HB3987

LRB09907386RLC27502b

99TH GENERAL ASSEMBLY

State of Illinois

2015 and 2016

HB3987

by Rep. Barbara Wheeler

SYNOPSIS AS INTRODUCED:

720 ILCS 5/17-52.5 was 720 ILCS 5/16D-5.5
720 ILCS 5/17-55

Amends the Criminal Code of 2012. Expands the definition of "computer" to include equipment of cloud-based networks of remote servers hosted on the Internet to store, manage, and process data. Makes the definition of "computer" apply to multiple provisions under the computer fraud subdivision of the Code.

LRB099 07386 RLC 27502 b

A BILL FOR

AN ACT concerning criminal law.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 5. The Criminal Code of 2012 is amended by changing Sections 17-52.5 and 17-55 as follows:

(720 ILCS 5/17-52.5) (was 720 ILCS 5/16D-5.5)

Sec. 17-52.5. Unlawful use of encryption.

(a) For the purpose of this Section:

~~"Computer" means an electronic device which performs logical, arithmetic, and memory functions by manipulations of electronic or magnetic impulses and includes all equipment related to the computer in a system or network.~~

"Computer contaminant" means any data, information, image, program, signal, or sound that is designated or has the capability to: (1) contaminate, corrupt, consume, damage, destroy, disrupt, modify, record, or transmit; or (2) cause to be contaminated, corrupted, consumed, damaged, destroyed, disrupted, modified, recorded, or transmitted, any other data, information, image, program, signal, or sound contained in a computer, system, or network without the knowledge or consent of the person who owns the other data, information, image, program, signal, or sound or the computer, system, or network.

"Computer contaminant" includes, without limitation: (1) a virus, worm, or Trojan horse; (2) spyware that tracks computer activity and is capable of recording and transmitting such information to third parties; or (3) any other similar data, information, image, program, signal, or sound that is designed or has the capability to prevent, impede, delay, or disrupt the normal operation or use of any component, device, equipment, system, or network.

"Encryption" means the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding, or a computer contaminant, to: (1) prevent, impede, delay, or disrupt access to any data, information, image, program, signal, or sound; (2) cause or make any data, information, image, program, signal, or sound unintelligible or unusable; or (3) prevent, impede, delay, or disrupt the normal operation or use of any component, device, equipment, system, or network.

"Network" means a set of related, remotely connected devices and facilities, including more than one system, with the capability to transmit data among any of the devices and facilities. The term includes, without limitation, a local, regional, or global computer network.

"Program" means an ordered set of data representing coded instructions or statements which can be executed by a computer and cause the computer to perform one or more

tasks.

"System" means a set of related equipment, whether or not connected, which is used with or for a computer.

(b) A person shall not knowingly use or attempt to use encryption, directly or indirectly, to:

(1) commit, facilitate, further, or promote any criminal offense;

(2) aid, assist, or encourage another person to commit any criminal offense;

(3) conceal evidence of the commission of any criminal offense; or

(4) conceal or protect the identity of a person who has committed any criminal offense.

(c) Telecommunications carriers and information service providers are not liable under this Section, except for willful and wanton misconduct, for providing encryption services used by others in violation of this Section.

(d) Sentence. A person who violates this Section is guilty of a Class A misdemeanor, unless the encryption was used or attempted to be used to commit an offense for which a greater penalty is provided by law. If the encryption was used or attempted to be used to commit an offense for which a greater penalty is provided by law, the person shall be punished as prescribed by law for that offense.

(e) A person who violates this Section commits a criminal offense that is separate and distinct from any other criminal

offense and may be prosecuted and convicted under this Section whether or not the person or any other person is or has been prosecuted or convicted for any other criminal offense arising out of the same facts as the violation of this Section.

(Source: P.A. 95-942, eff. 1-1-09; 96-1551, eff. 7-1-11.)

(720 ILCS 5/17-55)

Sec. 17-55. Definitions. For the purposes of Sections 17-50 through 17-53:

In addition to its meaning as defined in Section 15-1 of this Code, "property" means: (1) electronic impulses; (2) electronically produced data; (3) confidential, copyrighted, or proprietary information; (4) private identification codes or numbers which permit access to a computer by authorized computer users or generate billings to consumers for purchase of goods and services, including but not limited to credit card transactions and telecommunications services or permit electronic fund transfers; (5) software or programs in either machine or human readable form; or (6) any other tangible or intangible item relating to a computer or any part thereof.

"Access" means to use, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise utilize any services of, a computer, a network, or data.

"Computer" means an electronic device which performs logical, arithmetic, and memory functions by manipulations of electronic or magnetic impulses and includes all equipment

related to the computer in a system or network and cloud-based networks of remote services hosted on the Internet to store, manage, and process data.

"Services" includes but is not limited to computer time, data manipulation, or storage functions.

"Vital services or operations" means those services or operations required to provide, operate, maintain, and repair network cabling, transmission, distribution, or computer facilities necessary to ensure or protect the public health, safety, or welfare. Those services or operations include, but are not limited to, services provided by medical personnel or institutions, fire departments, emergency services agencies, national defense contractors, armed forces or militia personnel, private and public utility companies, or law enforcement agencies.

(Source: P.A. 96-1551, eff. 7-1-11.)