

SENATE BILL REPORT

ESHB 1440

As of March 20, 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: Passed House: 3/04/15, 97-0.

Committee Activity: Law & Justice: 3/12/15.

SENATE COMMITTEE ON LAW & JUSTICE

Staff: Tim Ford (786-7423)

Background: A cell site simulator, sometimes known as a stingray, is a device that acts like a cell phone tower and prompts mobile phones and other wireless devices to communicate with the simulator instead of with a wireless service provider's cell tower. Using a cell site simulator, a government agency or individual can locate, interfere with, and even intercept communications from cell phones and other wireless devices.

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. 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.

Washington's 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 (1) consent by all participants in the communication; (2) a warrant; or (3) a legally recognized exception to the warrant requirements. Consent is presumed obtained where one party announces the intent to record a conversation. There are limited exceptions for emergency response personnel, the Department of Corrections, building owners, and common carriers for the construction, maintenance, repair, and operations of equipment. Information obtained in violation of the Act is inadmissible in any civil or criminal case. Any person injured by a violation of the Act

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.

may bring a legal action for actual damages, including mental pain and suffering, or liquidated damages not to exceed \$1,000 and reasonable attorney's fees and costs of litigation.

The Act regulates the installation and use of a pen register and a trap and trace device. The Act does not regulate cell site simulators.

Summary of 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, and 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;
- 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.

Committee/Commission/Task Force Created: No.

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

Staff Summary of Public Testimony: PRO: Cell site simulators are being used in Pierce County and around the nation. This bill would regulate the procedures for their use. Courts were unaware that law enforcement has been using these devices. Not only do these devices collect information from your mobile phones, like emails, pictures, and messages, but they also disrupt the ability to make phone calls. The right to privacy in Washington is protected by Article I, section 7 of the Washington Constitution. Law enforcement should not be permitted to obtain evidence using a cell site simulator absent consent, a valid warrant, or a recognized exception to a warrant. Law enforcement, when seeking a warrant, should disclose to a judge if a cell site simulator will be used. The technology needs to be tested in court. Inaccurate information will lead to wrongful convictions. Without disclosure, the risk of abuse increases.

OTHER: The bill's definition of a cell site simulator is very broad. It should not include advanced power meters.

Persons Testifying: PRO: Representative Taylor, prime sponsor; Christopher Soghoian, American Civil Liberties Union (ACLU); Jared Friend, ACLU of WA; Ramona Brandes, WA Criminal Defense Lawyers, WA Defenders Assn.

OTHER: Brenda White, Snohomish PUD.

Persons Signed in to Testify But Not Testifying: No one.