

Part 3 Spyware Protection

13-40-301 Prohibition on the use of software.

A person who is not an owner or operator of a computer may not cause computer software to be copied on the computer knowingly, with conscious avoidance of actual knowledge, or willfully, if the software is used to:

- (1) modify, through intentionally deceptive means, settings of a computer controlling:
 - (a) the webpage that appears when an owner or operator launches an Internet browser or similar computer software used to access and navigate the Internet;
 - (b) the default provider or web proxy that an owner or operator uses to access or search the Internet; or
 - (c) an owner's or an operator's list of bookmarks used to access webpages;
- (2) collect, through intentionally deceptive means, personally identifiable information:
 - (a) through the use of a keystroke-logging function that records all or substantially all keystrokes made by an owner or operator of a computer and transfers that information from the computer to another person;
 - (b) in a manner that correlates personally identifiable information with data concerning all or substantially all of the webpages visited by an owner or operator, other than webpages operated by the person providing the software, if the computer software was installed in a manner designed to conceal from all authorized users of the computer the fact that the software is being installed; or
 - (c) by extracting from the hard drive of an owner's or an operator's computer, an owner's or an operator's Social Security number, tax identification number, driver license number, passport number, any other government-issued identification number, an account balance, or overdraft history for a purpose unrelated to any of the purposes of the software or service described to an authorized user;
- (3) prevent, through intentionally deceptive means, an owner's or an operator's reasonable efforts to block or disable the installation or execution of computer software by causing computer software that the owner or operator has properly removed or disabled to automatically reinstall or reactivate on the computer without the authorization of an authorized user;
- (4) intentionally misrepresent that computer software will be uninstalled or disabled by an owner's or an operator's action;
- (5) through intentionally deceptive means, remove, disable, or render inoperative security, antispayware, or antivirus computer software installed on an owner's or an operator's computer;
- (6) enable use of an owner's or an operator's computer to:
 - (a) access or use a modem or Internet service for the purpose of causing damage to an owner's or an operator's computer or causing an owner or operator, or a third party affected by that conduct, to incur financial charges for a service that the owner or operator did not authorize;
 - (b) open multiple, sequential, stand-alone messages in an owner's or an operator's computer without the authorization of an owner or operator and with knowledge that a reasonable computer user could not close the messages without turning off the computer or closing the software application in which the messages appear, unless the communication originated from the computer's operating system, a software application the user activated, or a service provider that the user chose to use, or was presented for any of the purposes described in Section 13-40-303; or

- (c) transmit or relay commercial electronic mail or a computer virus from the computer, if the transmission or relay is initiated by a person other than the authorized user without the authorization of an authorized user;
- (7) modify, without the authorization of an owner or operator, any of the following settings related to the computer's access to, or use of, the Internet:
 - (a) settings that protect information about an owner or operator for the purpose of taking personally identifiable information of the owner or operator;
 - (b) security settings, for the purpose of causing damage to a computer; or
 - (c) settings that protect the computer from the uses identified in Subsection (6); or
- (8) prevent, without the authorization of an owner or operator, an owner's or an operator's reasonable efforts to block the installation of, or to disable, computer software by:
 - (a) presenting the owner or operator with an option to decline installation of computer software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds;
 - (b) falsely representing that computer software has been disabled;
 - (c) requiring in an intentionally deceptive manner the user to access the Internet to remove the software with knowledge or reckless disregard of the fact that the software frequently operates in a manner that prevents the user from accessing the Internet;
 - (d) changing the name, location, or other designation information of the software for the purpose of preventing an authorized user from locating the software to remove it;
 - (e) using randomized or intentionally deceptive filenames, directory folders, formats, or registry entries for the purpose of avoiding detection and removal of the software by an authorized user;
 - (f) causing the installation of software in a particular computer directory or in computer memory for the purpose of evading an authorized user's attempt to remove the software from the computer; or
 - (g) requiring, without the authority of the owner of the computer, that an authorized user obtain a special code or download software from a third party to uninstall the software.

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-302 Other prohibited conduct.

- A person who is not an owner or operator of a computer may not, with regard to the computer:
- (1) induce an owner or operator to install a computer software component onto the owner's or the operator's computer by intentionally misrepresenting that installing the computer software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content; or
 - (2) use intentionally deceptive means to cause the execution of a computer software component with the intent of causing the computer to use the computer software component in a manner that violates any other provision of this chapter.

Repealed and Re-enacted by Chapter 200, 2010 General Session

13-40-303 Exceptions.

Sections 13-40-301 and 13-40-302 do not apply to the monitoring of, or interaction with, an owner's or an operator's Internet or other network connection, service, or computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes,

diagnostics, technical support, maintenance, repair, network management, authorized updates of computer software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing computer software prescribed under this chapter.

Enacted by Chapter 200, 2010 General Session