

1 AN ACT concerning business.

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

4 Section 1. This Act may be cited as the Illinois Spyware  
5 Prevention Initiative Act.

6 Section 5. Definitions. In this Act:

7 "Advertisement" means a communication, the primary purpose  
8 of which is the commercial promotion of a commercial product or  
9 service, including content on an Internet web site operated for  
10 a commercial purpose.

11 "Authorized user", with respect to a computer, means a  
12 person who owns or is authorized by the owner or lessee to use  
13 the computer. "Authorized user" does not include a person or  
14 entity that has obtained authorization to use the computer  
15 solely through the use of an end user license agreement.

16 "Computer software" means a sequence of instructions  
17 written in any programming language that is executed on a  
18 computer.

19 "Computer virus" means a computer program or other set of  
20 instructions that is designed to degrade the performance of or  
21 disable a computer or computer network and is designed to have  
22 the ability to replicate itself on other computers or computer  
23 networks without the authorization of the owners of those  
24 computers or computer networks.

25 "Consumer" means an individual who resides in this State  
26 and who uses the computer in question primarily for personal,  
27 family, or household purposes.

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

30 "Deceptive" means any one of the following:

31 (1) By means of materially false or fraudulent  
32 statement.

1           (2) By means of a statement or description that omits  
2           or misrepresents material information in order to deceive  
3           the consumer.

4           (3) By means of material failure to provide any notice  
5           to an authorized user regarding the download or  
6           installation of software in order to deceive the consumer.

7           "Execute", when used with respect to computer software,  
8           means the performance of the functions of the carrying out of  
9           the instructions of the computer software.

10          "Internet" means the global information system that is  
11          logically linked together by a globally unique address space  
12          based on the Internet Protocol (IP), or its subsequent  
13          extensions, and that is able to support communications using  
14          the Transmission Control Protocol/Internet Protocol (TCP/IP)  
15          suite, or its subsequent extensions, or other IP-compatible  
16          protocols, and that provides, uses, or makes accessible, either  
17          publicly or privately, high level services layered on the  
18          communications and related infrastructure.

19          "Person" means any individual, partnership, corporation,  
20          limited liability company, or other organization, or any  
21          combination thereof.

22          "Personally identifiable information" means any one of the  
23          following:

24                (1) First name or first initial in combination with  
25                last name.

26                (2) Credit or debit card numbers or other financial  
27                account numbers.

28                (3) A password or personal identification number  
29                required to access an identified financial account.

30                (4) Social security number.

31                (5) Any of the following information in a form that  
32                personally identifies an authorized user: (i) account  
33                balances; (ii) overdraft history; (iii) payment history;  
34                (iv) a history of Web sites visited; (v) home address; (vi)  
35                work address; or (vii) a record of a purchase or purchases.

1 Section 10. Computer spyware; authorized user. A person or  
2 entity that is not an authorized user shall not, with actual  
3 knowledge, with conscious avoidance of actual knowledge, or  
4 willfully, cause computer software to be copied onto a  
5 consumer's computer and use the software to do any of the  
6 following:

7 (1) Modify, through deceptive means, any of the  
8 following settings related to the computer's access to, or  
9 use of, the Internet:

10 (A) The page that appears when an authorized user  
11 launches an Internet browser or similar software  
12 program used to access and navigate the Internet.

13 (B) The default provider or Web proxy an authorized  
14 user uses to access or search the Internet.

15 (C) An authorized user's list of bookmarks used to  
16 access Web pages.

17 (2) Collect, through deceptive means, personally  
18 identifiable information that meets any of the following  
19 criteria:

20 (A) It is collected through the use of a  
21 keystroke-logging function that records all keystrokes  
22 made by an authorized user who uses the computer and  
23 transfers that information from the computer to  
24 another person.

25 (B) It includes all or substantially all of the Web  
26 sites visited by an authorized user, other than Web  
27 sites of the provider of the software, if the computer  
28 software was installed in a manner designed to conceal  
29 from all authorized users of the computer the fact that  
30 the software is being installed.

31 (C) It is a data element that is extracted from the  
32 consumer's computer hard drive for a purpose wholly  
33 unrelated to any of the purposes of the software or  
34 service described to an authorized user.

35 (3) Prevent, without the authorization of an  
36 authorized user, through deceptive means, an authorized

1 user's reasonable efforts to block the installation of, or  
2 to disable software by causing software that the authorized  
3 user has properly removed or disabled to automatically  
4 reinstall or reactivate on the computer without the  
5 authorization of an authorized user.

