**Locating Wireless Devices FAQs**

**Q1:     How can the government obtain location information for wireless devices?**

There are two principal ways for the government to obtain location information about cellular phones and other wireless devices:  (1) through compelled or voluntary disclosures from the wireless provider for that device (e.g., Verizon or AT&T), and (2) through use of specialized equipment by law enforcement.

**Q2:     What location information is available from a wireless provider?**

Wireless providers typically have access to two types of location information for their subscribers’ wireless devices:  (1) cell-site data, and (2) latitude-longitude data.

*Cell-site data* (also known as “tower/face information” or “cell tower/sector records”) identifies the antenna tower and, in some cases, the 120-degree face of the tower to which a wireless device is connected at the beginning and end of each call or communication.  These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas.  Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device.  Accordingly, at best, cell-site data reveals the neighborhood in which a wireless user is located at the time a call starts and ends; it does not provide continuous tracking and is not a virtual map of the wireless user’s movements.  Despite its relative lack of precision, cell-site information is an important investigative tool that can help law enforcement establish physical surveillance and locate kidnapping victims, fugitives, and targets of criminal investigations.

*Latitude-longitude data* (sometimes referred to as “E-911 data” or “GPS data”) provides relatively precise location information about the wireless device itself, either via GPS tracking technology built into the wireless device itself or by triangulating on the device’s signal using data from several of the provider’s cell towers.  Only some providers are capable of providing latitude-longitude data at all; most of those providers do not retrieve or store this kind of data in the normal course of business but must instead undertake additional steps to generate the data in response to a law enforcement request.

Upon being served with the appropriate legal process, a wireless provider should be able to provide prospective cell-site data and may be able to provide latitude-longitude location information about a particular wireless device’s current location, as long as the wireless device is turned on.  Some providers also store historical cell-site information, although currently they are unlikely to have historical latitude-longitude data.

In certain cases, a wireless provider may be able to provide information about all wireless devices that were connecting to a particular cell tower at a particular time.  If this type of information would be useful to your investigation, please contact CCIPS at (202) 514-1026 for the latest guidance and go-bys.

**Q3:     In an emergency, how can law enforcement obtain location information quickly from a wireless provider?**

In an emergency situation (such as a kidnapping or rescuing a lost hiker), law enforcement may be able to request and accept voluntary disclosures of location information from a wireless provider pursuant to 18 U.S.C. § 2702.  In particular, law enforcement should consider requesting voluntary disclosure from the provider pursuant to 18 U.S.C. § 2702(c)(4) by explaining to the provider that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.  Law enforcement also should consider whether the provider could voluntarily disclose the information pursuant to 18 U.S.C. § 2702(c)(2) based on a consent theory.  In particular, some wireless providers require subscribers to agree to terms of service that allow the provider to disclose information about the account where the provider reasonably believes that disclosure is necessary to prevent, for example, loss of life or bodily harm.  If the service provider for the target wireless device has an applicable provision in its terms of service, law enforcement may seek disclosure of location information for the target wireless device.

If there is no basis for voluntary disclosure, or if the provider has refused to disclose information voluntarily, law enforcement should instead compel disclosure of the information by serving the provider with appropriate legal process, as described in more detail below.  Law enforcement may also be able to obtain prospective cell-site data by complying with the emergency disclosure procedures of 18 U.S.C. § 3125 (and thereby committing to obtain a hybrid cell-site order within 48 hours).

**Q4:     What legal process is required to compel historical cell-site data from a wireless provider?**

Because cell-site records constitute a “record or other information pertaining to a subscriber” under 18 U.S.C. § 2703(c)(1), the government may use either a 2703(d) court order or a search warrant to obtain historical cell-site information from a wireless provider.

**Q5:     What legal process is required to compel prospective cell-site data from a wireless provider?**

In many districts, investigators may obtain prospective cell-site data from a wireless provider by using a “hybrid” application and order that satisfies the requirements of both the Pen/Trap statute and 18 U.S.C. § 2703(d).  The hybrid application should contain: (i) a government attorney’s affirmation “that the information likely to be obtained is relevant to an ongoing criminal investigation,” as required by the Pen/Trap statute, and (ii) a further demonstration by the government attorney of “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation,” as required by 18 U.S.C. § 2703(d).  Hybrid orders otherwise generally follow the procedures for pen/trap orders.

