate itself on other computers or computer networks  
21 without the authorization of the owners of those computers or  
22 computer networks;

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

3       5. "Execute", when used with respect to computer software,  
4 means the performance of the functions or the carrying out of the  
5 instructions of the computer software;

6       6. "Intentionally deceptive" means any of the following:

7           a. an intentionally and materially false or fraudulent  
8 statement,

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

12           c. an intentional and material failure to provide a  
13 notice to an owner or operator regarding the  
14 installation or execution of computer software for the  
15 purpose of deceiving the owner or operator;

16       7. "Internet" means the global information system that is  
17 logically linked together by a globally unique address space based  
18 on the Internet protocol (IP), or its subsequent extensions, and  
19 that is able to support communications using the transmission  
20 control protocol/Internet protocol (TCP/IP) suite, or its subsequent  
21 extensions, or other IP-compatible protocols, and that provides,  
22 uses, or makes accessible, either publicly or privately, high-level

1 services layered on the communications and related infrastructure  
2 described in this paragraph;

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

7 9. "Message" means a graphical or text communication presented  
8 to an authorized user of a computer;

9 10. "Person" means any individual, partnership, corporation,  
10 limited liability company, or other organization, or any combination  
11 thereof; and

12 11. "Personally identifiable information" means any of the  
13 following information if it allows the entity holding the  
14 information to identify the owner or operator of a computer:

- 15 a. the first name or first initial in combination with  
16 the last name,  
17 b. a home or other physical address including street  
18 name,  
19 c. personal identification code in conjunction with a  
20 password required to access an identified account,  
21 other than a password, personal identification number  
22 or other identification number transmitted by an

- 1 authorized user to the issuer of the account or its
- 2 agent,
- 3 d. social security number, tax identification number,
- 4 driver license number, passport number, or any other
- 5 government-issued identification number,
- 6 e. account balance, overdraft history, or payment history
- 7 that personally identifies an owner or operator of a
- 8 computer, or
- 9 f. biometric information.

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

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

- 17 1. Modify, through intentionally deceptive means, settings of a
- 18 computer that control any of the following:
  - 19 a. the web page that appears when an owner or operator
  - 20 launches an Internet browser or similar computer
  - 21 software used to access and navigate the Internet or a
  - 22 private network,

- 1           b.    the default provider or web proxy that an owner or  
2                   operator uses to access or search the Internet, or  
3           c.    a list of bookmarks used by an owner or operator to  
4                   access web pages;

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

- 7           a.    the use of a keystroke-logging function that records  
8                   all or substantially all keystrokes made by an owner  
9                   or operator of a computer and transfers that  
10                  information from the computer to another person,  
11           b.    in a manner that correlates personally identifiable  
12                  information with data regarding all or substantially  
13                  all of the web sites visited by an owner or operator,  
14                  other than web sites operated by the person providing  
15                  such software, if the computer software was installed  
16                  in a manner designed to conceal from all authorized  
17                  users of the computer the fact that the software is  
18                  being installed, or  
19           c.    by extracting from the Random Access Memory (RAM) or  
20                  storage media of a computer of an owner or operator,  
21                  the social security number, tax identification number,  
22                  driver license number, passport number, any other  
23                  government-issued identification number, account

1 balances, or overdraft history of an owner or operator  
2 for a purpose unrelated to any of the purposes of the  
3 software or service described to an authorized user;

4 3. Prevent, through intentionally deceptive means, the  
5 reasonable efforts of an owner or operator to block the installation  
6 of or execution of, or to disable, computer software by causing  
7 computer software that the owner or operator has properly removed or  
8 disabled to automatically reinstall or reactivate on the computer  
9 without the authorization of an authorized user;

10 4. Intentionally misrepresent that computer software will be  
11 uninstalled or disabled by the action of an owner or operator;

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

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

17 a. accessing or using a modem or Internet service for the  
18 purpose of causing damage to the computer of an owner  
19 or operator or causing an owner or operator, or a  
20 third party affected by such conduct to incur  
21 financial charges for a service that the owner or  
22 operator did not authorize,

1           b.    opening multiple, sequential, stand-alone messages in  
2                    the computer of an owner or operator without the  
3                    authorization of an owner or operator and with  
4                    knowledge that a reasonable computer user could not  
5                    close the messages without turning off the computer or  
6                    closing the software application in which the messages  
7                    appear. This subparagraph shall not apply to  
8                    communications originated by the operating system of  
9                    the computer, originated by a software application  
10                  that the user chooses to activate, originated by a  
11                  service provider that the user chooses to use, or  
12                  presented for any of the purposes described in Section  
13                  6 of this act, or

14           c.    transmitting or relaying commercial electronic mail or  
15                    a computer virus from the computer, where the  
16                    transmission or relaying is initiated by a person  
17                    other than the authorized user and without the  
18                    authorization of an authorized user;

19           7.    Modify any of the following settings-related access of the  
20    computer, or use of, the Internet:

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

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

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

5           8.    Prevent, without the authorization of an owner or operator,  
6   the reasonable efforts of an owner or operator to block the  
7   installation of, or to disable, computer software by doing any of  
8   the following:

9           a.    presenting the owner or operator with an option to  
10                   decline installation of computer software with  
11                   knowledge that, when the option is selected by the  
12                   authorized user, the installation nevertheless  
13                   proceeds,