6 (4) Misrepresent that software will be uninstalled or  
7 disabled by an authorized user's action, with knowledge  
8 that the software will not be so uninstalled or disabled.

9 (5) Through deceptive means, remove, disable, or  
10 render inoperative security, antispyware, or antivirus  
11 software installed on the computer.

12 Section 15. Computer spyware; unauthorized user.

13 (a) A person or entity that is not an authorized user shall  
14 not, with actual knowledge, with conscious avoidance of actual  
15 knowledge, or willfully, cause computer software to be copied  
16 onto a consumer's computer and use the software to do any of  
17 the following:

18 (1) Take control of the consumer's computer by doing  
19 any of the following:

20 (A) Transmit or relay commercial electronic mail  
21 or a computer virus from the consumer's computer, where  
22 the transmission or relaying is initiated by a person  
23 other than the authorized user and without the  
24 authorization of an authorized user.

25 (B) Access or use the consumer's modem or Internet  
26 service for the purpose of causing damage to the  
27 consumer's computer or of causing an authorized user to  
28 incur financial charges for a service that is not  
29 authorized by an authorized user.

30 (C) Use the consumer's computer as part of an  
31 activity performed by a group of computers for the  
32 purpose of causing damage to another computer,  
33 including, but not limited to, launching a denial of  
34 service attack.

35 (D) Open multiple, sequential, stand-alone

1 advertisements in the consumer's Internet browser  
2 without the authorization of an authorized user and  
3 with knowledge that a reasonable computer user cannot  
4 close the advertisements without turning off the  
5 computer or closing the consumer's Internet browser.

6 (2) Modify any of the following settings related to the  
7 computer's access to, or use of, the Internet:

8 (A) An authorized user's security or other  
9 settings that protect information about the authorized  
10 user for the purpose of stealing personal information  
11 of an authorized user.

12 (B) The security settings of the computer for the  
13 purpose of causing damage to one or more computers.

14 (3) Prevent, without the authorization of an  
15 authorized user, an authorized user's reasonable efforts  
16 to block the installation of, or to disable software, by  
17 doing any of the following:

18 (A) Present the authorized user with an option to  
19 decline installation of software with knowledge that,  
20 when the option is selected by the authorized user, the  
21 installation will nevertheless occur.

22 (B) Falsely represent that software has been  
23 disabled.

24 (b) Nothing in this Section shall apply to any monitoring  
25 of, or interaction with, a subscriber's Internet or other  
26 network connection or service, or a protected computer, by a  
27 telecommunications carrier, cable operator, computer hardware  
28 or software provider, or provider of information service or  
29 interactive computer service for network or computer security  
30 purposes, diagnostics, technical support, repair, authorized  
31 updates of software or system firmware, authorized remote  
32 system management, or detection or prevention of the  
33 unauthorized use of or fraudulent or other illegal activities  
34 in connection with a network, service, or computer software,  
35 including scanning for and removing software proscribed under  
36 this Act.

1 Section 20. Spyware installation misrepresentation.

2 (a) A person or entity, who is not an authorized user,  
3 shall not do any of the following with regard to the computer  
4 of a consumer in this State:

5 (1) Induce an authorized user to install a software  
6 component onto the computer by misrepresenting that  
7 installing software is necessary for security or privacy  
8 reasons or in order to open, view, or play a particular  
9 type of content.

10 (2) Deceptively cause the copying and execution on the  
11 computer of a computer software component with the intent  
12 of causing an authorized user to use the component in a way  
13 that violates any other provision of this Section.

14 (b) Nothing in this Section shall apply to any monitoring  
15 of, or interaction with, a subscriber's Internet or other  
16 network connection or service, or a protected computer, by a  
17 telecommunications carrier, cable operator, computer hardware  
18 or software provider, or provider of information service or  
19 interactive computer service for network or computer security  
20 purposes, diagnostics, technical support, repair, authorized  
21 updates of software or system firmware, authorized remote  
22 system management, or detection or prevention of the  
23 unauthorized use of or fraudulent or other illegal activities  
24 in connection with a network, service, or computer software,  
25 including scanning for and removing software proscribed under  
26 this Act.

27 Section 25. Penalty.

28 (a) A person who violates Section 10, 15, or 20 of this Act  
29 shall be guilty of a Class B misdemeanor.

30 (b) Absolute liability as provided under Section 4-9 of the  
31 Criminal Code of 1961 shall be imposed for a violation of  
32 Section 20.

33 Section 30. Severability. If any provision of this Act or

1 its application to any person or circumstance is held invalid,  
2 the invalidity of that provision or application does not affect  
3 other provisions or applications of this Act that can be given  
4 effect without the invalid provision or application.