SUBJECT: Criminal and civil consequences for communication services offenses

COMMITTEE: Regulated Industries — favorable, without amendment

VOTE: 4 ayes — King, Hunter, Crabb, Guillen

0 nays

3 absent — Turner, Baxter, Wolens

SENATE VOTE: On final passage, May 20 — voice vote (Barrientos, Carona recorded nay)

WITNESSES: (On House companion bill, HB 2121:)

For — Todd Flournoy and Van Stevenson, Motion Picture Association of America; Kathy Grant, Texas Cable and Telecommunications Association; (Registered, but did not testify:) Susan Patten, Time Warner Cable Southwest

SB 1116

Williams

(Wilson)

Against — Douglass Barnes and Adina Levin, Electronic Frontier Foundation of Austin and ACLU; Richard Lawson, Verizon Southwest; (Registered, but did not testify:) Brad Denton, Texas Telephone Association; Henry Flores, Sprint; Tim Morstad, Consumers Union; Tom "Smitty" Smith, Public Citizen; Leslie Ward, SBC

On — Shannon Edmonds, Texas District and County Attorneys Association

BACKGROUND: Penal Code, sec. 31.12 establishes an offense for theft of or tampering with

mulitchannel video or information services. Sec. 31.13 establishes an offense for manufacturing, distributing, or advertising a decoding device for use to commit an offense under sec. 31.12. Sec. 31.14 establishes an offense for knowingly selling or leasing a decoding device for use to commit an offense

under sec. 31.12.

DIGEST: SB 1116 would amend the Penal Code to establish communications services

offenses. Committing an offense would require intent to defraud a communications service provider. The bill would define communication device, communication service and service provider, and unauthorized access device. Communication service would include any service provided for a

charge to facilitate the origination or transfer of signs, signals, writing, images, sounds, data, audio, or video by any means, including an Internet-based distribution system, network, or facility. In addition, the bill would establish civil liabilities for communication services offenses.

Offenses. The bill would create an offense for theft of or tampering with communication services. Committing an offense would require committing theft or tampering without the effective consent of a communication service provider and with intent to defraud. An offense would include obtaining or using a communication service without paying the provider.

The bill would create an offense for possession or use of a communication device or unauthorized access device. A person would commit an offense if, with intent to defraud a communication service provider, he or she knowingly possessed or used a device to commit an offense under sec. 31.12 or 31.14. An offense would be a Class C misdemeanor (punishable by a maximum fine of \$500), unless it was shown at trial that an offense involved five or more devices in a single criminal episode, making it a Class A misdemeanor (up to one year in jail and/or a maximum fine of \$4,000).

The bill would create an offense for manufacturing, distributing, selling, leasing, or advertising a communication device or unauthorized access device with the intent to defraud a communication service provider. Committing an offense would require manufacturing, developing, assembling, importing to or exporting from the state, licensing, distributing, advertising, selling, or leasing a communication device for use to commit an offense under sec. 31.12 or sec. 31.13, an unauthorized access device, or plans or instructions for building a device with the knowledge that the recipient intended to use the information to commit an offense. An offense would be a state-jail felony (180 days to two years in a state jail and an optional fine of up to \$10,000) if it was shown at trial that the offense included more than one but less than 50 devices or if the defendant had been convicted once before of a similar offense. It would be a third-degree felony (two to 10 years in prison and an optional fine of up to \$10,000) if the offense included more than 50 devices or if the defendant had been convicted at least twice before of similar offenses.

To establish a presumption of intent to defraud in a communication services offense, a provider would have to send written notice to an offender stating

that the provider had reason to believe there was an unauthorized connection between the offender's property and the provider's system, that the offender possessed or controlled a device that allowed unauthorized access to the provider's communication service, or that the offender possessed five or more communication or unauthorized access devices for an unlawful purpose. Intent to defraud would be presumed if an offender did not admit to or deny the provider's statements within 30 days of receiving notice. The presumption would not apply to a state or local law enforcement agency, a communication service provider, or a person that manufactured, offered for sale, or possessed a multipurpose device not intended to commit an offense.

It would be a defense to prosecution for a communication services offense that a person took an accused action with a multipurpose device for a reason other than committing an offense; that the device had a commercially significant use or purpose; and that the device was not marketed as an unauthorized access device.

Civil liabilities. A claimant in a civil suit involving a communication services offense could choose any time before a final judgment was entered to recover damages through either of two methods. The first would include actual damages incurred by the claimant arising out of the offense and any profits earned by the defendant attributable to the offense. The second would include an amount of damages specified by the court for each device involved in the offense or each day the offense was committed; however, the amount of damages would have to be between \$2,500 and \$10,000. If the court found that a communication services offense was committed wilfully and for financial gain, the court could increase the damages awarded under either method by up to \$50,000 for each device or for each day the offense was committed.

