AMENDED IN SENATE AUGUST 21, 2006

AMENDED IN SENATE AUGUST 10, 2006

AMENDED IN SENATE JUNE 20, 2006

AMENDED IN ASSEMBLY MAY 30, 2006

AMENDED IN ASSEMBLY MAY 17, 2006

AMENDED IN ASSEMBLY APRIL 26, 2006

CALIFORNIA LEGISLATURE—2005–06 REGULAR SESSION

ASSEMBLY BILL No. 2415

Introduced by Assembly Member Nunez
(Principal coauthor: Assembly Member Leno)

February 23, 2006

An act to add Chapter 34 (commencing with Section 22948.5) to Division 8 of the Business and Professions Code, relating to network security.

LEGISLATIVE COUNSEL'S DIGEST

AB 2415, as amended, Nunez. Network security.

Existing law, the Consumer Protection Against Computer Spyware Act, provides specified protections for the computers of consumers in this state against certain types of computer software.

This bill would require a device that includes an integrated and enabled wireless access point, if the device is manufactured on or after October 1, 2007, for use in a small office, home office, or residential setting, and that is used in a federally unlicensed spectrum, to either include a warning advising the consumer how to protect his or her wireless network connection, a warning sticker, or provide other

protection that, among other things, requires affirmative action by the consumer prior to use of the device. The bill would provide that if any part of these provisions or their applications are held invalid, the invalidity would not affect other provisions.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. The Legislature finds and declares the following:

(a) With the increasing use of low power, unlicensed wireless technology in residences, home offices, and small offices, consumers are unknowingly allowing their personal information on their small office, home office, or residential networks to be accessed by unauthorized users who piggyback onto their network connection.

(b) Piggybacking occurs when an unauthorized user connects its client device to a wireless local area network (WLAN) access point or router in order to utilize the small office, home office, or residential network's broadband access connection to reach the Internet. The practice is becoming a serious issue for people who reside in densely populated areas or live in apartment buildings where wireless transmission waves can travel easily through walls, floors, and ceilings.

(c) Consumers are generally unaware when an unauthorized user is using their broadband network connection, as most are not sufficiently aware to determine if someone has tapped into their network. Enabled security avoids this problem by preventing all but the most determined attempts to tap into a consumer's network.

(d) In 2003, it was estimated that there were 3.9 million households with wireless access to the Internet. Currently, there are about 7.5 million households with wireless access, and that number is expected to rise to 16.2 million households by the end of the year.

(e) In December 2005, the National Cyber Security Alliance (NCSA) found that, "more than one out of four homes had a wireless network (26%) and nearly half of these homes (47%)

failed to encrypt their connection, a safety precaution needed to protect wireless networks from outside intruders."

(f) There is disagreement as to whether it is legal for someone to use another person's WiFi connection to browse the Internet if the owner of the WiFi connection has not put a password on it. While Section 502 of the Penal Code prohibits the unauthorized access to computers, computer systems, and computer data, authorized use is determined by the specific circumstances of the access. There are also federal laws, including the Computer Fraud and Abuse Act (18 U.S.C. Sec. 1030 et seq.), that prohibit the intentional access to a computer without authorization.

SEC. 2. Chapter 34 (commencing with Section 22948.5) is added to Division 8 of the Business and Professions Code, to read:

CHAPTER 34. NETWORK SECURITY

22948.5. For purposes of this chapter, the following terms have the following meanings:

(a) "Federally unlicensed spectrum" means a spectrum for which the Federal Communications Commission does not issue a specific license to a user, but instead certifies equipment that may be used in a segment of spectrum designated for shared use.

(b) "Small office" means a business with 50 or fewer employees within the company.

(c) "Spectrum" means the range of frequencies over which electromagnetic signals can be sent, including radio, television, wireless Internet connectivity, and every other communication enabled by radio waves.

(d) "Wireless access point" means a device, such as a premises-based wireless network router or a wireless network bridge, that allows wireless clients to connect to it in order to create a wireless network for the purpose of connecting to an Internet service provider.

(e) "Wireless client" means a wireless device that connects to a wireless network for the purpose of connecting to an Internet service provider.

22948.6. (a) A device that includes an integrated and enabled wireless access point, such as a premises-based wireless network router or wireless access bridge, that is for use in a small office,

home office, or residential setting and that is sold as new in this state for use in a small office, home office, or residential setting shall be manufactured to comply with one of the following:

(1) Include in its software a security warning that comes up as part of the configuration process of the device. The warning shall advise the consumer how to protect his or her wireless network connection from unauthorized access. This requirement may be met by providing the consumer with instructions to protect his or her wireless network connection from unauthorized access, which may refer to a product manual, the manufacturer's Internet *Web* site, or a consumer protection Internet *Web* site that contains accurate information advising the consumer on how to protect his or her wireless network connection from unauthorized access.

(2) Have attached to the device a temporary warning sticker that must be removed by the consumer in order to allow its use. The warning shall advise the consumer how to protect his or her wireless network connection from unauthorized access. This requirement may be met by advising the consumer that his or her wireless network connection may be accessible by an unauthorized user and referring the consumer to a product manual, the manufacturer's Internet *Web* site, or a consumer protection Internet *Web* site that contains accurate information advising the consumer on how to protect his or her wireless network connection from unauthorized access.

(3) Provide other protection on the device that *does all of the following*:

(A) Advises the consumer that his or her wireless network connection may be accessible by an unauthorized user.

(B) Advises the consumer how to protect his or her wireless network connection from unauthorized access.

(C) Requires an affirmative action by the consumer prior to allowing use of the product.

Additional information may also be available in the product manual or on the manufacturer's Internet *Web* site.

(4) Provide other protection prior to allowing use of the device, that is enabled without an affirmative act by the consumer, to protect the consumer's wireless network connection from unauthorized access.

(b) This section shall only apply to devices that include an integrated and enabled wireless access point and that are used in a federally unlicensed spectrum.

(c) This section shall only apply to products that are manufactured on or after October 1, 2007.

22948.7. The provisions of this chapter are severable. If any provision of this chapter 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.

O