CALL DETAIL & CELL SITE EVIDENCE

Cellular phones operate as a two-way radio that transmits and receives signals when the user is in the range of the devices service provider's antennas. The antennas may be on a tower, building or other structure and are referred to as a cell site. A cellular service provider maintains a cellular network of cell sites which may or may not overlap with other cell sites. A cell site may contain one or more antennas. If the user is moving, the device has the ability to switch to other cells in the network as long as they are in range of a cell site that is operational and can handle the network traffic.

Call Detail Records

Cellular service providers maintain records of a user's calls, text messaging, data usage as well as the dates and times and cell sites used by those communications. These records were intended for customer billing purposes and to help to optimize the design of the service provider's cellular network. As the use of mobile devices has increased, so has the use of these records for establishing a user's location during a particular time, such as placing a person at the scene of a crime. But the practice is coming under attack in courts nationwide, challenging an established practice by law enforcement that has lead to thousands of convictions. The use of historical cell site location data is different than the real-time triangulation of three cell towers to locate a phone or GPS technology using satellites. The accuracy of triangulation or GPS data is not in dispute, but phone companies do not routinely collect or save that data for an individual phone. Also, accuracy of the call and text message logs is not being questioned.

The accuracy of triangulation or GPS data is not in dispute, but phone companies do not routinely collect or save that data for an individual phone.

Cell Site Analysis

Cell Site Analysis is the science of reconstructing the physical movements of a mobile telephone or device and establishing the historical geographical location of a phone when calls, text messages or downloads are sent or received, using the data from mobile phone service providers. Cell Site Analysis is derived from historical data and is often based on many assumptions. However the evidence produced from such advanced investigations can be especially powerful in attributing contact between individuals, establishing the proximity to a scene of crime, identifying patterns of movement of suspects and testing the strength of alibi evidence. Evidence from Cell Site Analysis can be combined with other evidence such as CCTV or call data records to determine if the accused was in fact at the scene of the crime or to confirm an alibi.

Non Digital Evidence

- Subscriber Account Information
- Cell Site Information
- Call Detail Records (CDR's)
  - Retention varies by provider

Subscriber Account Information

Prior to using call detail records, the use and ownership of a device must be established. A user may have a service contact with a provider which will document personal demographic information used for the services and billing purposes. This subscriber information may include:

1. Name
2. Address
3. DOB
4. Other telephone contact information such as work/home phone
5. E-mail address(es)
6. Device make/model/serial number and network identification information

Although this information may be useful to identify the party registered as the owner, there is still the possibility that someone other than the device's owner may have used the device at any given time.

Pre-Paid Phones

Cellular phones may be sold with no user contract and without a subscriber account. A pre-paid device is sold by a retailer and the user pre-pays for the cellular and data usage. The use of pre-paid phones requires additional evidence to establish the use and ownership of a device. However, there is still a viable defense that someone other than the phone's owner used the phone. Therefore, the identity of the user of a pre-paid device may create additional challenges in the admissibility of cell site records under Federal Rules of Evidence. Specifically, Rule 104(b) provides that "[w]hen the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition." The offering party must first prove that the person possessed the cell phone to use the location data from that phone to establish the location of a person.

There is still a viable defense that someone other than the phone's owner was in possession or used the phone.

Call Detail Records (CDR)

Call detail records are the billing records cellular service providers use to keep track of their customers' calls and cellular data usage. They show the date and time of all calls made or received, the numbers called, the duration of each call and the cell sites used to begin and end a call. When a user traveling, the device may use many cell sites during the call but only the first and last cell site used by the call is maintained. When a mobile device user places or receives a call, that call will typically connect to a cell site to make the call. Two exceptions are:

1. When a call is placed to a mobile device that is turned off or out of range of the network, the call is routed to voicemail and no cell-site is used.
2. When a user uses a third-party application to communicate via voice or messaging over a Wi-Fi network.

Sending or receiving text messages or using phone data will also utilize cell sites for the connection, although a user can set the device to use Wi-Fi for these communications when in range of a Wi-Fi network to which they have access.

If a forensic examination of a device had been conducted, the service provider call detail records can be used to validate the findings of that examination by comparing items such as call logs and text message dates, times and party information. The CDR may also provide information of data that had been deleted and not recovered by the forensic process because it had been overwritten.

Call Detail Retention

Currently in the U.S. there are five major cellular service providers, although some of them operate under different names. For example, Boost Mobile is part of Sprint Corporation. Other companies lease access and resell devices from one or more of the five major providers and are

known as mobile virtual network operators. IRIS LLC has obtained the latest data retention information for common data types for the five providers and compiled the information in the IRIS LLC Cellular Service Provider Retention Schedule 6-22-18 available in the Digital Evidence Toolbox/Retention Schedule-Sample Letters section.

