



**Substitute House Bill No. 7291**

**Public Act No. 17-221**

**AN ACT CONCERNING THE USE OF CELL SITE SIMULATOR DEVICES BY LAW ENFORCEMENT OFFICIALS TO CONDUCT CELLULAR TELEPHONE SURVEILLANCE.**

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Section 54-41a of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2017*):

The following words and phrases, as used in this chapter, [shall] have the following meanings, unless the context otherwise requires:

(1) "Wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of telephone or telegraph between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of intrastate, interstate or foreign communications;

(2) "Intercept" means the intentional overhearing or recording of a wire communication through the use of any electronic, mechanical or other device or a cell site simulator device;

(3) "Electronic, mechanical or other device" means any device or

**Substitute House Bill No. 7291**

apparatus which can be used to intercept a wire communication other than (A) any telephone or telegraph instrument, equipment or facility, or any component thereof (i) furnished to the subscriber or used by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business, or (ii) being used by a communications common carrier in the ordinary course of its business, or (B) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(4) "Cell site simulator device" means a device that transmits or receives radio waves for the purpose of conducting one or more of the following operations: (A) Identifying, locating or tracking the movements of a communications device, (B) intercepting, obtaining, accessing or forwarding the communications, stored data or metadata of a communications device, (C) affecting the hardware or software operations or functions of a communications device, (D) forcing transmissions from, or connections to, a communications device, (E) denying a communications device access to other communications devices, communications protocols or services, or (F) spoofing or simulating a communications device, cell tower, cell site or service. "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 a passive interception device or digital analyzer that does not send signals to a communications device under surveillance. "Cell site simulator device" does not include any device used or installed by an electric distribution company, as defined in section 16-1, solely to the extent that such device is used by the electric distribution company to measure electrical usage, to provide services to customers or to operate the electric grid;

**Substitute House Bill No. 7291**

[(4)] (5) "Person" means any officer, agent or employee of the state of Connecticut or any political subdivision thereof, and any individual, partnership, association, joint stock company, trust, limited liability company or corporation;

[(5)] (6) "Investigative officer" means (A) any officer of the Connecticut state police, (B) the chief inspector or any inspector in the Division of Criminal Justice who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, (C) any municipal police officer who has been duly sworn as a special state police officer under the provisions of section 29-177 and who is currently assigned to the state-wide narcotics task force or the state-wide organized crime investigative task force and is acting under the direct authority of the Connecticut state police, and (D) any attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in this chapter;

[(6)] (7) "Law enforcement officer" means any officer of any organized police department of this state or of the state police of any other state, an official of the Federal Bureau of Investigation, Drug Enforcement Administration or United States Customs Service, or the United States attorney for the district of Connecticut or a person designated by him in writing to receive the contents of any wire communication or evidence derived therefrom;

[(7)] (8) "Contents", when used with respect to any wire communication, means and includes any information concerning the identity of the parties to such communication or the existence, substance, purport or meaning of that communication;

[(8)] (9) "Panel of judges" or "panel" means any panel or panels of three Superior Court judges specifically designated by the Chief Justice of the Supreme Court from time to time to receive applications for, and to enter orders authorizing, interceptions of wire communications in

**Substitute House Bill No. 7291**

accordance with the provisions of this chapter;

[(9)] (10) "Communication common carrier" means any person engaged as a common carrier for hire in the transmission of communications by wire or radio;

[(10)] (11) "Aggrieved person" means a person who was a party to any intercepted wire communication, a person against whom the interception was directed, a person named in any order authorizing an interception, or a person having a property interest in any premises involved in any interception.

Sec. 2. Section 54-47aa of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2017*):

(a) For the purposes of this section:

(1) "Basic subscriber information" means: (A) Name, (B) address, (C) local and long distance telephone connection records or records of session times and durations, (D) length of service, including start date, and types of services utilized, (E) telephone or instrument number or other subscriber number or identity, including any assigned Internet protocol address, and (F) means and source of payment for such service, including any credit card or bank account number;

(2) "Call-identifying information" means dialing or signaling information that identifies the origin, direction, destination or termination of each communication generated or received by a subscriber or customer, excluding geo-location data, by means of any equipment, facility or service of a telecommunications carrier;

(3) "Cell site simulator device" means a device that transmits or receives radio waves for the purpose of conducting one or more of the following operations: (A) Identifying, locating or tracking the movements of a communications device, (B) intercepting, obtaining,

***Substitute House Bill No. 7291***

accessing or forwarding the communications, stored data or metadata of a communications device, (C) affecting the hardware or software operations or functions of a communications device, (D) forcing transmissions from, or connections to, a communications device, (E) denying a communications device access to other communications devices, communications protocols or services, or (F) spoofing or simulating a communications device, cell tower, cell site or service. "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 a passive interception device or digital analyzer that does not send signals to a communications device under surveillance. "Cell site simulator device" does not include any device used or installed by an electric distribution company, as defined in section 16-1, solely to the extent that such device is used by the electric distribution company to measure electrical usage, to provide services to customers or to operate the electric grid;

