

State Legislation: Suggested Act 5

Act 5: Security Protection on Wireless Access Devices

- 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 STATE for use in a small office, home office, or residential setting (hereinafter Device) shall be manufactured to comply with one of the following:
 - i. 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.
 - ii. 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.
 - iii. Provide other protection on the Device that does all of the following:
 1. Advises the consumer that his or her wireless network connection may be accessible by an unauthorized user.
 2. Advises the consumer how to protect his or her wireless network connection from unauthorized access.
 3. 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.
 - iv. 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 a Device that includes an integrated and enabled wireless access point and that is used in a federally unlicensed spectrum.
- c. This section shall only apply to a Device that is manufactured on or after October 1, 2007 [or other date].
- d. To comply with Section (a)(iii)(3), the following must be satisfied:
 - i. The Device is programmed so it will provide protection of the wireless network connection from unauthorized access without an affirmative act by the consumer; and
 - ii. A consumer must take affirmative action to disable or opt out of the protection settings; and
 - iii. A consumer who disables or opts out of the protection settings must click to accept or otherwise acknowledge a statement that advises the consumer that the protection settings will not be applied and warns the consumer of the consequences of not enabling the protection settings.
- e. Any Device sold as new in STATE after December 31, 2008 [or other date], must comply with section (a)(iii) or section (a)(iv).

Source. This Act is based on Cal. Bus. & Professions Code § 22948.6 (West 2006). I have adjusted the formatting, defined the term “Device” to avoid confusion, and added new sections (d) and (e). I was perplexed by California’s version of section (a)(iii)(3) and its reference to affirmative action by the consumer. I have defined what I think the section means, and expanded it somewhat, in the new section (d). I also added section (e) to encourage a second, higher level of compliance for devices that will be available in 2009 and thereafter. It seems that, by then, we should be able to get past warning stickers and making consumers look up instructions, which may not be simple to follow, for how to secure their networks. An enacting state need not include the new sections (or any part of it for that matter), and may want to adjust the dates.

Purpose. This Act helps residents of STATE to secure their wireless networks. The state has an interest in secured wireless networks for several reasons. First, (as discussed with respect to Act 3) minors and others can access pornography over the unsecured, unfiltered wireless networks of neighbors and businesses, which are beyond the ability of the parent to control. This undermines the efforts of parents to supervise computer use and take precautions in homes and schools. Second, unsecured wireless networks create a fertile field for identity theft, privacy invasions, and fraud. Third, there is an increase use of unsecured wireless networks to commit crimes on the Internet, including the transmission and storage of child pornography. Law enforcement tracing such activity will trace it to particular computers and networks. Computer owners without secure networks may be totally unaware that others have used their access points for such purposes, but that fact will be difficult to prove.

This Act covers devices sold to individuals and businesses that are unlikely to have customized equipment and the expert technical staff to incorporate protections against wireless theft. The Act requires manufacturers of such devices, in the minimum, to (1) inform and warn users of the risks, and (2) tell them how to secure their network. For devices sold beginning in 2009, manufacturers must comply with the second two of the four compliance choices, sections (a)(iii) and (a)(iv). Manufacturers must then configure their devices to provide security so that consumers don't need to worry about how to set up the necessary protections. Choice (a)(iii) allows manufactures to allow customers to opt out of the default security procedure, but only by affirmatively doing so and acknowledging the warning.

Most such devices on the market are already configured to advise the consumer on how to set up security protection, although they do not clearly warn the consumer of the risks. Some current devices assume the consumer wants a secured network, unless the consumer selects the alternative set up. Because consumers are poorly informed about the risks, they continue to buy devices that do not explain how to make the network secure nor the risks of an unsecured network. This statute encourages manufacturers to be responsible social actors and help consumers without a great deal of technical savvy secure their networks.

To avoid a burden on manufacturers, the effective date is delayed, giving them time to comply. Because this statute (with the exceptions noted above) has already been enacted in California, most manufacturers will be compelled to comply to access California markets. However, other state governments can support this movement toward better consumer Internet choices and assure protection of their own citizens by enacting similar versions in their states.

Footnotes:

1. Insert appropriate state name.