I.R.I.S. LLC
Information Retrieval Investigative Services
For more Information, visit:
www.irisinvestigations.com
(860) 522-0001

Currently there are five major cellular providers operating in the United States. For a listing of subsidiaries and partners, see: https://en.wikipedia.org/wiki/List_of_United_States_mobile_virtual_network_operators

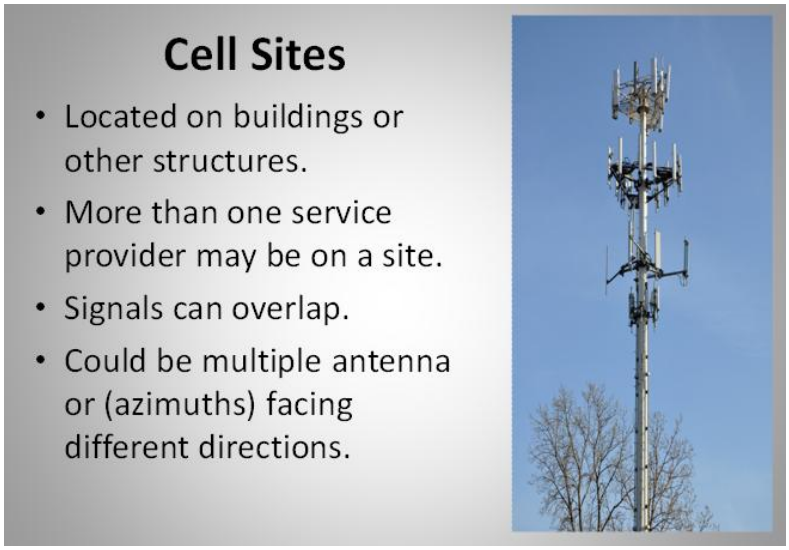
	Verizon	AT&T	Sprint (Boost/Virgin)	T-Mobile (Metro PCS)	US Cellular
Subscriber Information	7-10 years	7 years	Unlimited	3-5 years	7 years
Call Detail Records	1 rolling calendar year	7 years	18 months	2 years	1 year
Cell Towers Used by Phone for Calls	1 rolling calendar year	7 years	18 months	1 year	1 year
Tower Dumps	1 rolling calendar year	7 years	18 months	180 days	1 rolling calendar year
Range to Tower (RTT) Data	7 days	180 days	14 days(SMS) 90 days(Calls)	90 days	Not available
Text Message (SMS) Records	1 rolling calendar year	7 years	18 months	2 years	1 year
Text Message (SMS) Content	3-5 days	Not available	Not retained	Not retained	3-5 days
Cell Towers used for SMS Transmission	Not retained	1 year	Varies	180 days	Not retained
Pictures (MMS)	Not retained	Not retained	Not retained	Not retained	Not retained
IP Session Information	1 rolling calendar year	1 year	90 days	Not retained	1 year
IP Source & Destination Information	11 months	1 year	90 days	Not retained	Not available
Bill Copies (post-paid only)	Indefinitely, but depends on account	7 years	Indefinitely, but depends on account	2 years	7 years
Payment History (post-paid only)	Indefinitely, but depends on account	7 years	Indefinitely, but depends on account	5 years	1 year

IRIS LLC
DIGITAL EVIDENCE TOOLBOX: Cellular Service Provider Retention Schedule
Version 2 June 22, 2018

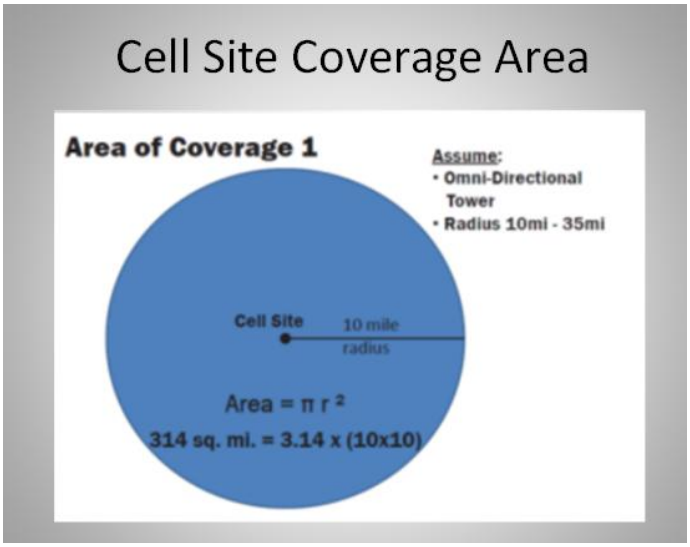
Letter of Preservation

The retention period may be extended by providing the service provider with a Letter of Preservation. A sample letter of preservation is available in the Digital Evidence Toolbox/Retention Schedule-Sample Letters section.