[(3)] (4) "Electronic communication service" means "electronic communication service" as defined in 18 USC 2510, as amended from time to time;

[(4)] (5) "Exigent circumstance" means an emergency involving danger of serious physical injury to or death of a person;

[(5)] (6) "Geo-location data" means information concerning the location of an electronic device, including the real-time and historical location of the device, that, in whole or in part, is generated by, derived from or obtained by the operation of an electronic device, including, but not limited to, a cellular telephone surveillance device and a cell site simulator device;

**Substitute House Bill No. 7291**

[(6)] (7) "Law enforcement official" means the Chief State's Attorney, a state's attorney, an inspector with the Division of Criminal Justice, a sworn member of the Division of State Police within the Department of Emergency Services and Public Protection or a sworn member of an organized local police department;

[(7)] (8) "Remote computing service" means "remote computing service" as defined in section 18 USC 2711, as amended from time to time; and

[(8)] (9) "Telecommunications carrier" means "telecommunications carrier" as defined in 47 USC 1001, as amended from time to time.

(b) A law enforcement official may apply for an ex parte order from a judge of the Superior Court to compel (1) a telecommunications carrier to disclose call-identifying information pertaining to a subscriber or customer, (2) a provider of electronic communication service or remote computing service to disclose basic subscriber information pertaining to a subscriber or customer, or (3) a telecommunications carrier or a provider of electronic communication service or remote computing service to disclose the content of a subscriber's or customer's communications or geo-location data associated with a subscriber's or customer's call-identifying information. The judge shall grant such order if the law enforcement official swears under oath to a statement of (A) a reasonable and articulable suspicion that a crime has been or is being committed and such call-identifying or basic subscriber information is relevant and material to an ongoing criminal investigation, in which case such order shall not authorize disclosure of the content of any communication or geo-location data, or (B) probable cause to believe that a crime has been or is being committed and the content of such subscriber's or customer's communications or the geo-location data associated with such subscriber's or customer's call-identifying information is relevant and material to an ongoing criminal investigation, in which case such

***Substitute House Bill No. 7291***

order shall authorize the disclosure of such information, content or geo-location data. Any such order entered pursuant to this subsection shall state upon its face the case number assigned to such investigation, the date and time of issuance and the name of the judge authorizing the order. The law enforcement official shall have any ex parte order issued pursuant to this subsection signed by the authorizing judge within forty-eight hours or not later than the next business day, whichever is earlier. No order pursuant to this subsection shall authorize the disclosure of any such information, content or data for a period in excess of fourteen days.

(c) (1) Except as provided in subdivision (2) of this subsection, a law enforcement official shall not install or otherwise use a cell site simulator device to obtain geo-location data unless such official has obtained an order from a judge of the Superior Court, pursuant to this subsection, that permits such installation or use. A law enforcement official may apply for an ex parte order from a judge of the Superior Court allowing the installation and use of a cell site simulator device to obtain geo-location data. The judge shall grant such order if the law enforcement official swears in a statement under oath that there is probable cause to believe that a crime has been or is being committed and the geo-location data associated with a subscriber's or customer's call-identifying information is relevant and material to an ongoing criminal investigation, in which case such order shall authorize the installation or use of a cell site simulator device to obtain geo-location data. Any order entered pursuant to this subdivision shall state upon its face the case number assigned to such investigation, the date and time of issuance of the order and the name of the judge authorizing the order. The law enforcement official shall have any ex parte order issued pursuant to this subdivision signed by the authorizing judge within forty-eight hours or not later than the next business day, whichever is earlier. No order issued pursuant to this subdivision shall authorize the installation of cell site simulator device to obtain geo-

***Substitute House Bill No. 7291***

location data for a period in excess of fourteen days.

(2) A law enforcement official may install and use a cell site simulator device to obtain geo-location data without an ex parte order for a period of time not exceeding forty-eight hours when (A) facts exist upon which to base a belief that the geo-location data is relevant and material to an ongoing criminal investigation; (B) the law enforcement official believes that exigent circumstances exist; and (C) the facts support the law enforcement official's belief that exigent circumstances exist. If the law enforcement official seeks to install and use a cell site simulator device to obtain geo-location data relating to the same criminal investigation for a period of time exceeding forty-eight hours, such official shall apply for an ex parte order in accordance with the provisions of subdivision (1) of this subsection. In addition, the law enforcement official shall file as part of the application, a statement under oath attesting to the facts and beliefs concerning the exigent circumstances that existed and supported the use of the cell site simulator device for a period of time not exceeding forty-eight hours. The law enforcement official shall include in such statement the date and time of use of the cell site simulator device.

