CHAPTER 715

COMPUTER SPYWARE AND MALWARE PROTECTION

Referred to in §331.307, 364.22, 701.1

715.1 Legislative intent.

It is the intent of the general assembly 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.

2005 Acts, ch 94, §1

715.2 Title.

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

2005 Acts, ch 94, §2

715.3 Definitions.

For purposes of this chapter, unless the context otherwise requires:

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 site operated for a commercial purpose.
2. "*Computer software*" means a sequence of instructions written in any programming language that is executed on a computer. "*Computer software*" does not include computer software that is an internet site or data components of an internet site that are not executable independently of the internet site.
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 site through which the software was made available.

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

2005 Acts, ch 94, §3; 2013 Acts, ch 90, §190, 191, 257

715.4 Prohibitions — transmission and use of software.

It is unlawful for a person who is not an owner or operator of a computer to transmit computer software to such computer knowingly or with conscious avoidance of actual knowledge, and to use such 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 internet site that appears when an owner or operator launches an internet browser or similar computer software used to access and navigate the internet.

b. The default provider or internet proxy that an owner or operator uses to access or search the internet.

c. An owner's or an operator's list of bookmarks used to access internet sites.

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 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 respecting all or substantially all of the internet sites visited by an owner or operator, other than internet sites operated by the person collecting such information.

c. By extracting from the hard drive of an owner's or an operator's computer, an owner's or an operator's social security number, tax identification number, driver's license number, passport number, any other government-issued identification number, account balances, or overdraft history.

3. Prevent, through intentionally deceptive means, an owner's or an operator's reasonable efforts to block the installation 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.

4. Intentionally misrepresent that computer software will be uninstalled or disabled by an owner's or an operator's action.

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

6. Take control of an owner's or an operator's computer by doing any of the following:

a. Accessing or using a modem or internet service for the purpose of causing damage to an owner's or an operator's computer or causing an owner or operator to incur financial charges for a service that the owner or operator did not authorize.

b. Opening multiple, sequential, stand-alone advertisements in an owner's or an operator's internet browser without the authorization of an owner or operator and which a reasonable computer user could not close without turning off the computer or closing the internet browser.

7. 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.

8. 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.

2005 Acts, ch 94, §4; 2013 Acts, ch 90, §192, 257
Referred to in §715.6

715.5 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 execution 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.

2005 Acts, ch 94, §5
Referred to in §715.6

715.6 Exceptions.

Sections 715.4 and 715.5 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, criminal investigation, or prevention of the use of or fraudulent or other illegal activities prohibited in this chapter in connection with a network, service, or computer software, including scanning for and removing computer software prescribed under this chapter. Nothing in this chapter shall limit the rights of providers of wire and electronic communications under 18 U.S.C. §2511.

2005 Acts, ch 94, §6; 2007 Acts, ch 126, §108; 2007 Acts, ch 215, §257

715.7 Criminal penalties.

1. A person who commits an unlawful act under this chapter is guilty of an aggravated misdemeanor.

2. A person who commits an unlawful act under this chapter and who causes pecuniary losses exceeding one thousand dollars to a victim of the unlawful act is guilty of a class "D" felony.

2005 Acts, ch 94, §7

715.8 Venue for criminal violations.

For the purpose of determining proper venue, a violation of this chapter shall be considered to have been committed in any county in which any of the following apply:

1. An act was performed in furtherance of the violation.

2. The owner or operator who is the victim of the violation has a place of business in this state.

3. The defendant has control or possession of any proceeds of the violation, or of any books, records, documents, property, financial instrument, computer software, computer program, computer data, or other material or objects used in furtherance of the violation.

4. The defendant unlawfully accessed a computer or computer network by wires, electromagnetic waves, microwaves, or any other means of communication.

5. The defendant resides.

6. A computer used as an object or an instrument in the commission of the violation was located at the time of the violation.

2005 Acts, ch 94, §8