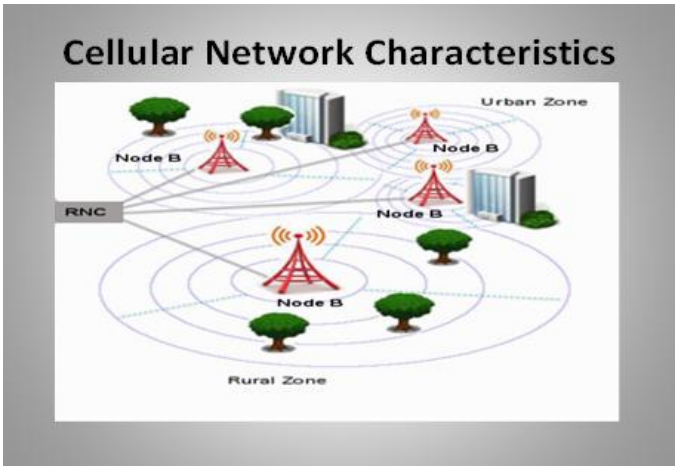
Cell Network Characteristics



Cell sites are often referred to as cell towers but they may be located on a building, water tower or other structure. A cell site may contain one antenna (Omni-directional) that covers a full 360° area. Most cell sites will contain either three antennas if on a tower, with each antenna covering a 120° area, or four antennas covering a 90° area if the site is located on a building. This coverage area is referred to as a sector. Cell site antennas have various ranges. In an urban area where usage is higher, cell sites typically will have a shorter range and the sites will be located closer together and with a larger overlap in coverage. Cell antennas may have a range of less than one mile or up to thirty miles or more.



An omni-directional site with a ten mile range could cover approximately 314 square miles. A cell site with a range of 30 miles could have a total coverage area of approximately 2,700 square miles.

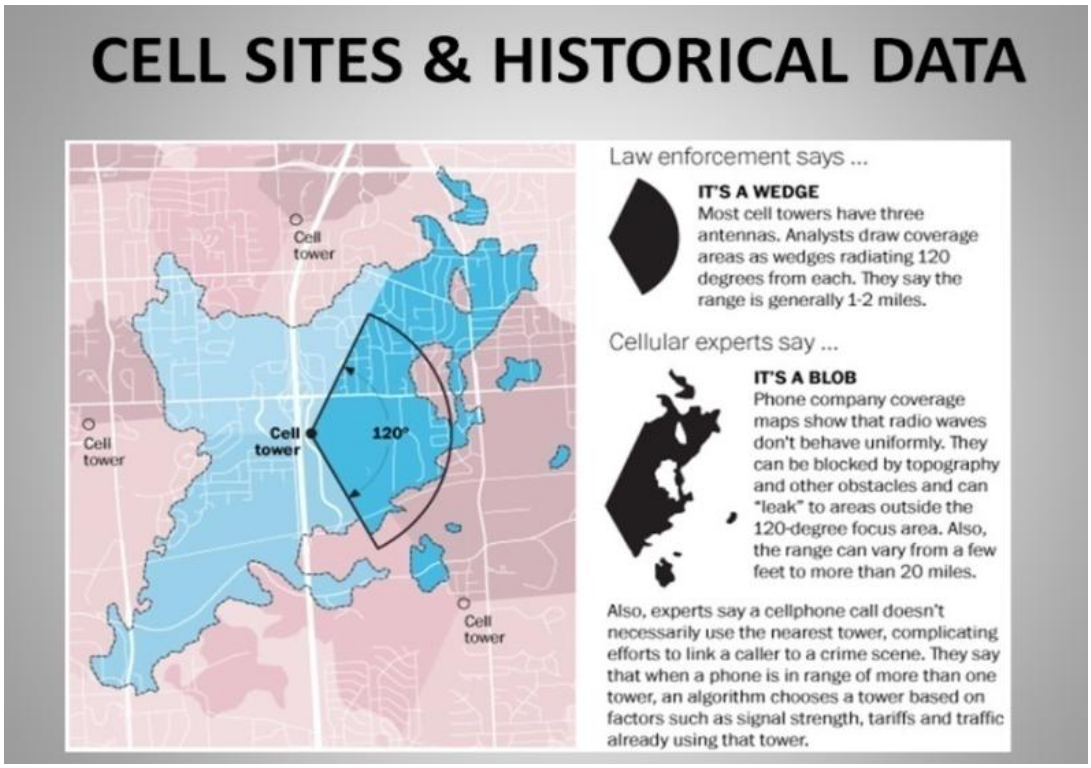


When a user places a call, the cell phone connects to a cell site. Adjoining cells provide some overlap in coverage to avoid disconnection from the network when the signal strength of the site servicing the call drops by transferring the call to the next *available* cell with the strongest signal. This primary feature of the cellular design provides that one cell site will pick up a call and ensure it goes through when another goes down. This process is known as a "hand-off." A hand-off may occur because the signal of the first cell weakens, as the user moves away from the site, and then subsequently strengthens after recognizing a closer cell. Thus, handing-off will occur as a cell phone user moves throughout multiple coverage areas. However, the geographic location of the user is not the only reason for a call switching cells, since many other factors may affect the signal strength between a cell phone and site.

