HOUSE DOCKET, NO. 1789 FILED ON: 1/13/2009

HOUSE . . . . . No. 227

The Commonwealth of Massachusetts

In the Year Two Thousand Nine

An Act relative to consumer protection against spyware..

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

The General Laws are hereby amended by inserting after chapter 93I the following chapter:-

93J. CONSUMER PROTECTION AGAINST COMPUTER SPYWARE ACT

Section 1. As used in this chapter, the following words shall, unless the context clearly otherwise requires, have the following meanings:-

"Advertisement", a communication, the primary purpose of which is the commercial promotion of a commercial product or service, including content on a website operated for a commercial purpose.

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

"Computer software", a sequence of instructions written in any programming language that is executed on a computer.

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

"Consumer", an individual who resides in this state and who uses the computer in question primarily for personal, family, or household purposes.

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

"Execute", when used with respect to computer software, the performance of the functions or the carrying out of the instructions of the computer software.

"Intentionally deceptive", includes: by means of an intentionally and materially false or fraudulent statement; by means of a statement or description that intentionally omits or misrepresents material information in order to deceive the consumer; or by means of an intentional and material failure to provide any notice to an authorized user regarding the download or installation of software in order to deceive the consumer.

"Internet", the global information system that is logically linked together by a globally unique address space based on the Internet Protocol (IP), or its subsequent extensions, and that is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols, and that provides,

uses, or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described in this subdivision.

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

"Personally identifiable information", includes any of the following: first name or first initial in combination with last name; credit or debit card numbers or other financial account numbers; a password or personal identification number required to access an identified financial account; social security number; any of the following information in a form that personally identifies an authorized user: account balances, overdraft history, payment history, a history of websites visited, home address, work address, or a record of a purchase or purchases.

Section 2. A person or entity that is not an authorized user, as defined, shall not, with actual knowledge, with conscious avoidance of actual knowledge, or willfully, cause computer software to be copied onto the computer of a consumer in this state and use the software to do any of the following:

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

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

(ii) The default provider or Web proxy the authorized user uses to access or search the Internet.

(iii) The authorized user's list of bookmarks used to access Web pages.

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

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

(ii) It includes all or substantially all of the Web sites visited by an authorized user, other than Web sites of the provider of 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.

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

(3) Prevent, without the authorization of an authorized user, through intentionally deceptive means, an authorized user's reasonable efforts to block the installation of, or to disable, software, by causing software that the authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer without the authorization of an authorized user.

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

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

Section 3. A person or entity that is not an authorized user, shall not, with actual knowledge, with conscious avoidance of actual knowledge, or willfully, cause computer software to be copied onto the computer of a consumer in this state and use the software to do any of the following:

(1) Transmitting or relaying commercial electronic mail or a computer virus from the consumer's computer, where the transmission or relaying is initiated by a person other than the authorized user and without the authorization of an authorized user.

(2) Accessing or using the consumer's modem or Internet service for the purpose of causing damage to the consumer's computer or of causing an authorized user to incur financial charges for a service that is not authorized by an authorized user.

(3) Using the consumer's computer as part of an activity performed by a group of computers for the purpose of causing damage to another computer, including, but not limited to, launching a denial of service attack.

(4) Opening multiple, sequential, stand-alone advertisements in the consumer's Internet browser without the authorization of an authorized user and with knowledge that a reasonable computer user cannot close the advertisements without turning off the computer or closing the consumer's Internet browser.

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

(i) An authorized user's security or other settings that protect information about the authorized user for the purpose of stealing personal information of an authorized user.

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

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

(iv) Presenting the authorized user with an option to decline installation of software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds.

(v) Falsely representing that software has been disabled.

(vi) Nothing in this section shall apply to any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected 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, repair, authorized updates of 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 software proscribed under this chapter.

Section 4. A person or entity, who is not an authorized user, shall not do any of the following with regard to the computer of a consumer in this Commonwealth:

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

(2) Deceptively causing the copying and execution on the computer f a computer software component with the intent of causing an authorized user to use the component in a way that violates any other provision of this section.

Section 5. Nothing in this chapter shall apply to any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected 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, repair, authorized updates of 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 software proscribed under this chapter.

Section 6. The Attorney General may bring a civil action against any person violating this chapter to enforce the penalties for the violation and may recover any or all of the following:

(1) a civil penalty of up to $100 per violation of this chapter, or up to $100,000 for a pattern or practice of such violations;

(2) costs and reasonable attorneys' fees; and

(3) an order to enjoin the violation.

Section 7. It is the intent of the legislature that this section is a matter of statewide concern. This chapter supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding spyware and notices to consumers from computer software providers regarding information collection. The provisions of this section are severable. If any provision of this section or its application is held invalid, that invalidity shall not affect any other provision or application that can be given effect without the invalid provision or application.