

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 618 Session of
2017

INTRODUCED BY CRUZ, YOUNGBLOOD, THOMAS AND GILLEN,
FEBRUARY 24, 2017

REFERRED TO COMMITTEE ON JUDICIARY, FEBRUARY 24, 2017

AN ACT

1 Amending Title 18 (Crimes and Offenses) of the Pennsylvania
2 Consolidated Statutes, in wiretapping and electronic
3 surveillance, further providing for definitions, for
4 exceptions to prohibition of interception and disclosure of
5 communications, for possession, sale, distribution,
6 manufacture or advertisement of electronic, mechanical or
7 other devices and telecommunication identification
8 interception devices and for general prohibition on use of
9 certain devices and exception, providing for application for
10 warrant for use of cell site simulator devices and for
11 issuance of warrant for use of cell site simulator devices
12 and further providing for reports concerning certain devices;
13 and making editorial changes.

14 The General Assembly of the Commonwealth of Pennsylvania
15 hereby enacts as follows:

16 Section 1. Section 5702 of Title 18 of the Pennsylvania
17 Consolidated Statutes is amended by adding a definition to read:
18 § 5702. Definitions.

19 As used in this chapter, the following words and phrases
20 shall have the meanings given to them in this section unless the
21 context clearly indicates otherwise:

22 * * *

23 "Cell site simulator device." A device that transmits or

1 receives radio waves for the purpose of conducting one or more
2 of the following operations:

3 (1) Identifying, locating or tracking the movements of a
4 communications device.

5 (2) Intercepting, obtaining, accessing or forwarding the
6 communications, stored data or metadata of a communications
7 device.

8 (3) Affecting the hardware or software of a
9 communications device.

10 (4) Forcing transmissions from or connections to a
11 communications device.

12 (5) Denying a communications device access to other
13 communications devices, communications protocols or
14 communications services.

15 (6) Spoofing or simulating a communications device, cell
16 tower, cell site or communication service, including, but not
17 limited to, an international mobile subscriber identity
18 catcher or other invasive mobile phone or telephone
19 surveillance or eavesdropping device that mimics a cell tower
20 and sends out signals to cause communications devices in the
21 area to transmit their locations, identifying information and
22 contents or a passive interception device or digital analyzer
23 that does not send signals to a communications device under
24 surveillance.

25 * * *

26 Section 2. Section 5704(5) of Title 18 is amended to read:

27 § 5704. Exceptions to prohibition of interception and
28 disclosure of communications.

29 It shall not be unlawful and no prior court approval shall be
30 required under this chapter for:

1 * * *

2 (5) Any investigative or law enforcement officer, or
3 communication common carrier acting at the direction of an
4 investigative or law enforcement officer or in the normal
5 course of its business, to use a pen register, trap and trace
6 device [or], telecommunication identification interception
7 device or cell site simulator device as provided in
8 Subchapter E (relating to pen registers, trap and trace
9 devices [and], telecommunication identification interception
10 devices and cell site simulator devices).

11 * * *

12 Section 3. Section 5705 heading of Title 18 is amended and
13 the section is amended by adding a paragraph to read:

14 § 5705. Possession, sale, distribution, manufacture or
15 advertisement of electronic, mechanical or other
16 devices [and], telecommunication identification
17 interception devices and cell site simulator devices.

18 Except as otherwise specifically provided in section 5706
19 (relating to exceptions to prohibitions in possession, sale,
20 distribution, manufacture or advertisement of electronic,
21 mechanical or other devices), a person is guilty of a felony of
22 the third degree if he does any of the following:

23 * * *

24 (6) Intentionally possesses a cell site simulator
25 device.

26 Section 4. The heading of Subchapter E of Chapter 57 of
27 Title 18 is amended to read:

28 SUBCHAPTER E

29 PEN REGISTERS, TRAP AND TRACE DEVICES

30 [AND], TELECOMMUNICATION IDENTIFICATION

1 INTERCEPTION DEVICES AND CELL SITE

2 SIMULATOR DEVICES

3 Section 5. Section 5771(a) and (b) of Title 18 are amended
4 and the section is amended by adding a subsection to read:

5 § 5771. General prohibition on use of certain devices and
6 exception.