District courts and magistrate judges have split on whether hybrid orders may be used to compel disclosure of prospective cell-site information.  Courts that have rejected hybrid orders for prospective cell-site information have generally required the government to obtain a warrant to compel its disclosure.  The following table lists the most recent published (or electronically available unpublished) decisions from magistrate and district court judges about the type of legal process needed to obtain cell-site location information.  (Although this chart suggests that hybrid orders are disfavored, judges accept hybrid orders as a matter of course in many of the districts not listed on this chart.)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Circuit** | **District** | **Legal Process Required** | **Most Recent Case** | **Type of Judge** |
| 1st Cir. | D. Mass.  | Search warrant | 530 F. Supp. 2d 367 (11/6/07) | Magistrate |
| D.P.R.  | Search warrant | 497 F. Supp. 2d 301 (7/18/07) | Magistrate |
| 2d Cir. | E.D.N.Y.  | Hybrid order | 2008 WL 5082506 (11/26/08) | District Court |
| S.D.N.Y.  | Hybrid order  | 460 F. Supp. 2d 448 (10/23/06) | District Court (Kaplan, J.) |
| Search warrant  | 2009 WL 159187 (1/13/09) | District Court (McMahon, J.) |
| W.D.N.Y.  | Search warrant | 415 F. Supp. 2d 211 (2/15/06) | Magistrate |
| 3d Cir. | W.D. Pa.  | Search warrant (in dicta only) | 534 F. Supp. 2d 585 (2/19/08) | Magistrate (aff’d by District Court) |
| 4th Cir. | D. Md.  | Search warrant | 439 F. Supp. 2d 456 (7/24/06) | Magistrate |
| S.D.W.V.  | Hybrid order (nonsubscriber only) | 415 F. Supp. 2d 663 (2/17/06) | Magistrate |
| 5th Cir. | W.D. La.  | Hybrid order | 411 F. Supp. 2d 678 (1/26/06) | Magistrate |
| S.D. Tex.  | Hybrid order  | 2007 WL 3036849 (10/17/07) | District Court |
| W.D. Tex. | Search warrant | 727 F. Supp. 2d 571 (7/29/10) | Magistrate. |
| 7th Cir. | N.D. Ind.  | Search warrant | 2006 WL 1876847 (7/5/06) | District Court |
| S.D. Ind.  | Search warrant | 2006 WL 3197181 (6/30/06) | District Court |
| E.D. Wis.  | Search warrant | 2006 WL 2871743 (10/6/06) | District Court |
| 9th Cir. | E.D. Cal.  | Hybrid order  | 2007 WL 397129 (2/1/07) | Magistrate |
| D.C. Cir. | D.D.C.  | Search warrant | 407 F. Supp. 2d 134 (1/6/06) | Magistrate |

Because this area of the law is developing rapidly, prosecutors or agents may have questions about current trends in different districts, and they should direct any such questions to CCIPS (202-514-1026) or their local CHIP.

**Q6:     What legal process is required to compel prospective latitude-longitude data from a wireless provider?**

A search warrant is typically required to compel prospective latitude-longitude data from a wireless provider, both because the provider may need get the information from the wireless device itself and because the government may be obtaining information about the user’s movements in a private space.  In rare cases, a wireless user or subscriber may have voluntarily disclosed latitude-longitude data about the device to the provider; please contact CCIPS at 202-514-1026 for the latest guidance about this type of situation.

**Q7:     How can law enforcement use its own equipment to obtain location information for a particular wireless device?**

A number of investigative agencies have access to specialized equipment, such as directional antennae, that can be used to obtain location information about a particular wireless device, unbeknownst to the device’s user and without the involvement of the wireless provider.  Such equipment may be used to locate, among other things, cell phones, computers that are accessing open wireless networks, and PC wireless data cards.

In order to use this type of equipment, law enforcement needs to obtain the appropriate legal process.  A search warrant will always be sufficient to authorize the use of this equipment, but other types of legal process may also be available in some situations.  For additional guidance about the types of legal process that are available in a specific case, please contact CCIPS at 202-514-1026.

In certain cases, the equipment described above can also be used to collect identifying information about the mobile device, such as its electronic serial number (ESN).  For more information about the authorization required to use the equipment for this purpose, please contact CCIPS at 202-514-1026 for the latest guidance and go-bys.

