Model Language: Geofence Warrants

Purpose:
This proposal establishes procedures and requirements for the authorization of reverse location searches by law enforcement or any government entity.

Section 1. Definitions.
As used in this chapter:
(1) "Anonymized" means identifying information connected to an electronic device in a manner such that the subject, including an individual, household, device, or Internet protocol address, is not identifiable to a law enforcement agency.
(2) "Cell site" means transmission or reception equipment, including a base-station antenna, that connects an electronic device to a network.
(3) "Cell site record" means the cell site location information of an electronic device that corresponds to a specific cell site and time frame.
(4) "Electronic device" means a device that enables access to or use of a location information service or can otherwise create or provide location information.
(5) "Geofence" means a specified geographic area defined by a virtual perimeter or geographic coordinates.
(6) "Government entity" means:
(a) state or local agency, including but not limited to a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission, or an individual acting or purporting to act for or on behalf of a state or local agency.
(b) an individual or entity acting for or on behalf of an entity described in Subsection (7)(a).
(7) "Identifying information" means information tied to an electronic device that identifies the user's or owner's:
(a) name;
(b) address;
(c) phone number;
(d) email; or
(e) other information that would identify the owner or user of the electronic device.
(8) "Location information" means:
(a) information concerning the geographical location of an electronic device that, in whole or in part, is generated, derived from, or obtained by the operation of an electronic device or the operation of a software application on an electronic device.

(b) "Location information" includes past, current, and future location information.

(9) "Reverse-location information" means historical location information for:

(a) a defined time period;

(b) within a geographic area ; and

(c) affecting more than one number of electronic devices, for which the identities of the owners or users of the electronic devices are unknown to law enforcement.

Section 2. Obtaining reverse-location information within a geofence — Warrant required for disclosure — Procedure.

(1) Except as provided in Section 6, for a criminal investigation or prosecution, a law enforcement agency may not obtain reverse-location information for electronic devices within a geofence unless:

(a) the law enforcement agency obtains a search warrant as provided under this section; and

(b) (i) the investigation or prosecution involves:

(A) a violent felony;

(ii) the law enforcement agency can demonstrate an imminent, ongoing threat to public safety.

(2) To obtain reverse-location information inside of a geofence, a law enforcement agency shall:

(a) include with the sworn warrant application:

(i) a map or other visual depiction that represents the geofence for which the warrant is seeking information; and

(ii) the following language at the beginning of the application in a legible font no smaller than other text appearing in the application:

"NOTICE: This warrant application seeks judicial authorization for the disclosure of reverse-location information of electronic devices near a crime at or near the time of the crime. If authorized, the warrant allows law enforcement to obtain historical location information of all devices within the area described in the warrant during the specified time from entities in possession of the relevant data. The electronic devices captured in the warrant may be owned or used by both alleged criminal perpetrators and individuals not involved in the commission of a crime. For this reason, any warrant issued must require the anonymization of all devices associated with the reverse-location information."; and

(b) establish probable cause to believe that evidence of a crime will be found within the geofence and within a specified period of time.

(3) If a court grants a warrant under Subsection (2), the court shall require that all electronic device data provided pursuant to the warrant be anonymized before the reverse-location information is released to the law enforcement agency.

Section 3. Obtaining reverse-location information based on cell site records — Warrant required for disclosure — Procedure.

(1) Except as provided in Section 6, for a criminal investigation or prosecution, a law enforcement agency may not obtain reverse-location information based on cell site records unless:

(a) the law enforcement agency obtains a search warrant as provided under this section; and

(b) (i) the investigation or prosecution involves:

(A) a violent felony;

(ii) the law enforcement agency can demonstrate an imminent, ongoing threat to public safety.

(2) To obtain cell-site based reverse-location information, a law enforcement agency shall:

(a) include with the sworn warrant application:

(i) a visual depiction or written description that identifies:

(A) the crime scene location and any other areas of interest related to the crime;

(B) the location of cell sites from which the reverse-location information is sought; and

(C) the distance between the locations described in Subsections (2)(a)(i)(A) and (B); and

(ii) the following language at the beginning of the application in a legible font no smaller than other text appearing in the application:

"NOTICE: This warrant application seeks judicial authorization for the disclosure of reverse-location information of electronic devices near a crime at or near the time of the crime. If authorized, the warrant allows law enforcement to obtain historical location information of all devices within the area described in the warrant during the specified time from entities in possession of the relevant data. The electronic devices captured in the warrant may be owned or used by both alleged criminal perpetrators and individuals not involved in the commission of a crime. For this reason, any warrant issued must require the anonymization of all devices associated with the

reverse-location information."; and

(b) establish probable cause to believe that evidence of a crime will be found within the cell site records described in Subsection (2)(a)(i) and within a specified period of time.