7 (a) General rule.--Except as provided in this section, no
8 person may install or use a pen register [or], a trap and trace
9 device or a telecommunication identification interception
10 device, without first obtaining a court order under section 5773
11 (relating to issuance of an order for use of certain devices)
12 [.] , or a cell site simulator device without first obtaining a
13 warrant under section 5773.1 (relating to issuance of warrant
14 for use of cell site simulator devices).

15 [(b) Exception.--The prohibition of subsection (a) does not
16 apply with respect to the use of a pen register, a trap and
17 trace device or a telecommunication identification interception
18 device by a provider of electronic or wire communication
19 service:

20 (1) relating to the operation, maintenance and testing
21 of a wire or electronic communication service or to the
22 protection of the rights or property of the provider, or to
23 the protection of users of the service from abuse of service
24 or unlawful use of service;

25 (2) to record the fact that a wire or electronic
26 communication was initiated or completed in order to protect
27 the provider, another provider furnishing service toward the
28 completion of the wire communication or a user of the service
29 from fraudulent, unlawful or abusive use of service; or

30 (3) with the consent of the user of the service.]

1 * * *

2 (b.2) Exceptions.--The prohibition of subsection (a) does
3 not apply with respect to the use of the following:

4 (1) A pen register, a trap and trace device or a
5 telecommunication identification interception device by a
6 provider of electronic or wire communication service:

7 (i) relating to the operation, maintenance and
8 testing of a wire or electronic communication service, to
9 the protection of the rights or property of the provider
10 or to the protection of users of the service from abuse
11 of service or unlawful use of service;

12 (ii) to record the fact that a wire or electronic
13 communication was initiated or completed in order to
14 protect the provider, another provider furnishing service
15 toward the completion of the wire communication or a user
16 of the service from fraudulent, unlawful or abusive use
17 of service; or

18 (iii) with the consent of the user of the service.

19 (2) A cell site simulator device by an investigative or
20 law enforcement agency, a government agency or a
21 communication common carrier acting at the direction of an
22 investigative or law enforcement officer:

23 (i) as provided in section 5773.1;

24 (ii) if the communications device is reported stolen
25 by the user;

26 (iii) with the consent of the user of the service;

27 or

28 (iv) with the consent of the legal guardian or next
29 of kin of the user if the user is believed to be deceased
30 or reported missing and unable to be contacted.

1 * * *

2 Section 6. Title 18 is amended by adding sections to read:

3 § 5772.1. Application for warrant for use of cell site
4 simulator devices.

5 (a) Application.--The Attorney General or a deputy attorney
6 general designated in writing by the Attorney General or a
7 district attorney or an assistant district attorney designated
8 in writing by the district attorney may make application for a
9 warrant or an extension of warrant under section 5773.1
10 (relating to issuance of warrant for use of cell site simulator
11 devices) authorizing or approving the installation and use of a
12 cell site simulator device under this subchapter. The
13 application shall be made in writing and under oath or
14 equivalent affirmation to:

15 (1) a court of common pleas having jurisdiction over the
16 offense under investigation; or

17 (2) any Superior Court judge when an application for a
18 warrant authorizing interception of communications is or has
19 been made for the targeted communications device or another
20 application for interception under this subchapter has been
21 made involving the same investigation.

22 (b) Contents of application.--An application under
23 subsection (a) shall include:

24 (1) The identity and authority of the attorney making
25 the application and the identity of the investigative or law
26 enforcement agency conducting the investigation.

27 (2) A certification by the applicant that the
28 information likely to be obtained is relevant to an ongoing
29 criminal investigation being conducted by that agency.

30 (3) An affidavit by an investigative or law enforcement

officer that establishes probable cause for the issuance of a
warrant or an extension under section 5773.1.

§ 5773.1. Issuance of warrant for use of cell site simulator
devices.

