FINAL BILL REPORT
ESHB 1440

C 222 L 15
Synopsis as Enacted

Brief Description: Prohibiting the use of a cell site simulator device without a warrant.

Sponsors: House Committee on Public Safety (originally sponsored by Representatives Taylor, Goodman, Pollet, Scott, Condotta, Shea, G. Hunt, Young, Moscoso, Smith, Ryu, Jinkins, Magendanz, Farrell and McCaslin).

House Committee on Public Safety
Senate Committee on Law & Justice

Background:

Generally, a cell site simulator is a device that can impersonate a wireless service provider's (i.e., cellular phone company's) cell tower, prompting mobile phones and other wireless devices to communicate with the simulators instead of with the legitimate cell towers. Such devices are able to intercept conversations and can track cell phone signals inside vehicles, homes, and insulated buildings.

A pen register is a device attached to a telephone line that records the phone numbers dialed from that telephone line. A trap and trace device is a device attached to a telephone line that records the telephone numbers of all calls coming into that telephone line. Federal and state law regulate the installation and use of both of these devices.

A pen register or trap and trace device may be installed and used by law enforcement agencies pursuant to an authorizing court order or in certain emergency situations.

Court Authorization. A law enforcement officer may apply to the superior court for a court order authorizing the installation and use of a pen register or a trap and trace device. The court must authorize the installation and use of the device if the court finds: (1) that the information likely to be gained is relevant to an ongoing criminal investigation; and (2) there is probable cause to believe that the device will lead to evidence of a crime, contraband, fruits of crime, items criminally possessed, weapons, or things by means of which a crime has been committed or reasonably appears about to be committed.

The court order must specify the identity of the person registered to the affected line, the identity of the subject of the criminal investigation, the number and physical location of the

---

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

affected line, and a statement of the offense to which the information likely to be obtained relates.

The court order is valid for a period not to exceed 60 days. A 60-day extension may be ordered based upon a new application and a court finding that there is probability that the information sought is more likely to be obtained under the extension than under the original order. No extension beyond the first extension may be granted unless: (1) there is a showing that there is a high probability that the information sought is more likely to be obtained under a subsequent order; or (2) there are extraordinary circumstances shown, such as immediate danger of death or injury to an officer. The existence of the pen register or trap and trace device may not be disclosed by any person except by court order.

If requested by the law enforcement officer and directed by the court, providers of wire or electronic communication services and other appropriate persons must provide the law enforcement officer authorized to install a pen register or trap and trace device with all information, facilities, and technical assistance necessary to complete the installation. A person who provides assistance must be reasonably compensated for the person's services and is immune from civil or criminal liability for any information, facilities, or assistance provided in good faith reliance on a court order authorizing the installation.

Emergency Situations. A pen register or trap and trace device may be installed without prior court authorization if a law enforcement officer and a prosecuting attorney or deputy prosecuting attorney jointly and reasonably determine that there is probable cause to believe that: (a) an emergency exists involving immediate danger of death or serious bodily injury to any person; (b) the pen register or trap and trace device needs to be installed before an authorizing court order can be obtained; and (c) grounds exist upon which an authorizing court order could be entered. A court order approving the use of the pen register or trap and trace device in an emergency situation must be obtained within 48 hours after its installation.

In the absence of an authorizing court order, the use of a pen register or trap and trace device must immediately terminate once the information sought is obtained, when the application for the order is denied, or when 48 hours have elapsed since the installation, whichever is earlier. If a court order approving the installation is not obtained within 48 hours, any information obtained from the installation is not admissible as evidence in any legal proceeding.

A law enforcement agency must file a monthly report with the Administrative Office of the Courts indicating the number of authorizations made by the agency without a court order, the date and time of each authorization, and whether a subsequent court authorization was sought and granted. An officer who knowingly installs a pen register or trap and trace device without court authorization and who does not seek court authorization within 48 hours is guilty of a gross misdemeanor.

Privacy Act. The Privacy Act (Act) restricts the interception or recording of private communications or conversations. As a general rule, it is unlawful for any person to intercept or record a private communication or conversation without first obtaining the consent of all persons participating in the communication or conversation. There are limited exceptions to this general rule that allow the communication or conversation to be

intercepted and recorded when only one party consents. The Act allows a court to order interceptions of communications without the consent of any party to the communication only in cases involving danger to national security, human life, or imminent arson or riot. Trap and trace devices are not considered private communications under the Act.

Electronic communication means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include any wire or oral communication, any communication made through a tone-only paging device, or any communication from a tracking device.

The act does not regulate cell site simulators.

Summary:

The Act is expanded to regulate the use of cell site simulators. The regulations applicable to pen registers and trap and trace devices are also extended to regulate cell site simulators. No person may install or use a cell site simulator device without prior court authorization except as specifically authorized under the Act. A law enforcement officer must obtain a court order for the installation and use of a cell site simulator unless there is probable cause to believe an emergency exists.

The court order must specify the following:

- the identity of who is subscribed to the affected line;
- the identity of the subject of the criminal investigation;
- the number and physical location of the affected line, the type of device, all categories of information to be collected from the targeted device, whether the cell site simulator device will incidentally collect information from any parties not specified in the court order, and any disruptions to access or use of a communications or Internet access network that may be created; and
- a statement of the offense to which the information likely to be obtained relates.

Law enforcement agencies authorized to use a cell site simulator device must: (1) take all steps necessary to limit the collection of any information or metadata to the target specified in the applicable court order; (2) take all steps necessary to permanently delete any information or metadata collected from any party not specified in the court order immediately following such collection, and not transmit or use such information or metadata for any purpose; and (3) delete any information or metadata collected from the target specified in the court order within 30 days if there is no longer probable cause to support the belief that such information or metadata is evidence of a crime.

The state and its political subdivisions, by means of a cell site simulator device, may not collect or use a person's electronic data or metadata without: (1) that person's informed consent; (2) a warrant, based upon probable cause, that describes with particularity the person, place, or thing to be searched or seized; or (3) acting in accordance with a legally recognized exception to the warrant requirements.

A cell site simulator device is a device that transmits or receives radio waves for the purpose of conducting one or more of the following operations: (1) identifying, locating, or tracking the movements of a communications device; (2) intercepting, obtaining, accessing, or forwarding the communications, stored data, or metadata of a communications device; (3) affecting the hardware or software operations or functions of a communications device; (4) forcing transmissions from or connections to a communications device; (5) denying a communications device access to other communications devices, communications protocols, or services; or (6) spoofing or simulating a communications device, cell tower, cell site, or service. A cell site simulator device includes, but is not limited to, an international mobile subscriber identity catcher or other invasive cell phone or telephone surveillance or eavesdropping device that mimics a cell phone tower and sends out signals to cause cell phones in the area to transmit their locations, identifying information, and communications content, or as a passive interpretation device or digital analyzer that does not send signals to a communications device under surveillance. A cell site simulator device does not include devices used or installed by an electric utility to measure electrical usage, to provide services to customers, or to operate the electric grid.

Electronic communication does not include any communication from a tracking device, but solely to the extent the tracking device is owned by the applicable law enforcement agency.

Votes on Final Passage:

House	97	0	
Senate	47	0	(Senate amended)
House	96	0	(House concurred)

Effective: May 11, 2015