

## HOUSE BILL No. 2343

By Representative Holland

2-8

---

9 AN ACT concerning computers; enacting the consumer protection  
10 against computer spyware act; prohibiting certain acts and providing  
11 penalties for violations.  
12

13 *Be it enacted by the Legislature of the State of Kansas:*

14 Section 1. This act shall be known and may be cited as the consumer  
15 protection against computer spyware act.

16 Sec. 2. For purposes of this act:

17 (a) "Advertisement" means a communication, the primary purpose  
18 of which is the commercial promotion of a commercial product or service,  
19 including content on an internet site operated for a commercial purpose.

20 (b) "Authorized user", with respect to a computer, means a person  
21 who owns or is authorized by the owner or lessee to use the computer.  
22 Authorized user does not include a person that has obtained authorization  
23 to use the computer solely through the use of an end-user license  
24 agreement.

25 (c) "Computer software" means a sequence of instructions written in  
26 any programming language that is executed on a computer.

27 (d) "Computer virus" means a computer program or other set of in-  
28 structions that is designed to degrade the performance of or disable a  
29 computer or computer network and is designed to have the ability to  
30 replicate itself on other computers or computer networks without the  
31 authorization of the owners of those computers or computer networks.

32 (e) "Consumer" means an individual who resides in this state and  
33 who uses the computer in question.

34 (f) "Damage" means any significant impairment to the integrity or  
35 availability of data, computer software, a system or information.

36 (g) "Execute", when used with respect to computer software, means  
37 the performance of the functions or the carrying out of the instructions  
38 of the computer software.

39 (h) "Intentionally deceptive" means any of the following:

40 (1) By means of an intentionally and materially false or fraudulent  
41 statement;

42 (2) by means of a statement or description that intentionally omits or  
43 misrepresents material information in order to deceive the consumer; or

- 1 (3) by means of an intentional and material failure to provide any  
2 notice to an authorized user regarding the download or installation of  
3 computer software in order to deceive the consumer.
- 4 (i) "Internet" means the global information system that is logically  
5 linked together by a globally unique address space based on the internet  
6 protocol, or its subsequent extensions, and that is able to support com-  
7 munications using the transmission control protocol/internet protocol  
8 suite, or its subsequent extensions, or other internet protocol compatible  
9 protocols, and that provides, uses, or makes accessible, either publicly or  
10 privately, high-level services layered on the communications and related  
11 infrastructure described in this subdivision.
- 12 (j) "Person" means any individual, association, partnership, corpora-  
13 tion, limited liability company or other entity.
- 14 (k) "Personally identifiable information" means any of the following:  
15 (1) First name or first initial in combination with last name;  
16 (2) credit or debit card numbers or other financial account numbers;  
17 (3) a password or personal identification number required to access  
18 an identified financial account;  
19 (4) social security number;  
20 (5) any of the following information in a form that personally iden-  
21 tifies an authorized user:  
22 (A) Account balances;  
23 (B) overdraft history;  
24 (C) payment history;  
25 (D) history of web sites visited;  
26 (E) home address;  
27 (F) work address; or  
28 (G) record of a purchase.
- 29 Sec. 3. A person that is not an authorized user shall not, with actual  
30 knowledge, with conscious avoidance of actual knowledge or willfully,  
31 cause computer software to be copied onto the computer of a consumer  
32 in this state and use the computer software to do any of the following:  
33 (a) Modify, through intentionally deceptive means, any of the follow-  
34 ing settings related to the computer's access to, or use of, the internet:  
35 (1) The page that appears when an authorized user launches an in-  
36 ternet browser or similar software program used to access and navigate  
37 the internet;  
38 (2) the default provider or web proxy the authorized user uses to  
39 access or search the internet; or  
40 (3) the authorized user's list of bookmarks used to access web sites.  
41 (b) Collect, through intentionally deceptive means, personally iden-  
42 tifiable information that meets any of the following criteria:  
43 (1) It is collected through the use of a keystroke-logging function that

1 records all keystrokes made by an authorized user who uses the computer  
2 and transfers that information from the computer to another person; or

3 (2) it includes all or substantially all of the web sites visited by an  
4 authorized user, other than web sites of the provider of the software, if  
5 the computer software was installed in a manner designed to conceal from  
6 all authorized users of the computer the fact that the software is being  
7 installed;

8 (3) it is a data element described in subsection (k)(2), (3), (4), (5)(A),  
9 or (5)(B) of section 2, and amendments thereto, that is extracted from  
10 the consumer's computer hard drive for a purpose wholly unrelated to  
11 any of the purposes of the computer software or service described to an  
12 authorized user.

13 (c) Prevent, without the authorization of an authorized user, through  
14 intentionally deceptive means, an authorized user's reasonable efforts to  
15 block the installation of, or to disable, computer software, by causing  
16 computer software that the authorized user has properly removed or dis-  
17 abled to automatically reinstall or reactivate on the computer without the  
18 authorization of an authorized user.

19 (d) Intentionally misrepresent that computer software will be unin-  
20 stalled or disabled by an authorized user's action, with knowledge that  
21 the computer software will not be so uninstalled or disabled.

22 (e) Through intentionally deceptive means, remove, disable or render  
23 inoperative security, antispyware or antivirus computer software installed  
24 on the computer.

