PLEASE NOTE: Legislative Information ***cannot*** perform research, provide legal advice, or interpret Maine law. For legal assistance, please contact a qualified attorney.

An Act To Create the Maine Spyware Prevention Act

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 10 MRSA c. 224-A is enacted to read:

CHAPTER 224-A

maine spyware prevention act

§ 1497-A. Short title

This chapter may be known and cited as "the Maine Spyware Prevention Act."

§ 1497-B. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

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

2. Authorized user. "Authorized user," with respect to a computer, means a person who owns, leases or is authorized by the owner or lessee to use the computer. "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.

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

4. Computer virus. "Computer virus" means 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.

5. Consumer. "Consumer" means an individual who uses a computer primarily for personal, family or household purposes.

6. Damage. "Damage" means any significant impairment to the integrity or availability of data, software, an operating system or information stored on or accessed by a computer.

7. Denial of service attack. "Denial of service attack" means an attempt by a malicious or unwitting user, process or system to prevent legitimate users from accessing a resource, usually a network service, by exploiting a weakness or design limitation in an information system.

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

9. Internet. "Internet" means the global information system that is logically linked together by a globally unique address space based on the Internet Protocol or its subsequent extensions and that is able to support communications using the Transmission Control Protocol/Internet Protocol suite or its subsequent extensions or other Internet Protocol-compatible protocols and that provides, uses or makes accessible, either publicly or privately, high-level services layered on the communications and related infrastructure.

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

11. Personally identifiable information. "Personally identifiable information" means:

A. A first name or first initial in combination with a last name;

B. Credit or debit card numbers or other financial account numbers;

C. A password or personal identification number required to access an identified financial account;

D. A social security number;

E. A driver's license number or state identification card number; or

F. Any of the following information in a form that personally identifies an authorized user:

(1) Account balances;

(2) Overdraft history;

(3) Payment history;

(4) A history of websites visited;

(5) Home address;

(6) Work address; and

(7) A record of a purchase or purchases.

12. Spyware. "Spyware" means software that can display advertisements such as pop-up ads, collect information about you or change settings on your computer, generally without appropriately obtaining your consent.

§ 1497-C. Violations; penalties

1. Unauthorized user; prohibited uses of software. A person that is not an authorized user may not knowingly or intentionally cause computer software to be copied onto a consumer's computer and use the software to:

A. Modify, through deceptive means, any of the following settings related to the computer's access to, or use of, the Internet:

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

(2) The default Internet service provider or proxy server an authorized user uses to access or search the Internet; and

(3) An authorized user's list of bookmarks used to access websites;

B. Collect, through deceptive means, personally identifiable information that:

(1) 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;

(2) Includes all or substantially all of the websites visited by an authorized user other than websites 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; or

(3) Is a data element that is 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;

C. Prevent, without the authorization of an authorized user, through deceptive means, an authorized user's reasonable efforts to block software installation 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;

D. 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;

E. Through deceptive means, remove, disable or render inoperative security, antispyware or antivirus software installed on the computer;

F. Take control of the consumer's computer by:

(1) Transmitting or relaying commercial electronic mail or a computer virus from the consumer's computer when the transmitting 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; or

(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;

G. Modify any of the following settings related to the computer's access to or use of the Internet:

(1) 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; and

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

H. Prevent, without the authorization of an authorized user, an authorized user's reasonable efforts to block software installation or to disable software by:

(1) 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 will nevertheless occur; or

(2) Falsely representing that software has been disabled.

2. Spyware installation misrepresentation. A person who is not an authorized user, with regard to the computer of a consumer in this State, may not intentionally or knowingly:

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

B. Deceptively cause the copying and execution on the computer of 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.

3. Exception. Nothing in this section applies 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 section.

4. Penalty. Violation of this section is a Class D crime.

SUMMARY

This bill creates the Maine Spyware Prevention Act, which is modeled after California and Illinois legislation. The bill protects consumers against the illegal use of computer software known as spyware.