



## 98TH GENERAL ASSEMBLY

### State of Illinois

2013 and 2014

HB5768

by Rep. Barbara Wheeler

#### SYNOPSIS AS INTRODUCED:

720 ILCS 5/17-52.5  
720 ILCS 5/17-55

was 720 ILCS 5/16D-5.5

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.

LRB098 19320 JLK 54472 b

1 AN ACT concerning criminal law.

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

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

6 (720 ILCS 5/17-52.5) (was 720 ILCS 5/16D-5.5)

7 Sec. 17-52.5. Unlawful use of encryption.

8 (a) For the purpose of this Section:

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

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

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

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

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

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

1 tasks.

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

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

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

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

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

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

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

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

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

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

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

6 (720 ILCS 5/17-55)

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

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

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

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

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

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

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

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