25 Sec. 4. (a) A person that is not an authorized user shall not, with  
26 actual knowledge, with conscious avoidance of actual knowledge or will-  
27 fully, cause computer software to be copied onto the computer of a con-  
28 sumer in this state and use the computer software to do any of the  
29 following:

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

32 (A) Transmitting or relaying commercial electronic mail or a com-  
33 puter virus from the consumer's computer if the transmission or relaying  
34 is initiated by a person other than the authorized user and without the  
35 authorization of an authorized user;

36 (B) accessing or using the consumer's modem or internet service for  
37 the purpose of causing damage to the consumer's computer or of causing  
38 an authorized user to incur financial charges for a service that is not  
39 authorized by an authorized user;

40 (C) using the consumer's computer as part of an activity performed  
41 by a group of computers for the purpose of causing damage to another  
42 computer, including, but not limited to, launching a denial of service  
43 attack; or

- 1 (D) opening multiple, sequential, stand-alone advertisements in the  
2 consumer's internet browser without the authorization of an authorized  
3 user and with knowledge that a reasonable computer user cannot close  
4 the advertisements without turning off the computer or closing the con-  
5 sumer's internet browser; or
- 6 (2) modify any of the following settings related to the computer's  
7 access to, or use of, the internet:
- 8 (A) An authorized user's security or other settings that protect infor-  
9 mation about the authorized user, for the purpose of stealing personal  
10 information of an authorized user; or
- 11 (B) the security settings of the computer, for the purpose of causing  
12 damage to one or more computers; or
- 13 (3) prevent, without the authorization of an authorized user, an au-  
14 thorized user's reasonable efforts to block the installation of, or to disable,  
15 computer software, by doing any of the following:
- 16 (A) Presenting the authorized user with an option to decline instal-  
17 lation of computer software with knowledge that, when the option is se-  
18 lected by the authorized user, the installation nevertheless proceeds; or
- 19 (B) falsely representing that computer software has been disabled.
- 20 (b) This section shall not apply to any monitoring of, or interaction  
21 with, a subscriber's internet or other network connection or service, or a  
22 protected computer, by a telecommunications carrier, cable operator,  
23 computer hardware or software provider or provider of information serv-  
24 ice or interactive computer service for computer network or computer  
25 security purposes, diagnostics, technical support, repair, authorized up-  
26 dates of computer software or system firmware, authorized remote system  
27 management, or detection or prevention of the unauthorized use of or  
28 fraudulent or other illegal activities in connection with a network, service,  
29 or computer software, including scanning for and removing computer  
30 software prescribed under this act.
- 31 Sec. 5. (a) A person who is not an authorized user shall not do any  
32 of the following with regard to the computer of a consumer in this state:
- 33 (1) Induce an authorized user to install a software component onto  
34 the computer by intentionally misrepresenting that installing computer  
35 software is necessary for security or privacy reasons or in order to open,  
36 view or play a particular type of content; or
- 37 (2) deceptively causing the copying and execution on the computer  
38 of a computer software component with the intent of causing an author-  
39 ized user to use the computer software component in a way that violates  
40 any other provision of this section.
- 41 (b) This section shall not apply to any monitoring of, or interaction  
42 with, a subscriber's internet or other network connection or service, or a  
43 protected computer, by a telecommunications carrier, cable operator,

1 computer hardware or software provider, or provider of information serv-  
2 ice or interactive computer service for computer network or computer  
3 security purposes, diagnostics, technical support, repair, authorized up-  
4 dates of computer software or system firmware, authorized remote system  
5 management, or detection or prevention of the unauthorized use of or  
6 fraudulent or other illegal activities in connection with a network, service,  
7 or computer software, including scanning for and removing computer  
8 software prescribed under this act.

9 Sec. 6. (a) The task force on computer technology and privacy is  
10 hereby established. The task force shall:

11 (1) Examine the problems associated with computer privacy and  
12 unauthorized access;

13 (2) make recommendations regarding enforcement of this act and  
14 enforcement cooperation with other states;

15 (3) make recommendations for implementation of this act; and

16 (4) make recommendations for additional necessary legislation con-  
17 cerning computer privacy and unauthorized computer access.

18 The task force shall submit a written report and any recommendations  
19 to the governor and the legislature on or before the first day of the regular  
20 legislative session in 2007.

21 (b) The task force shall have seven members appointed by the gov-  
22 ernor. The members shall have expertise in computer software develop-  
23 ment, computer technology, the internet, web site development or busi-  
24 ness use of computer and web technologies. Members shall be  
25 reimbursed for their mileage and expenses as provided in K.S.A. 75-3223,  
26 and amendments thereto.

27 (c) For budgeting and administrative purposes the task force shall be  
28 attached to the state corporation commission, which shall provide admin-  
29 istrative support to the task force.

30 (d) The task force and this section terminate on the first day of the  
31 regular legislative session in 2007.

32 Sec. 7. Violation of any provision of this act is guilty of a class A  
33 nonperson misdemeanor.

34 Sec. 8. (a) Nothing in this act shall be construed to prohibit the cop-  
35 ying of computer software onto a computer if an authorized user of such  
36 computer provides informed consent to the copying of such software onto  
37 the computer after the person who will copy, or cause to be copied, such  
38 software onto the computer informs the authorized user in a conspicuous  
39 and intuitive statement in at least 10-point boldfaced type, in immediate  
40 proximity to the space reserved for the owner to agree to the installation,  
41 of:

42 (1) The information that the software will collect and transmit;

43 (2) representative samples of the offers that the software will display;

- 1     (3) the frequency that the software will display an offer; and
- 2     (4) the tasks that the software will enable a person to perform with
- 3 the authorized user's computer from another computer or electronic
- 4 device.
- 5     (b) If a person other than an authorized user of a computer copies,
- 6 or causes to be copied, software onto such computer with the informed
- 7 consent of an authorized user, such person shall include in the software
- 8 a conspicuous and readily accessible uninstall program that allows the
- 9 authorized user of the computer to permanently remove the software.
- 10    Sec. 9. This act shall take effect and be in force from and after its
- 11 publication in the statute book.