(3) If a court grants a warrant under Subsection (2), the court shall require that all electronic device data provided pursuant to the warrant be anonymized before the reverse-location information is released to the law enforcement agency.

Section 4. Obtaining additional reverse-location information — Warrant required for disclosure — Procedure.

(1) If, after executing a warrant described in Section 2 or Section 3, a law enforcement agency seeks to obtain reverse-location information beyond the parameters of the warrant obtained under Section 2 or Section 3, the law enforcement agency shall:

(a) include in the sworn warrant application the specific electronic devices identified in the anonymized data for which the law enforcement agency seeks additional reverse-location information;

(b) establish probable cause to believe that evidence of a crime will be found within a specified period of time; and

(c) affirm that the crime described in Subsection (1)(b) is:

(i) the same crime or directly related to the crime that was the subject of the warrant obtained under Section 2 or Section 3; or

(ii) a crime subject to the judicially recognized plain view exception to the warrant requirement.

(2) If a court grants a warrant under Subsection (1), the court shall require that all electronic device data provided pursuant to the warrant be anonymized before the reverse-location information is released to the law enforcement agency.

Section 5. Obtaining identifying information connected to reverse-location information — Warrant required for disclosure — Procedure.

To obtain identifying information for an electronic device identified pursuant to a warrant obtained under Section 2, 3, or 4, a law enforcement agency shall establish in the sworn warrant application probable cause to believe that the electronic device was used or otherwise implicated in a crime.

Section 6. Exceptions to reverse-location warrant requirements.

(1) Notwithstanding any other provision in this chapter, a law enforcement agency may obtain reverse-location information without a warrant:

(a) in accordance with [INSERT RELEVANT STATE CODE]; or

(b) in accordance with a judicially recognized exception to warrant requirements.

(2) Nothing in this chapter:

(a) limits or affects the disclosure of public records under [INSERT RELEVANT STATE CODE];

(b) affects the rights of an employer under [INSERT RELEVANT STATE CODE] or an administrative rule adopted under [INSERT RELEVANT STATE CODE]; or

(c) limits the ability of a law enforcement agency to receive or use information, without a warrant or subpoena, from the National Center for Missing and Exploited Children under 18 U.S.C. Sec. 2258A.

Section 7. Use, disclosure, and destruction of reverse-location information — Anonymization.

(1) (a) A law enforcement agency may not use, copy, or disclose, for any purpose, reverse-location information obtained under a warrant under Section 2, 3, or 4, that:

(i) is not related to the crime that is the subject of the warrant; and

(ii) is collected as part of an effort to obtain the reverse-location information of an electronic device that is related to the crime that is the subject of the warrant obtained under Section 2, 3, or 4.

(b) The law enforcement agency shall destroy in an unrecoverable manner the reverse-location information described in Subsection (1)(a) as soon as reasonably possible after the criminal case is declined for prosecution or, if criminal charges are filed, the final disposition of the criminal case.

(2) (a) Reverse-location information obtained under Section 2, 3, or 4 may not be:

(i) compared with, merged with, linked to, or in any way electronically or otherwise connected to a source of electronic data, including a database or file, containing one or more points of data that includes the location information provided by an electronic device; or

(ii) used in any other criminal investigation or prosecution.

(b) Subsection (2)(a)(i) does not apply if all the electronic data, including the reverse-location information, is obtained for the purpose of investigating the same criminal incident.

(3) A person or entity that provides reverse-location information under this chapter shall ensure that the reverse-location information is anonymized before the reverse-location information is provided to a law enforcement agency.

Section 8. Notifications required — Exceptions — Delayed notification.

(1) (a) Except as provided in Subsection (1)(b) or (2), a law enforcement agency that executes a warrant under Section 5 shall serve a notice described in Subsection (3) on the owner of the electronic device for which identifying information was obtained:

(i) within 90 days after the day on which the identifying information is obtained by the law enforcement agency, but in no case more than three days after the day on which the investigation is concluded; or

(ii) if the owner of the electronic device for which the identifying information specified in the warrant is unknown to the law enforcement agency, within 90 days after the day on which the law enforcement agency identifies, or reasonably could identify, the owner.

(b) A law enforcement agency is not required to serve a notice described in Subsection (1)(a) to the owner of the electronic device for which identifying information was obtained if the owner resides outside of the United States.

(2) (a) (i) A law enforcement agency seeking a warrant in accordance with Section 5 may submit a request, and the court may grant permission, to delay service of the notice required under Subsection (1) for a period not to exceed 30 days, if the court determines that there is reasonable cause to believe that the notification may:

(A) endanger the life or physical safety of an individual;

(B) cause a person to flee from prosecution;

(C) lead to the destruction of or tampering with evidence;

(D) intimidate a potential witness; or

(E) otherwise seriously jeopardize an investigation or unduly delay a trial.

