SUBJECT: Law enforcement requests for location information from cell phones

COMMITTEE: Criminal Jurisprudence — committee substitute recommended

VOTE: 6 ayes — Canales, Hughes, Leach, Moody, Schaefer, Toth

1 nay — Herrero

2 absent — Carter, Burnam

WITNESSES: For — Heather Fazio, Texans for Accountable Government; Matthew Henry, Electronic Frontier Foundation; Scott Henson, Texas Electronic Privacy Coalition; W. Scott McCullough; Christopher Soghoian, American Civil Liberties Union; Ken Stanford II; (*Registered, but did not testify:* Cathie Adams, Texas Eagle Forum; Mary Anderson, Texans for Accountable Government; Sam Brannon, Texans for Accountable Government; Kristin Etter, Texas Criminal Defense Lawyers Association; Gregory Foster, Electronic Frontier Foundation; Kelly Holt, Central Texas Friends of Liberty, Texas Chapters of the John Birch Society; Travis Leete, Texas Criminal Justice Coalition; Emily Williams, Freedom of Information Foundation of Texas; and 22 individuals)

Against — Brian Tabor, Dallas Police Department; Jimmy Taylor, Houston Police Department; Tammy Thomas, Harris County District Attorney's Office; (*Registered, but did not testify:* Mark Clark, Houston Police Officers' Union; Lon Craft, Texas Municipal Police Association; Frederick Frazier, Dallas Police Association; Rodney Hill, Houston Police Department; James Jones, San Antonio Police Department; Randle Meadows, Arlington Police Association)

On — Alan Butler, Electronic Privacy Information Center; Margaret Jonon, Texas Department of Insurance; Steve Lowenstein; (*Registered, but did not testify:* Steven C. McCraw, Department of Public Safety; Wendy Reilly, Tech America)

BACKGROUND: Code of Criminal Procedure, ch. 18 governs search warrants. Art. 18.02 enumerates property, information, and other items for which a search warrant may be issued.

Art. 18.21 provides for warrants and searches related to pen registers and trap and trace devices, access to stored electronic communications, and mobile tracking devices. District courts are required to seal applications and orders granted under art. 18.21

DIGEST:

CSHB 1608 would provide for search warrants for location information from wireless communication devices. The bill would provide definitions, create procedures, change standards for sealing of records and administrative subpoenas, and require reporting of certain search warrant activity.

Search warrants. CSHB 1608 would amend the list of items for which a search warrant could be issued under Code of Criminal Procedure, art. 18.02 to add location information. The bill would exclude location information from the type of information that could be obtained by administrative subpoena under art. 18.21.

"Location information" would mean any information that:

- concerned the location of a cellular telephone or other wireless communications device; and
- was wholly or partly generated by or derived from the operation of the device.

A district judge would be able to issue a warrant for location information provided by the mobile tracking features of a cellular telephone or other wireless communications device. A warrant under this section could be issued in the same judicial district as, or in a contiguous judicial district to the site of:

- the investigation; or
- the person, vehicle, container, item, or object the movement of which would be tracked by the location information obtained from the wireless communication device.

The warrant could authorize the acquisition of location information obtained from a wireless communications device that, at the time the location information was acquired, was located outside the judicial district, but within the state if the applicant for the warrant reasonably believed the device to be located within the district at the time the warrant was issued.

A district judge could issue the warrant only on the application of a peace

officer. The application and sworn affidavit would need to contain information similar to affidavit requirements for other search warrants, including information about the wireless communications device to be monitored, and the facts giving rise to probable cause to believe that location information from the device would be likely to produce evidence in a criminal investigation.

A warrant issued under this section would need to be executed within the period provided by Art. 18.07 by properly serving the warrant on a communications common carrier, an electronic communications service, or a remote computing service. A warrant issued under this section would expire not later than the 90th day after the date the warrant was issued, and location information could not be obtained after the expiration date without an extension of the warrant. For good cause shown, the judge could grant an extension for an additional 90-day period.

Location information could be obtained from a wireless communications device without a warrant by a private entity or peace officer if the device was reported stolen by the owner, or by a peace officer if:

- there existed an immediate life-threatening situation; or
- the officer reasonably believed the device was in the possession of a fugitive from justice for whom an arrest warrant had been issued for committing a felony.

