



SPONSOR: Sen. McBride & Rep. Roy

DELAWARE STATE SENATE

143rd GENERAL ASSEMBLY

SENATE BILL NO. 124

AN ACT TO AMEND TITLE 6 OF THE DELAWARE CODE RELATING TO A COMPUTER SPYWARE PROTECTION ACT.

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

Section 1. Amend Title 6 of the Delaware Code by inserting therein a new Chapter 30 as follows:

“CHAPTER 30. COMPUTER SPYWARE PROTECTION.

§ 3001. Short title

This Chapter may be cited as the ‘Computer Spyware Protection Act.’

§ 3002. Legislative Intent

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 owner’s or the operator’s computer.

§ 3003. Definitions

The following words, terms and phrases, when used in this Chapter, shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

- (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 Web site operated for a commercial purpose.
- (2) ‘Computer software’ means a sequence of instructions written in any programming language this is executed on a computer. ‘Computer software’ does not include computer software that is a web page or data components of a web page that are not executable independently of the web page.
- (3) ‘Damage’ means any significant impairment to the integrity or availability of data, software, a system, or information.
- (4) ‘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.
- (5) ‘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.
- 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.

(6) 'Internet' means the same as defined in Section 4.1.

(7) 'Owner or operator' means the owner or lessee of a computer, or a person using such computer with the owner or lessee's authorization, but does not include a person who owned a computer prior to the first retail sale of the computer.

(8) 'Person' means the same as defined in Section 4.1.

(9) 'Personally identifiable information' means any of the following information with respect to 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. An electronic mail address.
- d. Credit or debit card number, bank account number, or any password or access code associated with a credit or debit card or bank account.
- e. Social security number, tax identification number, driver's license number, passport number, or any other government issued identification number.
- f. Account balance, overdraft history, or payment history that personally identifies an owner or operator of a computer.

(10) 'Transmit' means to transfer, send, or make available computer software using the Internet or any other medium, including local area networks of computers other than a wireless transmission, and a disc or other data storage device.

'Transmit' does not include an action by a person providing any of the following:

- a. An Internet connection, telephone connection, or other means of transmission capability such as a compact disc or digital video disc through which the computer software was made available.
- b. The storage or hosting of the computer software program or an Internet web page through which the software was made available.

- 48 c. An information location tool, such as a directory, index, reference, pointer, or hypertext link, through which
49 the user of the computer located the computer software, unless the person transmitting receives a direct
50 economic benefit from the execution of such software on the computer.

51 Section 4. Prohibitions, Transmission, And Use of Software.

52 It is unlawful for a person who is not an owner or operator of a computer to transmit computer software to such
53 computer knowingly or with conscious avoidance of actual knowledge, and to use such software to do any of the
54 following:

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

- 56 a. The web page that appears when an owner or operator launches an Internet browser or similar computer
57 software used to access and navigate the Internet.
58 b. The default provider or web proxy that an owner or operator uses to access or search the Internet.

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

- 61 a. The use of a keystroke-logging function that records keystrokes made by an owner or operator of a computer
62 and transfers that information from the computer to another person.
63 b. In a manner that correlates personally identifiable information with data respecting all or substantially all of
64 the Web sites visited by an owner or operator, other than Web sites operated by the person collecting such
65 information.
66 c. Prevent, through intentionally deceptive means, an owner's or an operator's reasonable efforts to block the
67 installation of, or to disable, computer software by causing computer software that the owner or operator has
68 properly removed or disabled to automatically reinstall or reactivate on the computer.

69 (3) Take control of an owner's or an operator's computer by doing any of the following:

- 70 a. Accessing or using a modem or Internet service for the purpose of causing damage to an owner's or an
71 operator's computer or causing an owner or operator to incur financial charges for a service that the owner or
72 operator did not authorize.
73 b. Opening multiple, sequential, stand-alone advertisements in an owner's or an operator's Internet browser
74 without the authorization of an owner or operator and which a reasonable computer user could not close
75 without turning off the computer or closing the Internet browser.

76 (4) Modify any of the following settings related to an owner's or an operator's computer access to, 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.

(5) Prevent 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:

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.

§ 3005. 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 executive of a computer software component with the intent of causing an owner or operator to use such component in a manner that violates any other provision of this chapter.

§ 3006. Exceptions

Sections 3004 and 3005 of this Title 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, 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 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 chapter.

§ 3007. Remedies

Violations of this Chapter shall be addressed as civil matters in one of the following ways:

- (1) The Attorney General may bring a civil action against a person who violates any provision of this chapter to recover actual damages, liquidated damages of at least one thousand dollars, not to exceed one million dollars, for each violation, attorney fees, and costs.
- (2) Upon motion of a party or on its own volition, a court may increase a damage award made pursuant to this section to an amount equal to not more than three times the amount otherwise recoverable under paragraph (1) of this section if the court determines that the defendant committed the violation willfully and knowingly.
- (3) Upon motion of a party or on its own volition, a court may reduce liquidated damages recoverable under paragraph (1) of this section, to a minimum of one hundred dollars, not to exceed one hundred thousand dollars for each violation if the court finds that the defendant established and implemented practices and procedures reasonably designed to prevent a violation of this chapter.”

Section 2. If any provision or clause of this Act or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this Act which can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

Section 3. This Act shall become effective 6 months following its enactment into law.

SYNOPSIS

Spyware is a catch-all term for computer programs that can track computer users’ movements online. There are hundreds of programs that range from innocuous ‘ad-ware,’ which generates pop-up advertisements, to more dangerous programs that can record a user’s keystrokes to gather personal information such as credit card numbers and passwords without their knowledge and forward this information to another entity without the consumer’s consent. Spyware is a serious problem that can create substantial privacy risks, increase the risk of identity theft, and cause serious degradation to personal and business computers that can cost millions of dollars in lost productivity and the purchase of anti-spyware software.

This Act prohibits the installation, transmission, and use of computer software that collects personally identifiable information, and authorizes the Attorney General to bring a civil action against anyone who violates any provision of this act and seek damages ranging from \$1,000 to \$1 million.

Author: Senator McBride