[(c)] (d) A law enforcement official may apply directly to a telecommunications carrier or provider of electronic communication service or remote computing service for production of geo-location data for a period not in excess of forty-eight hours, including real-time or historical geo-location data, or any combination of such data, pertaining to an identified subscriber or customer. The telecommunications carrier or provider of electronic telecommunication service or remote computing service may provide the requested geo-location data upon the applicant stating under oath: (1) That facts exist upon which to base a belief that the data sought is relevant and material to an ongoing criminal investigation; (2) a belief that exigent circumstances exist; and (3) the facts supporting the belief



***Substitute House Bill No. 7291***

that exigent circumstances exist. Any subsequent application for information from the same telecommunication carrier or provider of electronic communication service or remote computing service for production of geo-location data in connection with the same investigation shall be made pursuant to subsection (b) of this section.

~~[(d)]~~ (e) A telecommunications carrier shall disclose call-identifying information and a provider of electronic communication service or remote computing service shall disclose basic subscriber information to a law enforcement official when an order is issued pursuant to subsection (b) of this section.

~~[(e)]~~ (f) Not later than forty-eight hours after the issuance of an order pursuant to subsection (b) of this section, the law enforcement official shall mail notice of the issuance of such order to the subscriber or customer whose call-identifying information or basic subscriber information is the subject of such order, except that such notification may be delayed for a period of up to ninety days upon the execution of a written certification of such official to the judge who authorized the order that there is reason to believe that notification of the existence of the order may result in (1) endangering the life or physical safety of an individual, (2) flight from prosecution, (3) destruction of or tampering with evidence, (4) intimidation of potential witnesses, or (5) otherwise seriously jeopardizing the investigation. The law enforcement official shall maintain a true copy of such certification. During such ninety-day period, the law enforcement official may request the court to extend such period of delayed notification. Such period may be extended beyond ninety days only upon approval of the court. The applicant shall file a copy of the notice with the clerk of the court that issued such order. If information is provided in response to the order, the applicant shall, not later than ten days after receiving such information, file with the clerk a return containing an inventory of the information received. If a judge finds there is a significant likelihood

**Substitute House Bill No. 7291**

that such notification would seriously jeopardize the investigation and issues an order authorizing delayed notification under this subsection, the telecommunications carrier or provider of electronic communication service or remote computing service from whom the call-identifying information or basic subscriber information is sought shall not notify any person, other than legal counsel for the telecommunications carrier or provider of electronic communication service or remote computing service and the law enforcement official that requested the ex parte order, of the existence of the ex parte order. Any information provided in response to the court order shall be disclosed to the defense counsel.

~~[(f)]~~ (g) A telecommunications carrier or provider of electronic communication service or remote computing service that provides information pursuant to an order issued pursuant to subsection (b) of this section or pursuant to an application made pursuant to subsection ~~[(c)]~~ (d) of this section shall be compensated for the reasonable expenses incurred in providing such information.

~~[(g)]~~ (h) Any telecommunications carrier or provider of electronic communication service or remote computing service that provides information pursuant to an order issued pursuant to subsection (b) of this section or an application made pursuant to subsection ~~[(c)]~~ (d) of this section shall be afforded the legal protections provided under 18 USC 3124, as amended from time to time, with regard to such actions.

~~[(h)]~~ (i) No information obtained pursuant to [subsection (b) or (c)] subsections (b) to (d), inclusive, of this section shall be retained for a period in excess of fourteen days, unless such information relates to an ongoing criminal investigation. Any information provided pursuant to [said subsection (b) or (c)] subsections (b) to (d), inclusive, of this section shall be disclosed to the defense counsel.

~~[(i)]~~ (j) Not later than January fifteenth of each year, each law

***Substitute House Bill No. 7291***

enforcement official shall report to the Chief State's Attorney the information required by this subsection with respect to each order issued pursuant to [subsection (b)] subsections (b) and (c) of this section and each application made pursuant to subsection [(c)] (d) of this section in the preceding calendar year. The Chief State's Attorney shall, based upon the reports filed by each law enforcement official and not later than January thirty-first of each year, submit a report, in accordance with the provisions of section 11-4a, to the joint standing committee of the General Assembly having cognizance of matters relating to criminal law and procedure concerning orders issued pursuant to [subsection (b)] subsections (b) and (c) of this section and applications made pursuant to subsection [(c)] (d) of this section in the preceding calendar year. The report shall include the following information: (1) The number of orders issued pursuant to [subsection (b)] subsections (b) and (c) of this subsection and the number of applications submitted to telecommunications carriers or providers of electronic communication service or remote computing service pursuant to subsection [(c)] (d) of this section, (2) whether the order was directed to a telecommunications carrier, provider of electronic communication service or provider of remote computing service, (3) whether the information sought was call-identifying information or basic subscriber information, (4) the statutory offense or offenses that were the subject of the investigation, (5) the number of notifications that were delayed pursuant to subsection [(e)] (f) of this section, and the reason for such delayed notification, (6) the number of motions to vacate an order that were filed, and the number of motions granted or denied, (7) the number of investigations concluded and the final result of such investigations, and (8) the status of any criminal prosecution resulting from the investigation.

Approved July 10, 2017