



Rep. Darlene J. Senger

Filed: 3/6/2012

09700HB4642ham001

LRB097 13960 RLC 67017 a

1 AMENDMENT TO HOUSE BILL 4642

2 AMENDMENT NO. _____. Amend House Bill 4642 on page 1, line
3 5, by inserting ", 17-52.5," after "17-51"; and

4 on page 6, by inserting immediately after line 26 the
5 following:

6 "(d) Telecommunications carriers, commercial mobile
7 service providers, and providers of information services,
8 including, but not limited to, Internet service providers and
9 hosting service providers, are not liable under this Section,
10 except for willful and wanton misconduct, by virtue of the
11 transmission, storage, or caching of electronic communications
12 or messages of others or by virtue of the provision of other
13 related telecommunications, commercial mobile services, or
14 information services used by others in violation of this
15 Section."; and

16 on page 7, by inserting immediately below line 2 the following:

1 "(720 ILCS 5/17-52.5) (was 720 ILCS 5/16D-5.5)

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

3 (a) For the purpose of this Section:

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

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

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

1 any component, device, equipment, system, or network.

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

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

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

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

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

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

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

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

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

7 (c) Telecommunications carriers, commercial mobile service
8 providers, and providers of information services, including,
9 but not limited to, Internet service providers and hosting
10 service providers, are not liable under this Section, except
11 for willful and wanton misconduct, by virtue of the
12 transmission, storage, or caching of electronic communications
13 or messages of others or by virtue of the provision of other
14 related telecommunications, commercial mobile services, or
15 information services used by others in violation of this
16 Section. ~~Telecommunications carriers and information service~~
17 ~~providers are not liable under this Section, except for willful~~
18 ~~and wanton misconduct, for providing encryption services used~~
19 ~~by others in violation of this Section.~~

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

1 (e) A person who violates this Section commits a criminal
2 offense that is separate and distinct from any other criminal
3 offense and may be prosecuted and convicted under this Section
4 whether or not the person or any other person is or has been
5 prosecuted or convicted for any other criminal offense arising
6 out of the same facts as the violation of this Section.
7 (Source: P.A. 95-942, eff. 1-1-09; 96-1551, eff. 7-1-11.)".