

Senate Bill 1583

Sponsored by Senators GEORGE, SHIELDS, Representatives HUFFMAN, WILLIAMSON

SUMMARY

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure **as introduced**.

Prohibits public body from obtaining location information of cellular telephone or other electronic communication device without warrant, consent or certain emergent circumstances. Specifies warrant requirements. Requires public body to provide notice after obtaining location information. Prohibits use of information in adjudicatory proceeding when obtained in violation of prohibition.

Prohibits public body from obtaining personal electronic data without warrant, consent or certain emergent circumstances. Specifies warrant requirements. Requires public body to provide notice after obtaining personal electronic data. Prohibits use of data in adjudicatory proceeding when obtained in violation of prohibition.

A BILL FOR AN ACT

1
2 Relating to privacy.

3 **Be It Enacted by the People of the State of Oregon:**

4 **SECTION 1. As used in sections 1 to 3 of this 2014 Act:**

5 (1) **"Cellular telephone" has the meaning given that term in ORS 165.575.**

6 (2) **"Electronic communication device" means a device by which any kind of electronic**
7 **communication can be made, including but not limited to communication by telephonic fac-**
8 **simile and electronic mail.**

9 (3) **"Location information" means information concerning the location of a cellular tele-**
10 **phone or other electronic communication device, including both the current location and any**
11 **prior location of the telephone or device, that is generated by or derived from the operation**
12 **or possession of the cellular telephone or other electronic communication device.**

13 (4)(a) **"Personal electronic data" means:**

14 (A) **The record of a person's Internet website browsing history;**

15 (B) **The contents of an electronic mail account;**

16 (C) **The contents of a social media account;**

17 (D) **The record of a person's television program viewing history; and**

18 (E) **The data or contents of any electronic device, including a computer, tablet computer**
19 **or cellular telephone.**

20 (b) **"Personal electronic data" does not include:**

21 (A) **Information that is publicly available;**

22 (B) **Information that a member of the public could obtain by lawful means without the**
23 **consent of the subject of the information;**

24 (C) **Information that is provided to a public body by a third party, unless the information**
25 **was provided at the request of the public body;**

26 (D) **Information that is knowingly provided to a public body by the person who is the**
27 **subject of the information; or**

28 (E) **Information that is stored on an electronic device that has been abandoned or sold**

NOTE: Matter in **boldfaced** type in an amended section is new; matter *[italic and bracketed]* is existing law to be omitted. New sections are in **boldfaced** type.

1 by its owner.

2 (5) "Public body" has the meaning given that term in ORS 192.410.

3 (6) "Social media" has the meaning given that term in ORS 326.551.

4 **SECTION 2.** (1) Except as provided in subsection (3) of this section, a public body may
5 not obtain the location information of a cellular telephone or other electronic communication
6 device without a warrant.

7 (2) A warrant for the location information of a cellular telephone or other electronic
8 communication device may be issued by any circuit court judge upon written application by
9 a district attorney or a police officer. The application must include:

10 (a) The identity of the owner or user of the cellular telephone or other electronic com-
11 munication device;

12 (b) The reason for the location information request;

13 (c) The method that will be used to obtain the location information;

14 (d) Facts establishing probable cause that:

15 (A) The person who is the owner or user of the cellular telephone or other electronic
16 communication device has committed or is in the process of committing a particular crime;
17 and

18 (B) The location information contains evidence of the crime; and

19 (e) An assertion that other investigative procedures will not be effective or sufficient in
20 obtaining the evidence of the crime.

21 (3) A public body may obtain the location information of a cellular telephone or other
22 electronic communication device without a warrant under any of the following circum-
23 stances:

24 (a) The location information is necessary to respond to the user's request for emergency
25 services.

26 (b) The owner or user of the telephone or device consents to the disclosure of the lo-
27 cation information.

28 (c) There is probable cause to believe that the owner or user of the telephone or device
29 has committed a crime and exigent circumstances exist.