**Q8.     Must a search warrant for location information be issued in the district where the wireless device is located?**

A search warrant for location information can either be sought under a traditional Rule 41 theory or pursuant to 18 U.S.C. § 2703(c)(1)(A).  Warrants issued pursuant to Rule 41 alone can be used to collect location evidence prospectively, but courts may issue such warrants only for property located in the district when the warrant is issued (except in terrorism investigations).  Accordingly, an application for a search warrant based solely on the authority of Rule 41 should include some showing that the wireless device is currently located in the judicial district.  However, a warrant issued under 18 U.S.C. § 2703(c)(1)(A) may be issued by any court “with jurisdiction over the offense under investigation.”  Thus far, CCIPS is aware of a few magistrates who have rejected the idea that a warrant issued under 18 U.S.C. § 2703(c)(1)(A) can be used to obtain prospective location information.  If a magistrate does object to such a use of a § 2703 warrant, it would be necessary to rely solely on Rule 41.

**Q9.     Who is entitled to notice of a warrant for location information, and can that notice be delayed?**

Because a court could find that the Fourth Amendment requires it, it is prudent to follow Rule 41 notice procedures when seeking prospective latitude-longitude information pursuant to a warrant.  The best practice is to give notice of the warrant to the person(s) who actually used the target phone, if possible, and not merely to the registered owner (if different).  This notice can be delayed pursuant to the delayed notice provisions of 18 U.S.C. § 3101a(b)(3) and Rule 41(f)(3).

**Q10.   How can law enforcement compel a provider to disclose latitude-longitude information from the car navigation device (e.g., an OnStar device) of its customer?**

In general, latitude-longitude information for car navigation systems is stored in the target automobile, rather than with the service provider.  Nonetheless, the service provider should be able to access the location data in the car’s computer remotely and therefore can provide it to law enforcement in response to the appropriate process.  Because this data is probably protected by the Fourth Amendment, law enforcement should get a warrant to obtain this information, unless an exception to the warrant requirement applies.  In addition, because navigation devices often use wireless technology to communicate with the navigational service provider (e.g., OnStar), cell-site information for a particular navigational device may be available from the company that provides wireless service to the device.  (Please note that the wireless service provider for the device will often be a different company than the navigational service provider.)

**Q11.   When a wireless device might be located outside of the United States, may U.S. law enforcement still obtain location information about that device from a U.S. wireless provider?**

It is fine for U.S. law enforcement to seek cell-site location information from a U.S. provider for a wireless device that may be located out of the country because providers collect and store cell-site data in the ordinary course of business, regardless of where the device is located.  However, if U.S. law enforcement is seeking latitude-longitude information and has a reasonable basis for believing that the target device is located in another country, U.S. law enforcement should follow these steps to ensure that it does not intrude on the sovereignty of the foreign nation:

1. Serve the wireless provider for the device with appropriate legal process to obtain either historical or prospective cell-site data.

1. Upon receiving the cell-site data, determine the location of the cellular tower to which the wireless device most recently connected.

* 1. If the tower is located in the United States, law enforcement may proceed with a warrant for the latitude-longitude information.

* 1. If the tower is located in another country, it will be necessary to coordinate with that nation to get latitude-longitude information.  For further guidance on this type of international coordination, contact the Office of International Affairs at (202) 514-0000.

In general, it is always good practice to coordinate with the Office of International Affairs (202-514-0000) whenever an investigation might involve location information for a wireless device located in another country.

**Q12.   When obtaining location information for wireless devices, is it necessary to comply with the laws governing tracking devices?**

Both 18 U.S.C. § 3117 and Rule 41 include provisions that govern the use of “tracking devices,” which are defined as electronic or mechanical devices that permit the tracking of the movement of a person or object.  *See* 18 U.S.C. § 3117(b).  The Department of Justice believes that cell phones and other wireless devices that are knowingly possessed by a user should not be considered “tracking devices” within the meaning of this definition.  However, because a reviewing court may later conclude that a user’s own phone falls within the definition, the officer who executes a search warrant for location information should consider complying with Rule 41(f)(2)(A) as a precaution.  To do so, the officer should enter the exact date and time when the location-finding activity commenced, and for what period, on the warrant return.  Please note that, although Rule 41(f)(2) sets forth procedures that should be followed for tracking-device warrants, 18 U.S.C. § 3117 does not require that a warrant be used for the installation and use of a tracking device.

***Information obtained from*** [***http://dojnet.doj.gov/criminal/ccips/online/location.htm***](http://dojnet.doj.gov/criminal/ccips/online/location.htm)