A peace officer could apply for, and a district court could issue, an order authorizing the officer to obtain location information from a wireless communications device on the showing that there were reasonable grounds to believe that the device was in the possession of a fugitive from justice for whom an arrest warrant had been issued for a felony. Regardless of whether an order had been issued, a peace officer would need to apply for a warrant to obtain location information as soon as reasonably practicable. If the district judge found that the applicable situation had not occurred and declined to issue the warrant, any evidence obtained would not be admissible in a criminal action.

Sealing of records. The bill would remove the requirement that district courts seal applications and orders under art. 18.21. Instead, it would allow district courts to seal an application and order at the request of a prosecutor or peace officer. The application and order could be sealed for an initial period not to exceed 180 days. For good cause, the court could

grant one or more additional one-year periods.

If an application became subject to disclosure, the court would be required to redact identifying information that the court determined would cause an adverse result for a person who was a victim, witness, peace officer, or informant. On a showing of clear and convincing evidence that disclosure of the identifying personal information would cause an adverse result, the court would be able to permanently seal the application.

The court would be required to retain a record of any application made or order granted and submit the record to DPS in accordance with the reporting provisions of the bill.

Compelling production of business records with location information. A district court could issue a warrant under the bill to a communication common carrier, an electronic communications service, or a remote computing service to compel the production of the carrier's business records that disclosed location information about the carrier's customers, if there was probable cause to believe the records would provide evidence in a criminal investigation. This order would be available on application by:

- the director of the Texas Department of Public Safety or the director's designee;
- the inspector general of the Texas Department of Criminal justice or the inspector general's designee; or
- the sheriff or chief of a law enforcement agency or the sheriff or chief's designee.

Annual report of warrants and orders. In a certain time period after the expiration, extension, or denial of a warrant under art. 18.21, the court issuing the warrant or order would be required to submit to DPS the following information:

- the receipt of an application for a warrant or order under art. 18.21;
- the type of warrant or order for which the application was made;
- whether any application for an order of extension was granted, granted as modified by the court, or denied;
- the period of monitoring authorized by the warrant or order and the number and duration of any extensions of the warrant or order;
- the offense under investigation, as specified in the application for

the warrant or order or an extension of the warrant or order; and
- the law enforcement agency or prosecutor that submitted an application for the warrant or order or an extension of the warrant or order.

Not later than March 15 of each year, each prosecutor that submitted an application for a warrant or order or an extension under art 18.21 would be required to submit to DPS the following information for the preceding calendar year:

- the same information required to be submitted by a court under the bill with respect to each application submitted by the prosecutor for the warrant or order or an extension of the warrant or order;
- a general description of information collected under each warrant or order, including the approximate number of individuals for whom location information was intercepted and the approximate duration of the monitoring of the location information of those individuals;
- the number of arrests made as a result of information obtained under these warrants or orders;
- the number of criminal trials commenced as a result of information obtained under these warrants or orders; and
- the number of convictions obtained as a result of information obtained under these warrants or orders.

Information submitted to DPS under this section would be public information and subject to disclosure under the Public Information Act.

Not later than June 1 of each year, the public safety director of DPS would be required to submit a report to the governor, the lieutenant governor, the speaker of the House, and the chairs of the standing committees of the Senate and House of Representatives with primary jurisdiction over criminal justice.

The report would be required to contain the following information for the preceding calendar year:

- an assessment of the extent of tracking or monitoring by law enforcement agencies of pen register, trap and trace, ESN reader, and location information;
- a comparison of the ratio of the number of applications for warrants or orders made under art. 18.21 to the number of arrests and

convictions resulting from information obtained under a warrant or order issued under art. 18.21; and

- identification of the types of offenses investigated under a warrant or order issued under art. 18.21.

Effective date. The bill would take effect September 1, 2013.

SUPPORTERS SAY:

Personal privacy. CSHB 1608 would create a high standard for protection of Texans' Fourth Amendment rights, the right against unreasonable searches and seizures. A warrant under the bill would require a showing of probable cause, which would be an appropriate level of protection for the information sought under such a warrant.