A person who manufactured, offered for sale, or possessed a multipurpose device not intended to commit an offense would not be civilly liable for a communication services offense, unless the person intended to defraud a communication service provider and the device:

- was intended mainly for committing such an offense;
- had only a limited commercially significant use other than as an unauthorized access device; and

• was marketed for use as an unauthorized access device.

The bill would not impose criminal or civil liability on an entity lawfully acting in its capacity as a communication service provider, a municipality, a law enforcement agency, or any other state or local government agency. It would not impose liability on someone using a communication device to connect multipurpose devices at a residence or business unless the person intended to defraud or the device caused material harm to the communication provider's system. Breach of a service contract would not constitute intent to defraud a communication service provider unless the device was used to obtain service without compensation.

The bill would take effect September 1, 2003.

SUPPORTERS SAY:

SB 1116 would amend current-law offenses to take into account new criminal opportunities. As an increasing number of services are provided in a digital format, more cases of theft will occur through decryption or other technologies. Updating the law to reflect crimes in the digital age would deter criminals and discourage large-scale theft of communication services.

The bill would establish an offense for theft of communication services, such as from an online content provider. Companies are developing new online services providing content such as movies or music to customers. Movielink, where customers can download movies for a fee, and Apple Computer's new online music service are two examples of such services. However, many companies are discouraged from offering such services because of the risk of theft or piracy. By establishing clear offenses and penalties for theft of these services, the bill would foster innovation by reducing uncertainty for companies that are considering developing a new service or product, thereby fostering innovation.

The bill also would establish offenses for making, distributing, or selling hardware devices used to steal communication services, such as cable or satellite TV. Such devices are advertised widely and sold over the Internet. For example, many websites sell cable TV descrambler boxes than can be used to steal cable television signals directly or with simple modification. The bill would establish that making, distributing, selling, or using such a device for theft of a communications service would be a criminal offense.

Law-abiding customers would not be penalized, as the bill's provisions would apply only in cases where there was intent to defraud the communication service provider. The bill would not affect multipurpose devices that could be used for both legitimate and illegal activities, such as smart cards. In fact, the bill would specify a defense for multipurpose devices intended for legitimate purposes. There is no reason to believe that prosecutors or communication service providers would pursue criminal penalties or civil suits frivolously against innocent users.

Rep. Wilson plans to offer a floor substitute that would eliminate the bill's presumption of intent to defraud, in order to alleviate concerns about misuse of the bill's provisions. In addition, the floor substitute would lower the minimum civil penalty from \$2,500 to \$500 and would allow the courts to determine damages as they found to be just.

OPPONENTS SAY:

While piracy of copyrighted material or using devices to steal cable TV or other services should be illegal and strictly punished, the bill's broad wording, procedures for presuming intent to defraud, and civil liabilities would be ripe for abuse. In trying to deal with a few bad actors, the bill could subject lawabiding consumers to prosecution or civil suits from unscrupulous communication service providers

Communication service providers could use the new offenses that the bill would create to harass and intimidate law-abiding consumers. For example, a computer smart card would fall under the bill's definition of a communication device. These cards are used for legitimate purposes, such as unlocking doors or accessing computers; however, they also can be reprogrammed for illegal activities, such as stealing cable TV service. In an effort to discourage customers from owning or using smart cards because of their potential for abuse, a communication service provider could notify the customer that it had reason to believe that the person possessed a communication device. If a customer did not respond in 30 days, whether because the customer did not understand the letter or was out of town, the provider would have established intent to defraud regardless of whether the person was using the card for a legitimate purpose.

Companies could use the bill's provisions to discourage or intimidate consumers from owning or buying certain products. In the smart card

example, the company would have established intent to defraud if the person did not respond. The company then could pursue a civil case against the person, taking advantage of the statutory minimum damages the bill would establish. These damages would not necessarily have to relate to the value of the service alleged to have been stolen. A few highly-publicized verdicts could be enough to intimidate consumers from buying certain products.

Moreover, overzealous pursuit of alleged offenders could discourage other consumers from buying new communications-related devices. Consumer electronics companies have many new communications-technology devices in the production pipeline. However, consumers could be discouraged from buying new products for fear that their cable provider or Internet service provider would construe the products as being used for illegal purposes and would pursue criminal or civil penalties against them.

SB 1116 is unnecessary. Current law already includes offenses for the activities that the bill is intended to discourage. Theft of Internet or data services already is illegal under Penal Code, sec. 33.02. Theft of copyrighted content is prohibited by federal copyright law.

NOTES:

The companion bill, HB 2121 by Wilson, was reported favorably, as substituted, by the House Regulated Industries Committee on May 10.