SUBJECT: Prohibiting fraudulent acquisition of customer telephone records

COMMITTEE: Business and Industry — committee substitute recommended

VOTE: 9 ayes — Giddings, Elkins, Darby, Bailey, Bohac, Castro, Martinez, Solomons, Zedler

0 nays

WITNESSES: For — None

Against — None

On — Richard Lawson, Texas Telephone Association; C. Brad Schuelke, Office of the Attorney General; Paul Carmona, Office of the Attorney General; (*Registered, but did not testify*: Ron Hinkle, Verizon Wireless)

BACKGROUND: On January 12, 2007, President Bush signed H.R. 4709, the federal Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. 1039. The bill amended the federal criminal code to prohibit obtaining confidential phone records information from a telecommunications carrier or IP-enabled voice service provider by making false or fraudulent statements to an employee, providing false or fraudulent documents, or accessing customer accounts through the Internet or by fraudulent computer-related activities without prior authorization by the customer. It establishes a criminal penalty of a fine and up to 10 years imprisonment or both, with an enhanced punishment of a fine and twice the prison sentence for the fraudulent acquisition or disclosure of these telephone records without the consumer's consent.

DIGEST: CSHB 73 would amend the Business and Commerce Code to make it an offense to obtain, attempt to obtain, or conspire with another person to obtain the telephone record of any resident of this state and would provide a criminal penalty.

A "telephone record" would be a written, electronic, or oral record, other than a caller identification record, created by a telephone company about a customer that included:

- the telephone number dialed by a customer or number of an incoming call made to a customer;
- the time a call was made to or by a customer;
- the duration of the call; or
- the location from which the call was initiated or received by a customer.
-

"Telephone company" would mean a provider of commercial telephone services regardless of the technology, including landline, radio, wireless, microwave, satellite, Voice over Internet Protocol (VoIP), or other cable, broadband, or digital technology.

Unauthorized or fraudulent act. Under CSHB 73, a person would commit an offense:

- if the person obtained, attempted to obtain, or conspired to obtain a telephone record of a resident of this state without authorization of the resident by:
  - making a statement the person knew to be false to a telephone company or its agent;
  - fraudulently accessing the record through the telephone company's Website; or
  - providing to a telephone company a document that the person knew to be fraudulent, lost or stolen, or false or fictitious;
- if a person sold, transferred, or attempted to sell or transfer a telephone record of a resident without the resident's authorization;
- if a person offered to obtain or sell a telephone record that had been or would be obtained without authorization from the resident; or
- if a person asked another person to obtain a telephone record of a resident knowing that the record would be obtained in a manner prohibited by the provisions of the bill.

If conduct that constituted an offense also constituted an offense under another section of the Business and Commerce Code or any other law, including the Penal Code, the person could be prosecuted under either or both sections. The bill would not create a private right of action, but a violation would be a deceptive trade practice under the Deceptive Trade Practices Act (DTPA), Business and Commerce Code, subch E, ch. 17, under the authority of the attorney general with a punishment of up to $20,000 per violation.

Penalties. An offense would be a class A misdemeanor (normally punishable by up to one year in jail and/or a maximum fine of $4,000), but the maximum fine under these circumstances would be $20,000.

Forfeiture. In addition to the above penalties, a person convicted of an offense could be required to forfeit personal property used or intended to be used in a violation. The provisions of this bill would be included in the definition of contraband contained in Code of Criminal Procedure, Art. 59.01(2).

Retribution. A person convicted of an offense would be ordered to pay a resident whose telephone record was obtained in a prohibited manner an amount equal to the sum of:

- the greater of the resident's financial loss, if the proof of the loss was submitted to the satisfaction of the court, or $1,000; and
- the amount of any financial gain received by the person as the direct result of an offense.

Venue. A criminal offense could be prosecuted in the county in which the customer whose telephone record was the subject resided at the time of the offense or any county in which any part of the offense took place, regardless of whether the defendant was ever present in the county.

