# Scientific Working Group on Digital Evidence

## SWGDE Recommendations for Cell Site Analysis

**Disclaimer:**
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

**Redistribution Policy:**
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

**Requests for Modification:**
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

**Intellectual Property:**
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

# SWGDE Recommendations for Cell Site Analysis

## Table of Contents



## Table of Figures

## 1. Purpose

The purpose of this document is to provide recommendations on the use of Historic Cell Site Location Information (HCSLI) contained in Call Detail Records (CDR) when conducting Cell Site Analysis (CSA).

## 2. Scope

This document provides information and recommended guidelines for using HCSLI contained within CDRs to conduct CSA. The intended audience for this document is practitioners who have training, knowledge, and experience in using these investigative techniques that may include investigators, analysts, and attorneys. This document is not intended to be a training manual or to replace standard organizational procedures. This document is not all inclusive and does not account for every possible scenario related to CSA. CSA should not be confused with mobile device forensics. Refer to *SWGDE Best Practices for Mobile Phone Forensics* for details of mobile device forensics best practices, linked here. CSLI may be obtained through other means, including law enforcement surveillances such as, pen registers and trap and trace devices with prospective cell site information, mobile device forensics, and location data that may exist in cloud or remote locations. While obtaining the location information through other means can be invaluable, the focus of this document is limited to HCSLI contained within the CDRs, as maintained by the cellular service providers relative to CSA.

## 3. Call or Communications Detail Records Data Preservation, Obtainment, Documentation, and Archiving

### 3.1 Introduction

Cellular service providers maintain records through the normal course of business or as required by law, which contain certain historical information, to include CDRs with HCSLI. This information can be obtained through an appropriate legal process. Additionally, data may also be available from other sources, including data from non-cellular providers that are considered official business records, from the forensic extraction of mobile devices, from law enforcement surveillances (e.g., pen registers), and potentially even cloud-based or remote locations.

It is beyond the scope of this document to discuss, in detail, various legal avenues that an analyst might pursue to preserve or obtain CDRs with HCSLI. Those seeking HCSLI should consult with legal counsel for specific guidance in a particular investigation within their jurisdiction. Practitioners are encouraged to become familiar with the particulars of each of these possible legal channels. Federal, state, and local laws might also provide guidance. Practitioners should always be mindful to comply with their own organization's policies and procedures. In order to preserve or obtain CDRs with HCSLI, practitioners may make use of one or more of the following legal instruments, in addition to other legal instruments, which may be applicable in certain jurisdictions.

### 3.1.1 Preservation Requests

Title 18 U.S. Code § 2703(f) provides law enforcement officials with the ability to order the preservation of records and other evidence held by an electronic communications provider. Preservation requests allow law enforcement to order providers to preserve data. In doing so, data that may otherwise be perishable (e.g., deleted by the provider) is preserved prior to the obtainment of the appropriate legal authority to secure the release of the preserved data.

### 3.1.2 Customer Consents

Electronic communications service providers may be able to release customer-related data to law enforcement officials after customer consent. Additional information relating to consent can be found in Title 18 U.S. Code § 2702(c)(2).

### 3.1.3 Lawful Emergencies and Exigent Requests (e.g., kidnappings, hostages, etc.):

Federal and some state laws allow for the immediate and voluntary release of CSA data by providers in certain specific emergency situations. Consult Title 18 U.S. Code § 2702(b)(8).

### 3.1.4 Search Warrants and Court Orders

Perhaps the most common method of obtaining HCSLI from CDR data in a criminal investigation is with a search warrant or, where permitted, other appropriate court order. In civil matters, civil court rules might allow for the use of a subpoena.

**** LEGAL INSTRUMENT NOTES****

In criminal cases, subpoenas are not accepted by US courts or communications providers to authorize the release of location-based data from cellular telephone records. However, in civil matters, various legal instruments may be allowed for obtaining CSA data.

***Legal issues change rapidly and are subject to interpretation, therefore always consult with your appropriate local legal counsel or prosecutor regarding all legal matters before acting.***

## 3.2 Service of Legal Demands

In order to obtain HCSLI CDR data from cellular providers, personnel requesting the data will typically need to serve legal demands to electronic communications providers. While service in person may be possible, legal demands are typically served electronically (e.g., email, website service), or via fax. It is important that both original and copies of legal demands be preserved and that the service of legal process be appropriately documented.

## 3.3 Obtaining Cell Site Lists and Reference Sheets and Court Admission Issues

In addition to the specific CSA data itself, it is also important to obtain any applicable cell site lists from the time in question, indicating where cell site antennas are located and how they are configured in the involved geographic areas. Even if CDRs are provided, which include specific latitude and longitude references to the antennas used by a target device, it is necessary to have the neighboring cell site locations and information to conduct CSA more thoroughly. It is also important to compare the latitude and longitude coordinates listed in the CDRs to ensure they are consistent with the cell site list.

Other useful data are any available reference sheets, instruction sheets, or legends that may be available to assist in properly interpreting the provided data. For example, time zones may be reported in various ways and it is imperative that the appropriate time zone is determined for the location of the device. It is also important to obtain a cell site list for the appropriate time period (e.g., not using a 2016 list when analyzing 2011 records).