Cell phone geolocation data can be extremely revealing and is often extremely accurate about every place a person went to and when they were there. Texans deserve to have their privacy protected to the greatest possible extent. Currently, the Texas Department of Insurance and other agencies obtain location data without judicial oversight. All that is needed to obtain this data is an administrative subpoena, which is an inappropriately low standard for such revealing information. CSHB 1608 would ensure that this data was protected from search unless law enforcement met an appropriately high burden of proof to access it.

The fugitive exception under the bill would not be exceptional in the criminal justice system, and would provide safeguards to unreasonable search and seizure. Any evidence gathered would be inadmissible in court if there were no subsequent finding of probable cause and the search warrant were not issued.

Privacy law. CSHB 1608 would comport with the U.S. Department of Justice's position on geolocation data. The law would be in step with federal standards and would make Texas a leader in privacy law. Privacy law, particularly privacy law related to cell phone data, is a confusing patchwork. By codifying these practices and creating high standards for privacy protection, CSHB 1608 would emphasize that privacy law was a priority for Texans.

A 2012 U.S. Supreme Court case, *United States v. Jones,* 132 S. Ct. 945, held that location searches implicate the Fourth Amendment. By requiring a warrant and a high legal standard to obtain this information, CSHB 1608 would conform to constitutional requirements for privacy in location data

and would bring Texas in line with the decision in *United States v. Jones.* Opinions differ regarding whether *United States v. Jones* found the search in question unconstitutional. The opinion only held that the search required a warrant and not that any aspect of the search itself, including its length, was unconstitutional.

Data requests. Modern technology makes it increasingly easy to gather information for surveillance purposes. U.S. Rep. Edward Markey (D-Mass.) conducted an informal query of several communications companies to ascertain how often location data were requested and discovered that there were about 1.3 million federal, state, and local law enforcement requests for cell phone records to wireless carriers in 2011 from all major companies, excluding T-Mobile. This is a widespread issue and will only continue to grow as mobile technology becomes more sophisticated and pervasive.

Unsealing of records and transparency. Unsealing of records under CSHB 1608 would help protect and inform the public about how their data is being accessed and used. Many kinds of records that must be sealed at first are eventually unsealed, but location data remains sealed indefinitely. Unfortunately, if a person is surveilled under a sealed warrant, they may never know about it. The irony is that only criminals who are eventually charged discover they were being surveilled, while innocent people may never find out. With tens of thousands of these kinds of orders being made every year, sealed warrants constitute a kind of secret docket that the public will never know about or see. Unsealing these records is crucial for transparency and the protection of the public.

Reporting. The reporting requirements under CSHB 1608 would be an important tool for the Legislature to determine how to move forward on location data. Although CSHB 1608 would be an important first step, reporting requirements would provide the information needed to know how often these requests happen, how and when they are used, and how effective they are. All of these data points would be essential for the Legislature to determine whether the law was working and how it could be fixed. Reporting also would ensure that authorities were accessing this information responsibly, which is impossible to tell under the current system.

Effect on law enforcement. The bill would not place an undue burden on law enforcement. The bill seeks only to ensure that Fourth Amendment

concerns would be addressed and protected in Texas. Law enforcement still could use many of the tools already at its disposal and would be able to access location data when probable cause existed. This standard would be appropriately high, and the barrier created would not be unnecessarily burdensome or obstructive to law enforcement efforts.

Third-party data still would be available to law enforcement under the bill. The bill would provide a higher standard to access and compulsory disclosure of such data because the data have serious privacy implications. Regardless of the manner in which companies use their location records, these records are extremely revealing about a person's activities and associations. This data deserves additional protection under the law.

CSHB 1608 would not raise barriers to law enforcement unnecessarily or prevent peace officers from protecting the public. The bill would protect the public from illegal and inappropriate invasions of privacy, and would only reinforce the idea that law enforcement exists to help the public and not harm them.

OPPONENTS SAY:

Personal privacy. CSHB 1608 would be detrimental to personal privacy and would violate a person's reasonable expectation of privacy in certain situations. The bill would allow an officer to obtain a location information warrant for 180 days or more, just by signing a warrant, and would provide no prosecutorial oversight.