Handing-off will occur as a cell phone user moves throughout multiple coverage areas.

Other Factors

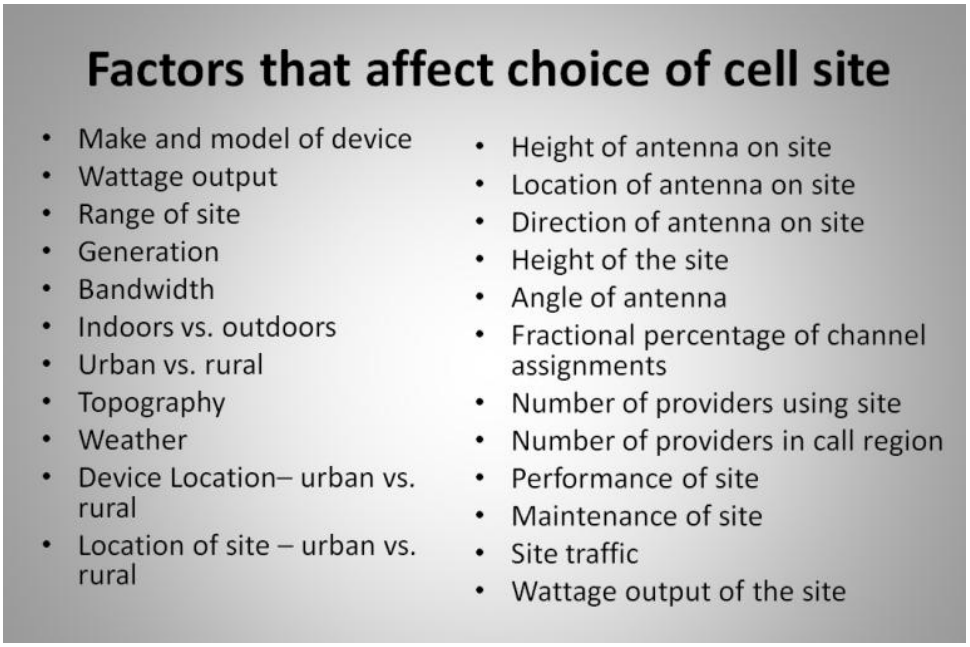
Cell sites are typically identified as circles with wedge shaped sectors on a two-dimensional map. But the radio signals can be blocked by man-made or natural obstacles and the coverage is not uniform. Cell phone experts may offer propagation maps which better depict the coverage at a specific time, but will not necessarily represent the actual coverage at the time in question.



The cell site used is not always the closest cell site. Service provider's call detail records can only narrow location to the geographic coverage area of the originating and terminating cell sites, rather than pinpoint the specific location. It cannot be determined that the cell phone was closest to the site processing the call because factors other than geographic location can affect signal strength. A better theory on which to offer historical cell site data is not to prove where the phone user was at a specific time, but to prove where he or she could not have been.

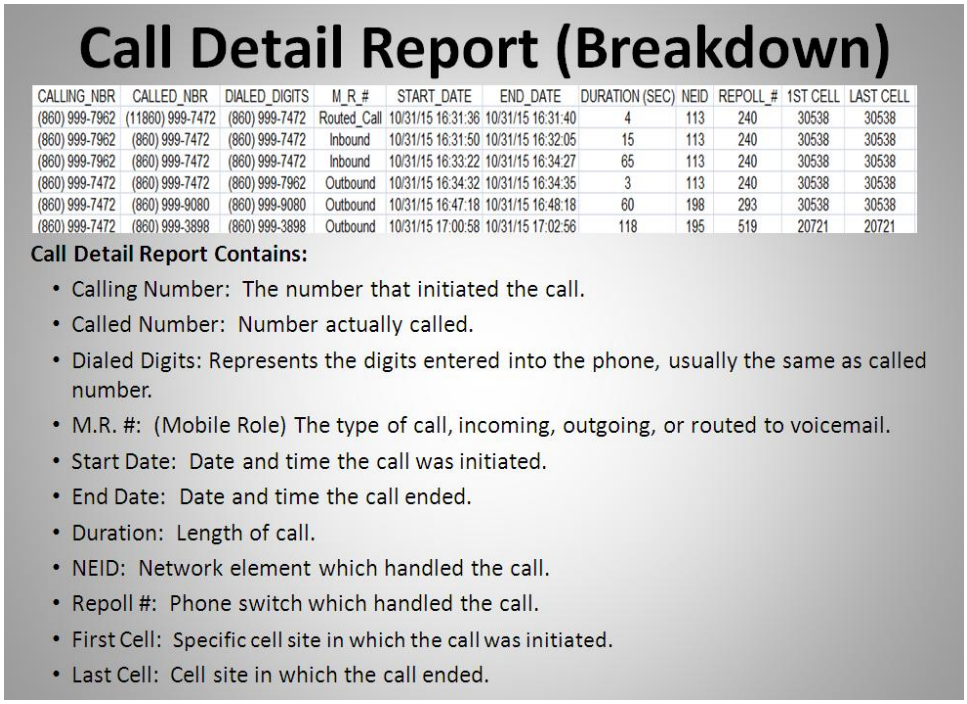
A better theory is not to prove where the phone user was at a specific time, but to prove where it could not have been.