30 (d) There is immediate danger of death or serious physical injury to a person and the
31 location information is necessary to prevent the death or injury.

32 (e) The location information is necessary to search for, rescue or recover any person who
33 is missing, injured or deceased.

34 (4)(a) If a public body obtains the location information of a cellular telephone or other
35 electronic communication device, the public body must make a good faith effort to provide
36 notice to the owner or user of the telephone or device within three days after obtaining the
37 location information. The notice must be in writing and must contain the following infor-
38 mation:

39 (A) The nature of the inquiry;

40 (B) The location information that was provided to the public body and the date on which
41 it was provided; and

42 (C) The identity of the provider of the location information.

43 (b) The notification obligation described in this subsection does not apply if the public
44 body is unable to identify the owner or user of the telephone or device.

45 (c) A public body may include in the application for a warrant a request for an order

1 **waiving the notice requirement described in this subsection.**

2 **(5) Any location information that is obtained in violation of this section, and any evidence**
 3 **derived from that information:**

4 **(a) Is not admissible in, and may not be disclosed in, a judicial proceeding, administrative**
 5 **proceeding, arbitration proceeding or other adjudicatory proceeding; and**

6 **(b) May not be used to establish reasonable suspicion or probable cause to believe that**
 7 **an offense has been committed.**

8 **SECTION 3. (1) Except as provided in subsection (3) of this section, a public body may**
 9 **not obtain personal electronic data without a warrant.**

10 **(2) A warrant for personal electronic data may be issued by any circuit court judge upon**
 11 **written application by a district attorney or a police officer. The application must include:**

12 **(a) The identity of the person who is the subject of the personal electronic data sought;**

13 **(b) A description of the type of personal electronic data sought;**

14 **(c) The method that will be used to obtain the personal electronic data;**

15 **(d) Facts establishing probable cause that:**

16 **(A) The person who is the subject of the personal electronic data has committed or is in**
 17 **the process of committing a particular crime; and**

18 **(B) The personal electronic data contains evidence of the crime; and**

19 **(e) An assertion that other investigative procedures will not be effective or sufficient in**
 20 **obtaining the evidence of the crime.**

21 **(3) A public body may obtain personal electronic data without a warrant under any of the**
 22 **following circumstances:**

23 **(a) The person who is the subject of the personal electronic data and who uses, operates**
 24 **or owns the data or the account or device containing the data consents to the disclosure.**

25 **(b) The employer of the person who is the subject of the personal electronic data con-**
 26 **sents to the disclosure of the data and the employer owns the electronic device on which the**
 27 **data can be found.**

28 **(c) There is probable cause to believe that the person who is the subject of the personal**
 29 **electronic data has committed a crime and exigent circumstances exist.**

30 **(d) There is immediate danger of death or serious physical injury to a person and the**
 31 **personal electronic data is necessary to prevent the death or injury.**

32 **(e) The personal electronic data is necessary to search for, rescue or recover any person**
 33 **who is missing, injured or deceased.**

34 **(4)(a) If a public body obtains personal electronic data, the public body must make a good**
 35 **faith effort to provide notice to the person who is the subject of the personal electronic data**
 36 **within three days after obtaining the data. The notice must be in writing and must contain**
 37 **the following information:**

38 **(A) The nature of the inquiry;**

39 **(B) The personal electronic data that was provided to the public body and the date on**
 40 **which it was provided; and**

41 **(C) The identity of the provider of the personal electronic data.**

42 **(b) A public body may include in the application for a warrant a request for an order**
 43 **waiving the notice requirement described in this subsection.**

44 **(5) Any personal electronic data that is obtained in violation of this section, and any ev-**
 45 **idence derived from that data:**

1 **(a) Is not admissible in, and may not be disclosed in, a judicial proceeding, administrative**
2 **proceeding, arbitration proceeding or other adjudicatory proceeding; and**

3 **(b) May not be used to establish reasonable suspicion or probable cause to believe that**
4 **an offense has been committed.**

5