Exceptions. The prohibitions in the bill would not apply to a person who acted pursuant to a valid court order, warrant, subpoena, or civil investigative demand; nor to a telephone company that disclosed a telephone record if the disclosure were:

- otherwise authorized by law;
- necessary to provide service to a customer, protect an individual from fraudulent, abusive or unlawful use of a telephone record or telephone service; or protect the right or property of the company;
- to the National Center for Missing and Exploited Children in connection with a report submitted under the federal Victims of Child Abuse Act;
- for the purposes of testing the company's security procedures or systems for maintaining the confidentiality of customer information;

- to a governmental entity, if the company reasonably believed that an emergency involving danger of death or serious physical injury justified disclosure of the information;
- in connection with the sale or transfer of the company's business, the purchase or acquisition of another company's business, or the migration of a customer from one telephone company to another;
- necessary to initiate, render, bill, and collect the customer's charges, or to protect the customer of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; or
- while acting reasonably and in good faith, notwithstanding a later determination that the action was not authorized.

CSHB 73 could not be construed inconsistently with federal law or rule. The bill would not prohibit any lawfully authorized investigative, protective, or intelligence activity of a U.S. law enforcement agency, a U.S. intelligence agency, a state, or a political subdivision of a state.

The bill would take effect September 1, 2007.

SUPPORTERS SAY:

CSHB 73 would make fraudulently obtaining, attempting to obtain, or conspiring with another person to obtain the phone records of any resident of this state, including wireless call information, a civil violation, as well as a criminal violation. It would be a violation to fraudulently access a telephone record through a telephone company's Website.

Obtaining telephone records, particularly cellular phone information, through fraudulent misrepresentation is becoming more prevalent. This frequently occurs when a party poses as a phone company and gains access to a customer's telephone record without that customer's knowledge or permission. Often this practice is referred to as "pretexting" or "data mining" – the act of pretending to be someone else in order to secure another person's confidential information. Federal law and, to a wide extent, Texas law make pretexting of financial information illegal, but current state law does not specifically address telephone records.

The New York Times has referred to pretexting as a “shady subculture” that has turned into a “small industry.” Some private investigators routinely advertise their ability to search customer telephone records for a nominal price. Increasingly, companies are appearing on the Internet that offer this service. According to the Electronic Privacy Information

Center, at least 40 Websites offer personal cellular phone records for as little as a $37 fee. While private investigators may perform this service frequently in the context of individual cases, the opportunities for serious abuse have increased.

Wrongfully acquiring a person's calling information or patterns could lead to domestic violence or harm to confidential informants, witnesses, jurors, law enforcement officers, or their families. For example, a predator might pose as a law enforcement official to obtain mobile phone records of a police officer or a prosecution witness. An employer might wrongfully obtain an employee's telephone records to ascertain if the employee were consulting a psychiatrist.

Telephone companies retain customer's phone information for billing and collection. With landlines and wireless phones, certain records are required. For residential phone lines, these records usually are limited to long distance calls and not local or toll-free calls; for cellular phones, the records generally encompass all calls. CSHB 73 would define "telephone record" to include a telephone number dialed by the customer or an incoming call made to the customer and when available, the time and duration of those calls. It would also include the location from where a call was initiated or received. The bill would not cover surveillance of specific calls.

For many, their first awareness of pretexting telephone records was a recent, high-profile corporate scandal. The chair of Hewlett-Packard admitted to obtaining the assistance of a third party to spy on H-P's directors' personal phone records – both residential telephones and personal cellular phones – not the company's phone records. People impersonating these directors contacted telephone companies and obtained their personal telephone records to look for a pattern associated with media leaks. Later, H-P admitted to extending its surveillance scheme to nine journalists, including some at *The New York Times* and *The Wall Street Journal*.

