CHAPTER 715

COMPUTER SPYWARE, MALWARE, AND RANSOMWARE PROTECTION

Referred to in §331.307, 364.22, 701.1

SUBCHAPTER I

INTENT AND DEFINITIONS

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, Malware, and Ransomware Protection Act"*.

2005 Acts, ch 94, §2; 2023 Acts, ch 77, §1
Section amended

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 control language"* means ordered statements that direct a computer to perform specific functions.

3. *"Computer database"* means a representation of information, knowledge, facts, concepts, or instructions that is intended for use in a computer, computer system, or computer network that is being prepared or has been prepared in a formalized manner, or is being produced or has been produced by a computer, computer system, or computer network.

4. *"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.

5. *"Damage"* means any significant impairment to the integrity or availability of data, software, a system, or information.

6. *"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.

7. *"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.

8. *"Internet"* means the same as defined in section 4.1.

9. *"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.

10. *"Person"* means the same as defined in section 4.1.

11. *"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.

12. *"Ransomware"* means a computer or data contaminant, encryption, or lock that is placed or introduced without authorization into a computer, computer network, or computer system that restricts access by an authorized person to a computer, computer data, a computer system, or a computer network in a manner that results in the person responsible for the placement or introduction of the contaminant, encryption, or lock making a demand for payment of money or other consideration to remove the contaminant, encryption, or lock.

13. *"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; 2023 Acts, ch 77, §2
NEW subsections 2 and 3 and former subsections 2 – 9 renumbered as 3 – 11
New subsection 12 and former subsection 10 renumbered as 13

SUBCHAPTER II

COMPUTER SPYWARE AND MALWARE

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 subchapter.

2005 Acts, ch 94, §5; 2023 Acts, ch 77, §3
Referred to in §715.6
Subsection 2 amended

715.6 Exceptions.

Sections 715.4 and 715.5 shall not apply to the following:

1. 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 subchapter. Nothing in this subchapter shall limit the rights of providers of wire and electronic communications under 18 U.S.C. §2511.

2. The nonpayment or a violation of the terms of a legal contract with the owner or operator.

3. For complying with federal, state, and local law enforcement requests.

2005 Acts, ch 94, §6; 2007 Acts, ch 126, §108; 2007 Acts, ch 215, §257; 2023 Acts, ch 77, §4
Section amended

715.7 Criminal penalties.

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

2. A person who commits an unlawful act under this subchapter 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; 2023 Acts, ch 77, §5
Section amended

715.8 Venue for criminal violations.

For the purpose of determining proper venue, a violation of this subchapter 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; 2023 Acts, ch 77, §6
Unnumbered paragraph 1 amended

SUBCHAPTER III

RANSOMWARE

715.9 Ransomware prohibition.

1. A person shall not intentionally, willfully, and without authorization do any of the following:

a. Access, attempt to access, cause to be accessed, or exceed the person's authorized access to all or a part of a computer network, computer control language, computer, computer software, computer system, or computer database.

b. Copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database accessed in violation of paragraph *"a"*.

2. A person shall not commit an act prohibited in subsection 1 with the intent to do any of the following:

a. Cause the malfunction or interruption of the operation of all or any part of a computer, computer network, computer control language, computer software, computer system, computer service, or computer data.

b. Alter, damage, or destroy all or any part of data or a computer program stored, maintained, or produced by a computer, computer network, computer software, computer system, computer service, or computer database.

3. A person shall not intentionally, willfully, and without authorization do any of the following:

a. Possess, identify, or attempt to identify a valid computer access code.

b. Publicize or distribute a valid computer access code to an unauthorized person.

4. A person shall not commit an act prohibited under this section with the intent to interrupt or impair the functioning of any of the following:

a. The state.

b. A service, device, or system related to the production, transmission, delivery, or storage of electricity or natural gas in the state that is owned, operated, or controlled by a person other than a public utility as defined in chapter 476.

c. A service provided in the state by a public utility as defined in section 476.1, subsection 2.

d. A hospital or health care facility as defined in section 135C.1.

e. A public elementary or secondary school, community college, or area education agency under the supervision of the department of education.

f. A city, city utility, or city service.

g. An authority as defined in section 330A.2.

5. This section shall not apply to the use of ransomware for research purposes by a person who has a bona fide scientific, educational, governmental, testing, news, or other similar justification for possessing ransomware. However, a person shall not knowingly possess ransomware with the intent to use the ransomware for the purpose of introduction into the computer, computer network, or computer system of another person without the authorization of the other person.

6. A person who has suffered a specific and direct injury because of a violation of this section may bring a civil action in a court of competent jurisdiction.

a. In an action under this subsection, the court may award actual damages, reasonable attorney fees, and court costs.

b. A conviction for an offense under this section is not a prerequisite for the filing of a civil action.

2023 Acts, ch 77, §7
NEW section

715.10 Criminal penalties.

1. A person who commits an unlawful act under this subchapter and who causes pecuniary losses involving less than ten thousand dollars to a victim of the unlawful act is guilty of an aggravated misdemeanor.

2. A person who commits an unlawful act under this subchapter and who causes pecuniary losses involving at least ten thousand dollars but less than fifty thousand dollars to a victim of the unlawful act is guilty of a class "D" felony.

3. A person who commits an unlawful act under this subchapter and who causes pecuniary losses involving at least fifty thousand dollars to a victim of the unlawful act is guilty of a class "C" felony.

2023 Acts, ch 77, §8
NEW section

715.11 Venue.

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

1. Where the defendant performed the unlawful act.
2. Where the defendant resides.
3. Where the accessed computer is located.

2023 Acts, ch 77, §9
NEW section