(ii) When a delay of notification is granted under Subsection (2)(a)(i) and upon application by the law enforcement agency, the court may grant additional extensions of up to 30 days each.

(b) (i) A law enforcement agency that seeks a warrant in accordance with Section 5 may submit a request to the court, and the court may grant permission, to delay service of the notice required under Subsection (1), if the purpose of delaying the notification is to apprehend an individual:

(A) who is a fugitive from justice under [INSERT RELEVANT STATE CODE]; and

(B) for whom an arrest warrant has been issued for a violent felony offense as defined in [INSERT RELEVANT STATE CODE].

(ii) (A) The court may grant the request under Subsection (2)(b)(i) to delay notification until the individual who is a fugitive from justice under [INSERT RELEVANT STATE CODE] is apprehended by the law enforcement agency.

(B) A law enforcement agency shall service the notice required under Subsection (1) to the owner of the electronic device within 14 days after the day on which the law enforcement agency apprehends the individual described in Subsection (2)(b)(i).

(3) A notice required under Subsection (1) shall include:

(a) a copy of the warrant; and

(b) a written statement identifying:

(i) the offense specified in the warrant application;

(ii) the identity of the law enforcement agency that filed the application;

(iii) the date on which the location information or identifying information was obtained; and

(iv) the number and length of any authorized delays in serving the notice required under Subsection (1), including, if applicable, the name of the court that authorized the delay and a reference to the provision of this chapter that permitted the delay.

(4) A law enforcement agency shall serve the notice required under Subsection (1) to the owner of the electronic device by:

(a) personal service on the owner;

(b) first-class mail to the owner's last-known address; or

(c) other reasonable means if the owner's last-known address is unknown.

Section 9. Exclusion of records.

Reverse-location information or identifying information obtained in violation of the provisions of this chapter shall be subject to the rules governing exclusion as if the records were obtained in violation of the Fourth Amendment to the United States Constitution and [INSERT RELEVANT STATE CONSTITUTIONAL CODE].

Section 10. Reporting requirements for reverse-location warrants.

(1) As used in this section:

(a) "Anonymized" means the same as that term is defined in Section 1.

(b) "Committee" means [INSERT RELEVANT STATE CRIMINAL JUSTICE OR LAW ENFORCEMENT LEGISLATIVE COMMITTEE]

(c) "Electronic device" means the same as that term is defined in Section 1.

(d) "Government entity" means a state or local agency, including but not limited to a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission, or an individual acting or purporting to act for or on behalf of a state or local agency.

(e) "Law enforcement agency" means the same as that term is defined in Section 1.

(f) "Reverse-location information" means the same as that term is defined in Section 1.

(g) "Reverse-location warrant" means a warrant seeking reverse-location information under Section 2, 3, or 4.

(2) (a) Beginning January 1, 2024, a law enforcement agency or any government entity that obtained a reverse-location warrant shall annually on or before April 30 submit a report to the committee with the following data for the previous calendar year:

(i) the number of reverse-location warrants requested by the law enforcement agency under Section 2, 3, or 4;

(ii) the number of reverse-location warrants that a court or magistrate granted after a request described in Subsection (2)(a)(i);
(iii) the number of investigations that used information obtained under a reverse-location warrant to investigate a crime that was not the subject of the reverse-location warrant;
(iv) the number of times reverse-location information was obtained under an exception listed in Section 6;
(v) the warrant identification number for each warrant described under Subsection (2)(a)(ii) or (iii); and
(vi) the number of electronic devices for which anonymized electronic device data was obtained under each reverse-location warrant described under Subsection (2)(a)(ii).

(b) A law enforcement agency shall compile the report described in Subsection (2)(a) for each year in the standardized format developed by the committee under Subsection (4).

(3) If a reverse-location warrant is requested by a multijurisdictional team of law enforcement officers, the reporting requirement in this section is the responsibility of the commanding agency or governing authority of the multijurisdictional team.

(4) The committee shall:

(a) develop a standardized format for reporting the data described in Subsection (2);
(b) compile the data submitted under Subsection (2); and
(c) annually on or before August 1, make publicly available a report of the data described in Subsection (2).

Section 11. State Grant Requirements.

Beginning July 1, 2023, the [INSERT RELEVANT STATE AGENCY] may not award any grant of state funds to any entity subject to, and not in compliance with, the reporting requirements in [INSERT RELEVANT STATE CODE THAT ADDRESSES GRANTS TO LAW ENFORCEMENT AGENCIES].

To learn more about this model language, please contact David Iglesias at david@libertas.org