The geographic location of the user is not the only reason a cell site is used by the device. First, the technical characteristics of cell sites may affect signal strength, such as the number of sites available, the maintenance or repairs being performed, the height of the cell tower, the height above sea level, the wattage output and range of coverage. Second, technical characteristics of the antennas on cellular sites may affect signal strength, such as the number of antennas, the angle and direction the antenna is facing, height of each antenna and call traffic at any given time period. Third, the characteristics of the phone, such as the wattage output and generation of the phone's broadband capability, may affect signal strength. Fourth, signal strength may be influenced by environmental conditions such as weather and foliage as well as geographical factors and obstacles such as buildings.



Interpreting Call Detail Reports

Cellular service providers CDR's provide the same information with different formatting. The following example uses a Sprint sample report.



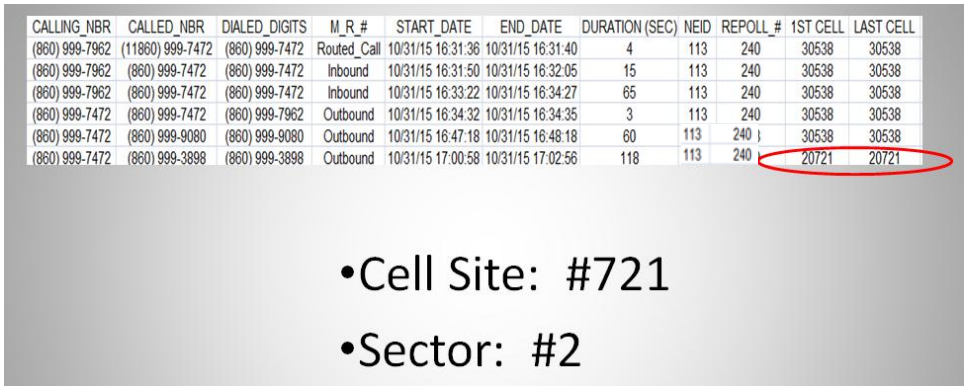
Call Detail Report (Breakdown)

CALLING_NBR	CALLED_NBR	DIALED_DIGITS	M_R_#	START_DATE	END_DATE	DURATION (SEC)	NEID	REPOLL_#	1ST CELL	LAST CELL
(860) 999-7962	(11860) 999-7472	(860) 999-7472	Routed_Call	10/31/15 16:31:36	10/31/15 16:31:40	4	113	240	30538	30538
(860) 999-7962	(860) 999-7472	(860) 999-7472	Inbound	10/31/15 16:31:50	10/31/15 16:32:05	15	113	240	30538	30538
(860) 999-7962	(860) 999-7472	(860) 999-7472	Inbound	10/31/15 16:33:22	10/31/15 16:34:27	65	113	240	30538	30538
(860) 999-7472	(860) 999-7472	(860) 999-7962	Outbound	10/31/15 16:34:32	10/31/15 16:34:35	3	113	240	30538	30538
(860) 999-7472	(860) 999-9080	(860) 999-9080	Outbound	10/31/15 16:47:18	10/31/15 16:48:18	60	198	293	30538	30538
(860) 999-7472	(860) 999-3898	(860) 999-3898	Outbound	10/31/15 17:00:58	10/31/15 17:02:56	118	195	519	20721	20721

Call Detail Report Contains:

- Calling Number: The number that initiated the call.
- Called Number: Number actually called.
- Dialed Digits: Represents the digits entered into the phone, usually the same as called number.
- M.R. #: (Mobile Role) The type of call, incoming, outgoing, or routed to voicemail.
- Start Date: Date and time the call was initiated.
- End Date: Date and time the call ended.
- Duration: Length of call.
- NEID: Network element which handled the call.
- Repoll #: Phone switch which handled the call.
- First Cell: Specific cell site in which the call was initiated.
- Last Cell: Cell site in which the call ended.

On the above Sprint sample, the first cell and last cell are listed with a numeric value identifying the cell site and sector information. Sprint provides a separate document which further identifies the cell site locations. If a device was active on more than one network, there may be multiple cell site location reports. Other providers may have the latitude, longitude and/or the approximate street address on the CDR.