(a) In general.--Upon an application made under section
5772.1 (relating to application for warrant for use of cell site
simulator devices), the court shall authorize the installation
and use of a cell site simulator device within this Commonwealth
if the court finds that there is probable cause to believe that
information relevant to an ongoing criminal investigation will
be obtained by the installation and use on the targeted
communications device. If exigent circumstances exist, the court
may verbally authorize the installation and use of a cell site
simulator device, conditioned upon the filing with the court
within 72 hours thereafter of an application for a warrant. If
granted, the warrant shall be retroactive to the time of the
installation and recite the verbal authorization. In the event
an application for a warrant is denied or no application is
made, the use of a cell site simulator device shall immediately
terminate and the metadata, data, information or contents
collected shall be deemed as having been obtained in violation
of this subchapter and shall not be admissible in a criminal
proceeding or used as probable cause in an effort to obtain a
warrant.

(b) Contents of warrant.--A warrant issued under this
section shall:

(1) Specify:

(i) That there is probable cause to believe that
information relevant to an ongoing criminal investigation
will be obtained from the targeted communications device.

1 (ii) The identity, if known, of the person or
2 persons using the targeted communications device.

3 (iii) The identity, if known, of the person who is
4 the subject of the criminal investigation.

5 (iv) The telephone number or other unique number
6 identifying the communication service account used by the
7 targeted communications device.

8 (v) If known, the physical location of the
9 communications device.

10 (vi) The type of communications device and the
11 communications protocols being used by the communications
12 device.

13 (vii) The geographic area that will be covered by
14 the cell site simulator device.

15 (viii) All categories of metadata, data, information
16 or contents to be collected from the targeted
17 communications device.

18 (ix) Whether the cell site simulator will
19 incidentally collect metadata, data, information or
20 contents from any person or communications device not
21 specified in the warrant and, if so, what categories of
22 information or metadata will be collected.

23 (x) Any disruptions to access or use of any
24 communications system that could be potentially created
25 by use of a cell site simulator device.

26 (xi) A statement of the offense to which the
27 information likely to be obtained by the cell site
28 simulator device relates.

29 (2) Direct that a government, investigative or law
30 enforcement agency authorized to use a cell site simulator

1 device under this chapter shall:

2 (i) Record and monitor all interceptions in
3 accordance with section 5714(a)(1) and (2) (relating to
4 recording of intercepted communications).

5 (ii) Take all steps necessary to limit the
6 collection of any information or metadata to the targeted
7 communications device specified in the applicable
8 warrant.

9 (iii) Seal only interceptions from the person and
10 communications device specified in the applicable warrant
11 in accordance with section 5714(b).

12 (iv) Permanently delete any information or metadata
13 collected from any person or communications device not
14 specified in the applicable warrant immediately following
15 the collection and shall not transmit, use or retain the
16 information or metadata for any purpose.

17 (c) Time period and extensions.--

18 (1) A warrant issued under this section shall authorize
19 the installation and use of a cell site simulator device for
20 a period not to exceed 60 days.

21 (2) Extensions of the warrant may be granted but only
22 upon an application for a warrant under section 5772.1 and
23 upon the judicial finding required under subsection (a). The
24 period of each extension shall not exceed 30 days.

25 (d) Nondisclosure of existence of a cell site simulator
26 device.--A warrant authorizing or approving the installation and
27 use of a cell site simulator device shall direct all of the
28 following:

29 (1) The warrant be sealed until otherwise ordered by the
30 court.

1 (2) The person owning or leasing the targeted
2 communications device or who has been ordered by the court to
3 provide assistance to the applicant not disclose the
4 existence of the cell site simulator device or the existence
5 of the investigation to the listed subscriber or to any other
6 person, unless or until otherwise ordered by the court.

7 Section 7. Section 5775 of Title 18 is amended to read:

8 § 5775. Reports concerning certain devices.

9 (a) Attorney General.--The Attorney General shall annually
10 report to the Administrative Office of Pennsylvania Courts on
11 the number of orders for pen registers, trap and trace devices
12 [and], telecommunication identification interception devices and
13 warrants for cell site simulator devices applied for by
14 investigative or law enforcement agencies of the Commonwealth or
15 its political subdivisions.

16 (b) District attorney.--Each district attorney shall
17 annually provide to the Attorney General information on the
18 number of orders for pen registers, trap and trace devices
19 [and], telecommunication identification interception devices and
20 warrants for cell site simulator devices applied for on forms
21 prescribed by the Attorney General.

22 Section 8. This act shall take effect in 60 days.