A.C.A. § 4-111-102

Current through all legislation of the 2023 Regular Session and the 2023 First Extraordinary Session.

AR - Arkansas Code Annotated* > *Title 4 Business and Commercial Law* > *Subtitle 7. Consumer Protection* > *Chapter 111 Consumer Protection Against Computer Spyware Act

4-111-102. Definitions.

As used in this chapter:

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

(2) "Authorized user", with respect to a computer, means a person that owns or is authorized by the owner or lessee to use the computer;

(3) "Bundled software" means software that is acquired through the installation of a large number of separate programs in a single installation when the programs are wholly unrelated to the purpose of the installation as described to the authorized user;

(4)

(A) "Cause to be copied" means to distribute or transfer computer software or any component of computer software.

(B) "Cause to be copied" does not include providing:

(i) Transmission, routing, intermediate temporary storage, or caching of software;

(ii) A compact disk, website, computer server, or other storage medium through which the software was distributed by a third party; or

(iii) A directory, index, reference, pointer, hypertext link, or other information location tool through which the user of the computer located the software;

(5) "Computer software" means a sequence of instructions written in any programming language that is executed on a computer but does not include a text or data file, including a cookie;

(6) "Computer virus" means a computer program or other set of instructions that is designed to do the following acts without the authorization of the owner or owners of a computer or computer network:

(A) Degrade the performance of or disable a computer or computer network; and

(B) Have the ability to replicate itself on another computer or computer network;

(7) "Damage" means any significant impairment to the integrity, confidentiality, or availability of data, software, a system, or information, including, but not limited to, the:

(A) Significant and intentional degradation of the performance of a computer or a computer network; or

(B) Intentional disabling of a computer or computer network;

(8) "Distributed denial of service" or "DDoS attack" means techniques or actions involving the use of one (1) or more damaged computers to damage another computer or a targeted computer system in order to shut the computer or computer system down and deny the service of the damaged computer or computer system to legitimate users;

(9) "Execute", when used with respect to computer software, means the performance of the functions or the carrying out of the instructions of the computer software;

(10) "Hardware" means a comprehensive term for all of the discrete physical parts of a computer as distinguished from:

(A) The data the computer contains or that enables it to operate; and

(B) The software that provides instructions for the hardware to accomplish tasks;

(11) "Intentionally deceptive" means with the intent to deceive an authorized user in order to either damage a computer or computer system or wrongfully obtain personally identifiable information without authority:

(A) To make an intentional and materially false or fraudulent statement;

(B) To make a statement or description that intentionally omits or misrepresents material information; or

(C) An intentional and material failure to provide any notice to an authorized user regarding the download or installation of software;

(12) "Internet" means:

(A) The international computer network of both federal and nonfederal interoperable packet switched data networks; or

(B) The global information system that:

(i) Is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions;

(ii) Is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, its subsequent extensions, or other IP-compatible protocols; and

(iii) Provides, uses, or makes accessible, either publicly or privately, high-level services layered on the communications and related infrastructure described in this subdivision (12);

(13) "Internet address" means a specific location on the internet accessible through a universal resource locator or internet protocol address;

(14) "Person" means one (1) or more individuals, partnerships, corporations, limited liability companies, or other organizations;

(15) "Personally identifiable information" means any of the following if it allows the entity holding the information to identify an authorized user by:

(A) First name or first initial in combination with last name;

(B) Credit or debit card numbers or other financial account numbers;

(C) A password or personal identification number or other identification required to access an identified account other than a password, personal identification number, or other identification transmitted by an authorized user to the issuer of the account or its agent;

(D) A Social Security number; or

(E) Any of the following information in a form that personally identifies an authorized user:

(i) Account balances;

(ii) Overdraft history;

(iii) Payment history;

(iv) A history of websites visited;

(v) Home address;

(vi) Work address; or

(vii) A record of a purchase or purchases; and

(16) "Phishing" means the use of electronic mail or other means to imitate a legitimate company or business in order to entice the user into divulging passwords, credit card numbers, or other sensitive information for the purpose of committing theft or fraud.

History

Acts 2005, No. 2255, § 1.