Generally, personal telephone records are obtained wrongfully by: 1) impersonating a customer either over the phone or through an Internet account, 2) hacking into on-line account Websites, or 3) breaching telephone companies' internal security, including that of wireless telecommunications providers. CSHB 73 would cover each of these methods of falsely securing telephone records and would provide a penalty

of up to one year in jail. In addition, it would make the fine for an offense up to $20,000 (raised from a class A misdemeanor fine of up to $4,000) to be consistent with the civil penalty in the DTPA. The bill would complement newly enacted federal law because it would apply to violations within the state of Texas that the federal statute would not reach.

Prohibiting the sale and use of personal phone information and making telephone record brokers accountable is essential to shutting down this growing market. Since 2006, 19 other states have enacted laws to prohibit wrongfully obtaining phone records. Until the Legislature enacts such a law, nefarious Websites and customer impersonators will continue to thrive in a gray area.

A related bill, SB 225 by Ellis, making fraudulently obtaining cellular phone records illegal and providing a civil penalty, would be an important first step. However, given the sensitive and confidential nature of personal telephone records – both landline and mobile phone information – the circumstances of some violations seem to warrant a criminal penalty, as well as the authority for the attorney general to pursue a case under the DTPA, in order to protect the public.

OPPONENTS SAY:

By including nine exceptions, CSHB 73 would increase greatly the burden of proof for the state in a criminal case. The exceptions would make it almost impossible for prosecutors to obtain a conviction. Prosecutors would have to specify all of the exceptions in every charging instrument. They also would have the burden of proof to show beyond a reasonable doubt that the nine exceptions would not apply to each allegation. If the bill instead made these nine items defenses to prosecution, prosecutors would have to rebut beyond a reasonable doubt only the exceptions raised by the defense, which would be a more practical standard.

CSHB 73 should not infringe on judges' discretion by requiring restitution. Judges already have authority to order plenary restitution. For example, they can make restitution a condition of probation and do in most cases.

Because many violations might not result in significant financial loss, the resulting payment of $1,000 to a person whose records were abused would not be an adequate remedy for the personal breach resulting from the violation. A private right of action under the DTPA would provide a

reasonable remedy against false, misleading, and deceptive practices and unconscionable actions.

OTHER OPPONENTS SAY:

A related bill, SB 225 by Ellis, would protect the privacy of a customer's wireless phone information and create a civil penalty. This would address much of the same fraudulent activity and be a sufficient safeguard.

NOTES:

CSHB 73 differs from the introduced version in the following ways:

- amending the Business and Commerce Code, rather than the Utilities Code;
- deleting the definition of "commercial mobile service provider," modifying the meaning of "telephone company," and expanding the definition of "telephone record" to include the location from which a call was initiated or at which it was received by a customer;
- specifying that the bill would not apply to expand the obligations or duties of a telephone company under federal or another state's law;
- expanding the section on unauthorized or fraudulent acts to include conspiring with another to obtain a telephone record of a resident without that person's authorization;
- making fraudulently accessing a telephone record through a telephone company's Website a violation;
- adding venue provisions;
- specifying that the bill would not create a private right of action;
- changing the criminal penalty to a class A misdemeanor, punishable by up to one year in jail and/or a fine up to $20,000, instead of range of punishment that could be a state jail felony, a third degree felony, or a second degree felony depending on the number of violations;
- requiring a person convicted of a violation to forfeit personal property used or intended to be used in a violation;
- including five additional exceptions to prosecution that were not in the original bill;
- stating that the bill may not be construed inconsistently with any applicable federal law;
- not prohibiting any lawfully authorized activity of a U.S. law enforcement agency, a U.S. intelligence agency, another state, or political subdivision of another state; and

- conforming the definition of "contraband" for the purpose of forfeiture to apply to a class A misdemeanor under Business and Commerce Code, sec. 35.153, rather than under the Utilities Code as in the introduced version.

SB 1815 by Van de Putte, which is almost identical to CSHB 73, has been referred to the Senate Business and Commerce Committee.

SB 225 by Ellis, a related bill that would amend the Utilities Code to protect the privacy of a customer's wireless phone information and include a civil penalty, passed the Senate on the Local and Uncontested Calendar on March 14 and has been referred to the House Regulated Industries Committee.