SUBJECT: Prohibiting Internet "spyware" transmission of unauthorized software

COMMITTEE: Business and Industry — committee substitute recommended

VOTE: 5 ayes — Giddings, Elkins, Martinez, Solomons, Taylor

0 nays

4 absent — Bailey, Bohac, Vo, Zedler

SENATE VOTE: On final passage, April 14 — 31-0

WITNESSES: *(On House companion, HB 1430 by McCall:)*
For — Andrew Wise, Microsoft Corporation

Against — None

DIGEST: CSSB 327 would establish the Consumer Protection Against Computer Spyware Act in the Business and Commerce Code.

The bill would prohibit a person who was not the owner or operator of a computer from knowingly transmitting computer software to a computer in Texas and using the software, through intentionally deceptive means, to:

- collect personally identifiable information (PII), which would be defined as a first name or first initial in combination with last name; a home or email address; a credit or debit card number; a bank account number; a password or access code for a credit or debit card or bank account; a social security, tax identification, driver's license or passport number or other government-issued identification number; or account balances, overdraft history, or payment history if alone or in combination with other information they personally identified the individual. PII could not be collected using a keystroke logging function, which records all keystrokes made by a person and transfers that information from the computer to another person, or in a way that correlated PII with information regarding all or substantially all of the websites visited by the

computer's owner or operator, other than websites of the software provider.

- cull certain kinds of PII from the consumer's computer hard drive for reasons unrelated to the purposes of the software or service described to an owner or operator of the computer, including a credit or debit card number, a bank account number, a password or access code associated with a credit or debit card number or a bank account, a social security number, account balances, or overdraft history.
- modify a setting that controlled any of the following: the page that appeared when an Internet browser or a similar software program was launched to access and navigate the Internet, the default browser or web proxy used to search the Internet, or a list of bookmarks used to access web pages.
- take control of the computer by accessing or using the computer's modem or Internet service to damage the computer, or cause the computer's owner or operator to incur financial charges for a service not authorized by the owner or operator.
- open, without the consent of the computer's owner or operator, an advertisement that was in the owner or operator's Internet browser in a multiple, sequential or stand-alone form and could not be closed by an ordinarily reasonable person using the computer without closing the browser or shutting down the computer.
- modify settings for access to or use of the Internet and protection of information for purposes of stealing PII of the computer's owner or operator.
- modify security settings relating to access to or use of the Internet to cause damage to one or more computers.
- prevent reasonable efforts of the computer's owner or operator to block the installation or execution of or to disable computer software by causing software the owner or operator had properly removed or disabled automatically to reinstall or reactivate on the computer.
- intentionally misrepresent that software would be uninstalled or disabled by the actions of the computer's owner or operator.
- remove, disable, or render inoperative security, antispyware, or antivirus computer software installed on the computer.
- prevent the owner's or operator's reasonable efforts to block the installation of or to disable computer software by presenting the owner or operator with an option to decline the software knowing that, when the option was selected, the installation would proceed,

or misrepresenting that software had been disabled.

- induce the owner or operator of a computer to install a software component by intentionally misrepresenting the extent to which the installation was necessary for security or privacy, for opening or viewing text, or for playing a particular type of musical or other content.
- copy and execute a software component deceptively, intending to cause the computer's owner or operator to use the component in a way that would violate the bill's provisions.

A person would have acted through intentionally deceptive means if the person, with the intent to deceive the computer's owner or operator, intentionally made a materially false or fraudulent statement, omitted or misrepresented material information, or failed to provide the computer's owner or operator with notice regarding the installation or execution of computer software.

A person would knowingly commit a violation by acting with actual knowledge of the facts that constituted the violation or consciously avoided information that would establish actual knowledge of the facts.

A person would have transmitted software if the person transferred, sent or made available computer software or a component of the software through the Internet, a local area network of computers, other non-wire transmission, a disc or other data storage device, or any other medium.

The bill would allow a provider of computer software, an owner of a web page or trademark, or a telecommunications carrier or Internet service provider who adversely was affected by violations in the bill to bring a civil action against the person committing the violation. In addition to any other remedy provided by law, a person bringing a civil action could seek injunctive relief to restrain the violator from continuing the violation and/or recover damages of up to $100,000 for each violation of the same nature or actual damages arising from the violation. The court could increase the award to up to three times actual damages as well as attorney's fees if it found the violations occurred with enough frequency to be a pattern or practice. If a violation caused a telecommunications carrier to incur costs for the origination, transport or termination of a call triggered using a customer's modem, the carrier could apply for a court order to enjoin the violation and recover costs the carrier was obligated to pay as a result of the violation.

The bill would make a person who committed a violation liable to the state for a civil penalty of up to $100,000 for each violation. If it appeared to the attorney general that a person was engaging in, had engaged in, or was about to engage in a violation, the attorney general could request a temporary restraining order or a permanent or temporary injunction.

The bill would take effect September 1, 2005.

SUPPORTERS SAY:

CSSB 327 would prohibit a number of activities related to "spyware," which is software secretly placed on a user's computer to monitor, collect, and transmit personally identifiable information without the user's knowledge or consent. Spyware is installed for a myriad of reasons, including tracking a user's on-line behavior, browsing for market research, sending pop-up ads, redirecting computer users to websites, or recording keystrokes, and can be transferred via spam or bundled with freeware, shareware, or games downloaded from the Internet. Spyware can cause the drastic slowing of infected computers, corruption of the hard drive, or disabling of hardware and software settings.

According to the National Cyber Security Alliance, nine out of 10 computers connected to the Internet are infected with spyware. A recent audit by Earthlink found that the average computer had more than 26 spyware programs installed. The net impact of this problem will be citizens' loss of confidence in the Internet and a reluctance to engage in online business transactions.

The bill would protect the privacy of Texas consumers and establish a cause of action for those adversely affected by spyware, including software companies, web page or trademark owners, and the general public through actions brought by the attorney general. Existing statutes do not expressly prohibit activities relating to spyware. By specifically identifying such prohibitions, the bill would provide clear authority for the attorney general and others to pursue civil actions against those who knowingly and deceptively transmit and use spyware.

The bill is carefully crafted to define and outline prohibited behaviors, rather than actually to define spyware. Beneficial uses of technology that could be defined as spyware would not be prohibited because the bill would specify that prohibited activities would have to be conducted with

an intent to deceive.

OPPONENTS SAY:

The activities addressed in CSSB 327 already are prohibited under existing laws addressing fraud and deceptive trade practices. Nothing prevents the attorney general or anyone else from taking civil action under these statutes.

The bill would generously apply the term "intent to deceive" in connection with prohibited behaviors, establishing a standard that could be difficult to prove and would raise the bar high for litigation. Because of the difficulty of proving intent, the bill could be virtually unenforceable.

Spyware is difficult to define, and beneficial uses, such as using "cookies" to collect and save credit card information so that it does not have to be reentered, could be affected. This is a rapidly changing technology and many potentially beneficial uses yet to be developed could be outlawed.

OTHER OPPONENTS SAY:

CSSB 327 should include provisions related to notice, consent and specification of purpose when spyware was used without the intent to deceive and thus not prohibited by most provisions in the bill.

The bill would have limited impact on the spyware problem because it does not address all uses of spyware. Various types of known spyware, many of which are not addressed by CSSB 327, could continue to be distributed.

NOTES:

The committee substitute is nearly identical to HB 1430, with additional provisions regarding legal actions for telecommunications carriers affected by spyware.

The companion bill, HB 1430, passed the House on April 26 and is pending in the Senate Criminal Justice Committee.