Additionally, the bill would provide for an illegal exception to the warrant requirement in the case of fugitives. Officers would be able to geolocate a person they considered to be a fugitive and then ask for a warrant later. This would be akin to allowing a police officer to kick down a person's front door and perform a search and then apply for a warrant once they had found the evidence they were looking for, and would be a violation of the Fourth Amendment.

Privacy law. CSHB 1608 would confuse and complicate the area of privacy law and run afoul of federal law and national standards in this area of law. The definition of "location information" in the bill would be unclear. It would disregard the nationally accepted definitions of location information and replace them with an ineffectual and unclear definition.

In *United States v. Jones*, the Supreme Court held that a 28-day time period was an unconstitutional length of time during which to track a

person's location data, and other Supreme Court cases have held 70-day tracking to be too long. The 90-day warrant allowed under CSHB 1608 would exceed the former limit more than threefold. Searches under this bill would be unconstitutional and violate privacy law.

OTHER OPPONENTS SAY:

Unsealing of records and transparency. By unsealing records, the bill would constitute an extreme change to certain kinds of search warrants and would render some law enforcement techniques ineffective. Currently, records under art. 18.21 are sealed by default, and this bill would remove that presumption and replace it with the opposite. Records would only be sealed on request of a peace officer or prosecutor. This change in practice would be onerous on law enforcement, which would need to apply and reapply to keep the records sealed, and would need to meet a high standard of proof to ensure indefinite sealing.

It's unclear how informants and witnesses would be affected by the unsealing of records. The bill is silent on whether an exonerated person would be able to have their information redacted from a record when it was unsealed.

Records of warrants contain sensitive information about law enforcement and investigation techniques. The U.S. Supreme Court has recognized that certain law enforcement techniques need to remain confidential in order to be effective and assist law enforcement in their duty to uphold the laws and Constitution. This bill would allow records containing such information to be exposed to public scrutiny, rendering such techniques useless.

Reporting. The reporting requirements in the bill would create a huge burden for prosecutors, courts, and DPS. For every warrant issued under art. 18.21 to be reported, compiled, and analyzed by DPS would create huge costs to taxpayers and the state budget. Taxpayers shouldn't be forced to bear the costs of extensive and unnecessary reporting requirements.

Effect on law enforcement efforts. The bill would seriously hinder the law enforcement efforts of police officers in Texas. The information for which law enforcement would need to obtain a warrant under the bill is the kind of information law enforcement currently uses to gain probable cause to continue an investigation. Removing this valuable source of evidence would stunt investigations and prevent the successful prosecution of many

criminals.

The bill would unreasonably tie the hands of law enforcement. Location information from cell phones is used to catch felons who kill police officers or kidnap children. Police are able to track criminals quickly by accessing real-time location data from a cell phone. This helps recover kidnapping victims and detain felons. The bill would raise barriers to these kinds of use and could result in the evidence discovered via the location data being suppressed and excluded from a trial. Under the provisions of this bill, murderers could go free because of the obstacles around which law enforcement would be required to maneuver.

The bill would require law enforcement to jump through hoops to obtain location information held by a third party. Historically, information held by a third party has a very low expectation of privacy. This bill would give unnecessary protection to business records that companies such as AT&T or Sprint use to load-balance their networks and ensure customer service. The requirements this bill would place on access to these business records is the same burden needed for content intercepts like wiretaps. That standard is unnecessarily high for records that are not even in the possession of the person to whom they relate.

In addition, the bill would be an unnecessary measure, one that addresses a very small percentage of cases and people. Concerns about easy access to data for surveillance purposes are overblown and would not require sweeping legislation and major changes in the Code of Criminal Procedure that this bill would provide.

Effect on law enforcement officers. CSHB 1608 is not friendly to government and would have a detrimental effect on the law enforcement community. Peace officers work in law enforcement because they want to protect citizens and help people. Bills, such as this one, that raise barriers to law enforcement efforts send the message that the Legislature doesn’t trust law enforcement. Modern technology provides important tools that allow law enforcement to successfully execute their duties, but this bill would attempt to take those tools away. This culture is disheartening to long-serving law enforcement officers and discourages recruitment. Law enforcement officers feel that their efforts and successes are being met with scorn and discouragement rather than gratitude and praise.