14          b.    falsely representing that computer software has been  
15                   disabled,

16          c.    requiring in an intentionally deceptive manner the  
17                   user to access the Internet to remove the software  
18                   with knowledge or reckless disregard of the fact that  
19                   the software frequently operates in a manner that  
20                   prevents the user from accessing the Internet,

21          d.    changing the name, location or other designation  
22                   information of the software for the purpose of

- 1 preventing an authorized user from locating the  
2 software to remove it,
- 3 e. using randomized or intentionally deceptive file  
4 names, directory folders, formats, or registry entries  
5 for the purpose of avoiding detection and removal of  
6 the software by an authorized user,
- 7 f. causing the installation of software in a particular  
8 computer directory or computer memory for the purpose  
9 of evading attempts by authorized users to remove the  
10 software from the computer, or
- 11 g. requiring, without the authority of the owner of the  
12 computer, that an authorized user obtain a special  
13 code or download software from a third party to  
14 uninstall the software.

15 SECTION 5. NEW LAW A new section of law to be codified  
16 in the Oklahoma Statutes as Section 776.14 of Title 15, unless there  
17 is created a duplication in numbering, reads as follows:

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

- 20 1. Induce an owner or operator to install a computer software  
21 component onto the computer of the owner or operator by  
22 intentionally misrepresenting that installing computer software is

1 necessary for security or privacy reasons or in order to open, view,  
2 or play a particular type of content; or

3 2. Using intentionally deceptive means to cause the execution  
4 of a computer software component with the intent of causing the  
5 computer to use such component in a manner that violates any other  
6 provisions of the Computer Spyware Protection Act.

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

10 Sections 4 and 5 of the Computer Spyware Protection Act shall  
11 not apply to the monitoring of, or interaction with, the Internet or  
12 other network connection, service, or computer of an owner or  
13 operator, by a telecommunications carrier, cable operator, computer  
14 hardware or software provider, or provider of information service or  
15 interactive computer service for network or computer security  
16 purposes, diagnostics, technical support, maintenance, repair,  
17 network management, authorized updates of computer software or  
18 system firmware, authorized remote system management, or detection  
19 or prevention of the unauthorized use of or fraudulent or other  
20 illegal activities in connection with a network, service, or  
21 computer software, including scanning for and removing computer  
22 software prescribed under this act.

1 SECTION 7. NEW LAW A new section of law to be codified  
2 in the Oklahoma Statutes as Section 776.16 of Title 15, unless there  
3 is created a duplication in numbering, reads as follows:

4 A. The Attorney General for the State of Oklahoma, an Internet  
5 service provider or software company that expends resources in good  
6 faith assisting authorized users harmed by a violation of the  
7 Computer Spyware Protection Act, or a trademark owner whose mark is  
8 used to deceive authorized users in violation of this act, may bring  
9 a civil action against a person who violates any provision of this  
10 act to recover actual damages, liquidated damages of at least One  
11 Thousand Dollars (\$1,000.00) per violation of the act, not to exceed  
12 One Million Dollars (\$1,000,000.00) for a pattern or practice of  
13 such violations, attorney fees, and costs.

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

18 C. The court may reduce liquidated damages recoverable under  
19 subsection A of this section, to a minimum of One Hundred Dollars  
20 (\$100.00), not to exceed One Hundred Thousand Dollars (\$100,000.00)  
21 for each violation if the court finds that the defendant established  
22 and implemented practices and procedures reasonably designed to  
23 prevent a violation of this act.

1 D. In the case of a violation of subparagraph a of paragraph 6  
2 of Section 4 of this act that causes a telecommunications carrier or  
3 provider of Voice over Internet Protocol service to incur costs for  
4 the origination, transport, or termination of a call triggered using  
5 the modem or Internet-capable device of a customer of such  
6 telecommunications carrier or provider as a result of such  
7 violation, the telecommunications carrier may bring a civil action  
8 against the violator to recover any or all of the following:

9 1. The charges the carrier or provider is obligated to pay to  
10 another carrier or to an information service provider as a result of  
11 the violation, including, but not limited to, charges for the  
12 origination, transport or termination of the call;

13 2. Costs of handling customer inquiries or complaints with  
14 respect to amounts billed for such calls;

15 3. Costs and a reasonable attorney fee; and

16 4. An order to enjoin the violation.

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

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

1       A. No provider of computer software or of an interactive  
2 computer service may be held liable for identifying, naming,  
3 removing, disabling, or otherwise affecting a computer program  
4 through any action voluntarily undertaken, or service provided,  
5 where the provider:

6       1. Intends to identify accurately, prevent the installation or  
7 execution of, remove, or disable another computer program on a  
8 computer of a customer of such provider;

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

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

14       B. A provider of computer software or interactive computer  
15 service is entitled to protection under this section only if the  
16 provider:

17       1. Has established internal practices and procedures to  
18 evaluate computer programs reasonably designed to determine whether  
19 or not a computer program exhibits behavior that violates this act;  
20 and

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

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

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

6 COMMITTEE REPORT BY: COMMITTEE ON AEROSPACE, COMMUNICATIONS &  
7 TECHNOLOGY, dated 3-21-06 - DO PASS, As Amended.