HOUSE BILL REPORT
ESHB 1440

As Passed House:
March 4, 2015

Title: An act relating to prohibiting the use of a cell site simulator device without a warrant.

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).

Brief History:
Committee Activity:
Public Safety: 2/4/15, 2/13/15 [DPS].
Floor Activity:
Passed House: 3/4/15, 97-0.

Brief Summary of Engrossed Substitute Bill

- Expands the Privacy Act to prohibit the use of a cellsite simulator device unless authorized pursuant to a court order or in certain emergency situations.
- Prohibits the state and its political subdivisions from collecting or using a person's electronic data or metadata without: (1) that person's informed consent; (2) a warrant; or (3) a legally recognized exception to the warrant requirements.
- Requires law enforcement to limit or delete certain types of information that is collected through the use of a cell site simulator device from a party not specified in a court order targeted for that purpose.

HOUSE COMMITTEE ON PUBLIC SAFETY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Goodman, Chair; Orwall, Vice Chair; Klippert, Ranking Minority Member; Hayes, Assistant Ranking Minority Member; Appleton, Griffey, Moscoso, Pettigrew and Wilson.

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.

Staff: Yvonne Walker (786-7841).

Background:

Generally a "cell site simulator" is known as 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 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.

Currently, Washington's Privacy Act (Act) does not regulate cell site simulators.

Privacy Act. The Privacy 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 "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.

Summary of Engrossed Substitute Bill:

The Act is amended to provide regulations for the use of cell site simulators. The same statutory provisions that regulate 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 whom is subscribed to the affected line;
- the identity of the subject of the criminal investigation;
- the number and physical location of the affected line, as well as 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 prohibits the transmittal or use of 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, cannot 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 including, but 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.

As defined in the Act, "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.

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill contains an emergency clause and takes effect immediately.

Staff Summary of Public Testimony:

(In support) Sting Rays, also known as cell tower simulator devices, collect data and metadata from cell phone devices. Although these devices are targeting a single individual, in actuality they are able to gather data from other cell phones that happened to come within range of the device.

These devices are designed to undermine a relationship of trust between a consumer and a private company. They are designed to fraudulently tell a person's phone that they are connected and are currently communicating with a cell phone company. These devices do not just capture information about targets they inherently have to sweep up information about other devices that connect to them. This is not just invading the privacy of a target on a court order but is also collecting information on innocent bystanders.

(In support with amendments) A few amendments should be added to the bill. The definition should be amended; additional requirements should be made on law enforcement to tell judges how they will be using these devices along with their impact; and lastly, there should be specific rules around the information collected from those individuals that are not targets of a court order.

The right to privacy in Washington has a long and important history and the Washington Constitution specifically protects the right to privacy. Law enforcement should not be able to use a cell site simulator absent a warrant, a recognized exception to the warrant requirement, or by consent. This bill will protect Washington citizens from warrantless data collection and invasion of privacy.

(With concerns) There is support for this version of the bill with one exception, the first section of the bill should be deleted as it reaches beyond the intent of the bill.

(Opposed) None.

Persons Testifying: (In support) Representative Taylor, prime sponsor; and Jared Friend, American Civil Liberties Union of Washington.

(In support with amendments) Kent Underwood, Washington Association of Criminal Defense Lawyers.

(With concerns) James McMahan, Washington Association of Sheriffs and Police Chiefs.

Persons Signed In To Testify But Not Testifying: None.