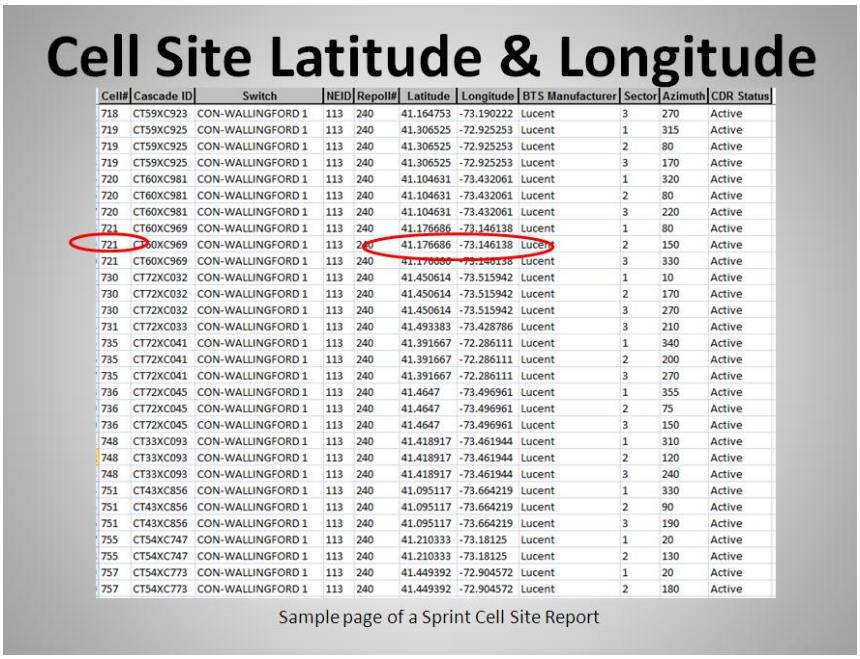
CALLING_NBR	CALLED_NBR	DIALED_DIGITS	M_R_#	START_DATE	END_DATE	DURATION (SEC)	NEID	REPOLL_#	1ST CELL	LAST CELL
(860) 999-7962	(11860) 999-7472	(860) 999-7472	Routed_Call	10/31/15 16:31:36	10/31/15 16:31:40	4	113	240	30538	30538
(860) 999-7962	(860) 999-7472	(860) 999-7472	Inbound	10/31/15 16:31:50	10/31/15 16:32:05	15	113	240	30538	30538
(860) 999-7962	(860) 999-7472	(860) 999-7472	Inbound	10/31/15 16:33:22	10/31/15 16:34:27	65	113	240	30538	30538
(860) 999-7472	(860) 999-7472	(860) 999-7962	Outbound	10/31/15 16:34:32	10/31/15 16:34:35	3	113	240	30538	30538
(860) 999-7472	(860) 999-9080	(860) 999-9080	Outbound	10/31/15 16:47:18	10/31/15 16:48:18	60	113	240	30538	30538
(860) 999-7472	(860) 999-3898	(860) 999-3898	Outbound	10/31/15 17:00:58	10/31/15 17:02:56	118	113	240	20721	20721

•Cell Site: #721

•Sector: #2

For the outbound call made on 10/31/15 at 17:00:58, the first and last cell site used was 20721:

The first number of the site is the sector used and the remainder is the cell-site identifier. That call used sector 2 of site 721 of the NEID (Wallingford, CT) as follows:



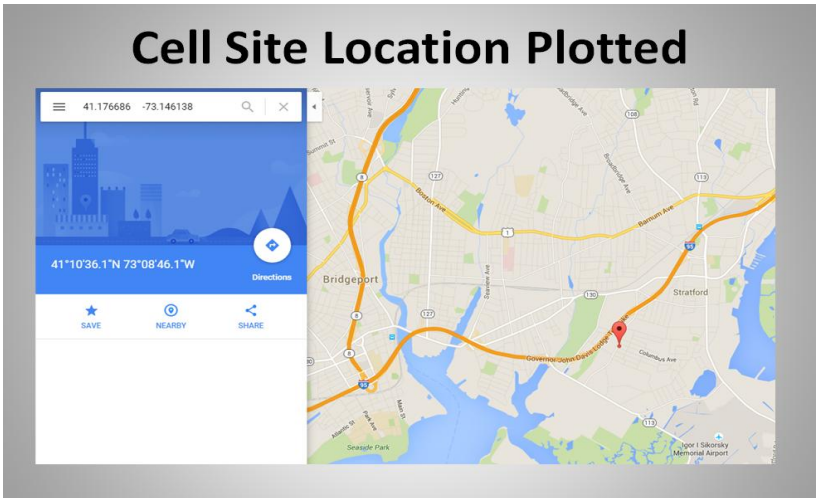
Cell#	Cascade ID	Switch	NEID	Repoll#	Latitude	Longitude	BTS Manufacturer	Sector	Azimuth	CDR Status
718	CT59XC923	CON-WALLINGFORD 1	113	240	41.164753	-73.190222	Lucent	3	270	Active
719	CT59XC925	CON-WALLINGFORD 1	113	240	41.306525	-72.925253	Lucent	1	315	Active
719	CT59XC925	CON-WALLINGFORD 1	113	240	41.306525	-72.925253	Lucent	2	80	Active
719	CT59XC925	CON-WALLINGFORD 1	113	240	41.306525	-72.925253	Lucent	3	170	Active
720	CT60XC981	CON-WALLINGFORD 1	113	240	41.104631	-73.432061	Lucent	1	320	Active
720	CT60XC981	CON-WALLINGFORD 1	113	240	41.104631	-73.432061	Lucent	2	80	Active
720	CT60XC981	CON-WALLINGFORD 1	113	240	41.104631	-73.432061	Lucent	3	220	Active
721	CT60XC969	CON-WALLINGFORD 1	113	240	41.176686	-73.146138	Lucent	1	80	Active
721	CT60XC969	CON-WALLINGFORD 1	113	240	41.176686	-73.146138	Lucent	2	150	Active
721	CT60XC969	CON-WALLINGFORD 1	113	240	[illegible]	[illegible]	Lucent	3	330	Active
730	CT72XC032	CON-WALLINGFORD 1	113	240	41.450614	-73.515942	Lucent	1	10	Active
730	CT72XC032	CON-WALLINGFORD 1	113	240	41.450614	-73.515942	Lucent	2	170	Active
730	CT72XC032	CON-WALLINGFORD 1	113	240	41.450614	-73.515942	Lucent	3	270	Active
731	CT72XC033	CON-WALLINGFORD 1	113	240	41.493383	-73.428786	Lucent	3	210	Active
735	CT72XC041	CON-WALLINGFORD 1	113	240	41.391667	-72.286111	Lucent	1	340	Active
735	CT72XC041	CON-WALLINGFORD 1	113	240	41.391667	-72.286111	Lucent	2	200	Active
735	CT72XC041	CON-WALLINGFORD 1	113	240	41.391667	-72.286111	Lucent	3	270	Active
736	CT72XC045	CON-WALLINGFORD 1	113	240	41.4647	-73.496961	Lucent	1	355	Active
736	CT72XC045	CON-WALLINGFORD 1	113	240	41.4647	-73.496961	Lucent	2	75	Active
736	CT72XC045	CON-WALLINGFORD 1	113	240	41.4647	-73.496961	Lucent	3	150	Active
748	CT33XC093	CON-WALLINGFORD 1	113	240	41.418917	-73.461944	Lucent	1	310	Active
748	CT33XC093	CON-WALLINGFORD 1	113	240	41.418917	-73.461944	Lucent	2	120	Active
748	CT33XC093	CON-WALLINGFORD 1	113	240	41.418917	-73.461944	Lucent	3	240	Active
751	CT43XC856	CON-WALLINGFORD 1	113	240	41.095117	-73.664219	Lucent	1	330	Active
751	CT43XC856	CON-WALLINGFORD 1	113	240	41.095117	-73.664219	Lucent	2	90	Active
751	CT43XC856	CON-WALLINGFORD 1	113	240	41.095117	-73.664219	Lucent	3	190	Active
755	CT54XC747	CON-WALLINGFORD 1	113	240	41.210333	-73.18125	Lucent	1	20	Active
755	CT54XC747	CON-WALLINGFORD 1	113	240	41.210333	-73.18125	Lucent	2	130	Active
757	CT54XC773	CON-WALLINGFORD 1	113	240	41.449392	-72.904572	Lucent	1	20	Active
757	CT54XC773	CON-WALLINGFORD 1	113	240	41.449392	-72.904572	Lucent	2	180	Active

Sample page of a Sprint Cell Site Report

The latitude and longitude of Sprint cell-site 721 is 41.176686, -73.146138.

<u>Plotting Cell Site Locations</u>

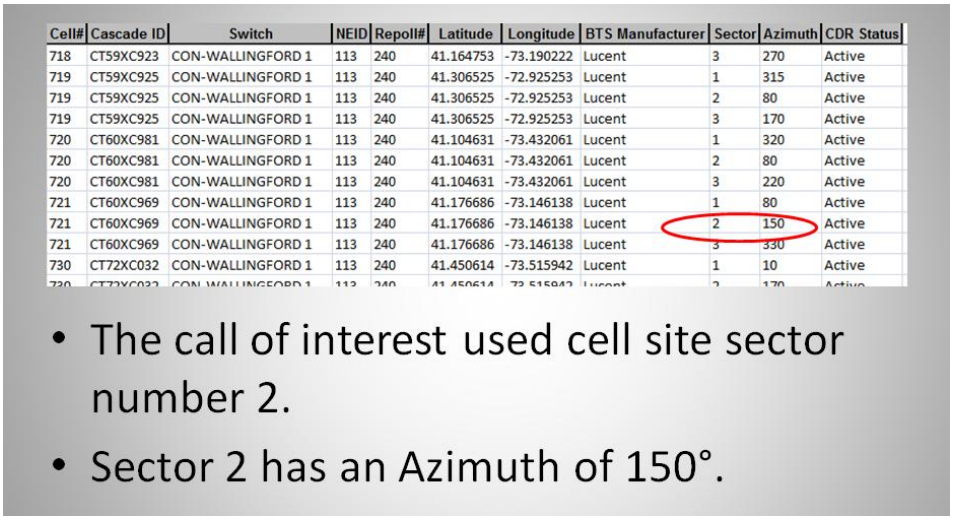
The site latitude and longitude can be plotted using on-line mapping tools such as Google Maps by entering the latitude and longitude in the map search box:



When this map location is viewed in Google Street View, the site is observed:

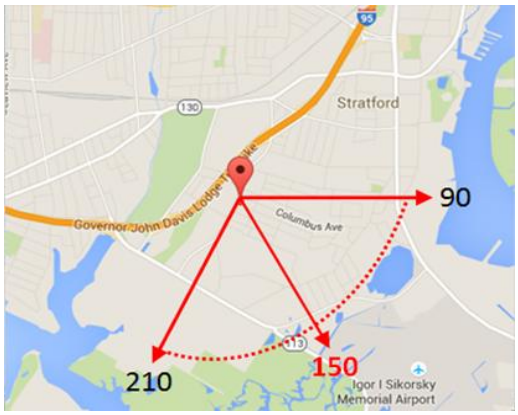
Sector Azimuth

On cell-sites with multiple sectors, the orientation of the antenna is identified.



Cell#	Cascade ID	Switch	NEID	RepoII#	Latitude	Longitude	BTS Manufacturer	Sector	Azimuth	CDR Status
718	CT59XC923	CON-WALLINGFORD 1	113	240	41.164753	-73.190222	Lucent	3	270	Active
719	CT59XC925	CON-WALLINGFORD 1	113	240	41.306525	-72.925253	Lucent	1	315	Active
719	CT59XC925	CON-WALLINGFORD 1	113	240	41.306525	-72.925253	Lucent	2	80	Active
719	CT59XC925	CON-WALLINGFORD 1	113	240	41.306525	-72.925253	Lucent	3	170	Active
720	CT60XC981	CON-WALLINGFORD 1	113	240	41.104631	-73.432061	Lucent	1	320	Active
720	CT60XC981	CON-WALLINGFORD 1	113	240	41.104631	-73.432061	Lucent	2	80	Active
720	CT60XC981	CON-WALLINGFORD 1	113	240	41.104631	-73.432061	Lucent	3	220	Active
721	CT60XC969	CON-WALLINGFORD 1	113	240	41.176686	-73.146138	Lucent	1	80	Active
721	CT60XC969	CON-WALLINGFORD 1	113	240	41.176686	-73.146138	Lucent	2	150	Active
721	CT60XC969	CON-WALLINGFORD 1	113	240	41.176686	-73.146138	Lucent	3	330	Active
730	CT72XC032	CON-WALLINGFORD 1	113	240	41.450614	-73.515942	Lucent	1	10	Active

This site has three sectors, so each sector is approximately 120°. The direction of the user is assumed to be in the following area:



Historical CDR/Cell-Site Analysis Issues

- No published principles or methods governing the estimation of cell site coverage area.
- Based on historical information, created for customer billing and network utilization.
- Many factors determine which site a device connects to, not necessarily the closest or strongest.
- All sites do not provide the same range and coverage can vary due to changing environmental factors.
- Locations identified by circles or pie shapes, bolstered by expert testimony, gives an incorrect impression.
- Service provider propagation maps may not reflect the state of the network during the exact time frame in question due to many changing variables.

Historical CDR/Cell Site Analysis Benefits

- Can help validate other findings, such as reports from the forensic examination of a device.
- Can show the device was in a general area at a given time or moved from one location to another.

Conclusion

Unlike real-time cell phone tracking, the methodology employed in historical cell site analysis should be properly scrutinized. A party against whom cell site evidence is offered should consider bringing a motion *in limine* to exclude it on grounds of admissibility. Otherwise, a party should timely raise an objection at trial on *Daubert* grounds to preserve the right to object to scientific or technical evidence and preserve the issue on appeal.

In almost all cases cell phone records will be admissible under the business records exception to the hearsay rule. Therefore, the hurdle to admissibility lies in authentication.

Tracking maps created from cell phone records should only be admitted with proper authentication of the underlying records. This prevents parties from offering evidence that may contain hearsay or lack a proper foundation, and would allow a witness to testify beyond the scope of what is actually supported by the evidence.

For more information on Call Detail Records, Cell-site Analysis and digital evidence, call now and speak with a certified expert. I.R.I.S. LLC is available 24 hours in emergency cases.