Finally, if use of the records in court is anticipated, it is important to prepare to meet any applicable rules of evidence requirements. To ensure admissibility of these business records in court, it is typically sufficient to obtain a business records affidavit not only for the CDRs, but also for the cell site list(s) and any applicable instruction pages or legend documentation. Practitioners should exercise caution as records may be purged by the time these affidavits are requested. It also may be important to use a local jurisdiction's business records affidavit (e.g., from the state where the prosecution is occurring) rather than a business records affidavit from the state where the records are held or produced, if applicable.

### 3.4 Potentially Available Location Data Other than Historical CDR Cell Sites

Additional data may be available in the form of engineering and switch data, cell site/network maintenance data, per call measurement data, mobile device forensics, and pen registers. Practitioners should recognize that this data may not be held long and will require additional expertise to properly obtain, interpret, analyze, and present.

### 3.5 Documentation

Practitioners should document the process and procedures used to conduct CSA. It is important to document where, how, when, and by whom the data was obtained. Additionally, documentation should include specifically what data was obtained and how the data was archived. Finally, those conducting CSA should also maintain current documentation, such as a detailed curriculum vitae (CV) that thoroughly documents their qualification to conduct CSA. The CV should include formal education, training, case experience, and relevant experience in the field of CSA.

## 4. Interpreting the Data Once Received

HCSLI used in CSA is typically obtained from historical CDRs sourced from the cell service providers. HCSLI may also be obtained in real-time from legally-authorized surveillances, namely, pen registers and trap and trace devices. It may also be possible to obtain reliable location data from physical cellular devices utilizing mobile device forensics. Those conducting CSA should be familiar with the type of records produced by the various service providers and the intricacies and anomalies associated with each provider.

### 4.1 Formats of Different Cellular Providers

Cellular providers produce various formats of CDRs. While the CDRs from various cellular providers may look very different, they generally contain the same basic type of information, to include the date and time of the transaction, the originating and terminating number, the duration, and the cell site and sector information at the initiation of the transaction. The common information contained in the CDRs permits the use of HCSLI in the CDRs for reliable CSA. It is important to properly interpret the information and recognize the differences in key terms from the various cellular providers. A CDR reference document, also known as a "carrier key," should be requested from each cellular provider when legal process is served.

### 4.2 Cellular Network Operators versus Mobile Virtual Network Operators (MVNO)

A cellular network operator is a wireless communications service provider that owns or controls all the elements necessary to sell and deliver services to an end user, including radio spectrum allocation, wireless network infrastructure (antennas and switches), backhaul infrastructure, provisioning computer systems, and repair services. Examples of cellular network operators are AT&T, Sprint, T-Mobile, and Verizon Wireless.

A Mobile Virtual Network Operator (MVNO) is a wireless communications service provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a cellular network operator to obtain bulk access to network services at wholesale rates, then the MVNO sets retail prices independently. Examples of MVNOs are NetZero, NET10 Simple Mobile, Straight Talk, and TracFone.

It is important to note that in order to obtain records, data, or surveillance access on an MVNO cell phone, contact must also be made with the actual network providing service to the cell phone, in addition to the MVNO.

### 4.3 Differences in Time Zone Reporting

Service providers report CDRs in various time zones. For example, times could be reported in the time zone where the device is located, where the switch is located, a centralized location for the provider, or, commonly in Universal Coordinated Time (UTC) (Greenwich Mean Time [GMT]).

Caution must be taken when analyzing CDRs and converting listed times, if required, to local times. Additional caution should be exercised regarding Daylight Savings Time (DST), when applicable, as not all jurisdictions observe DST. In some circumstances, a switch may encompass multiple time zones which could significantly impact time adjustments for accurate analysis. A single CDR could also contain a mix of times zones based on different regions of the United States, as well as span the change to or from DST.

### 4.4 Pen Registers and Traps and Trace Devices

Pen registers and traps and traces are real-time, or near real-time, surveillance actions conducted by law enforcement. Pen registers and traps and traces, with appropriate legal authority, provide real-time cell site and sector information along with DRAS (dialing, routing, addressing, and signaling) data such as date, time, and senders' and receivers' identifiers. DRAS and location data does not include the content of any communications. As a result, CSA may be conducted with pen register or trap and trace data in addition to historical CDRs. However, practitioners should be aware that more data may be available in CDRs than is available in pen register and trap and trace data.

## 5. Processing the Data for Casework or Lead Purposes—Preliminary Reporting

Practitioners frequently conduct preliminary analysis and mapping to aid investigative efforts. Those conducting CSA for these purposes should exercise caution when placing too much confidence in CSA findings without additional verification. Practitioners will often conduct CSA under short time constraints. In doing so, various methods may be used to report preliminary results such as verbal reporting, quick hand-drawn maps, automated mapping tools, etc. For example, images may be captured via screen capture utilities and be printed, sent in emails, or attached to other documents. While often useful for quick use, those conducting CSA should always strive to accurately report the data and reduce confusion related to findings, especially with lay personnel. It is recommended that any preliminary reporting reflect a disclaimer representing that the product is in draft form and has not been fully verified.

## 6. Processing the Data for Court and Legal Proceedings—Final Reporting

When processing CSA data for court or legal proceedings, additional steps should be taken to ensure that the analysis was properly conducted and verified (including manual validation). Additionally, working with map images must be done with care so that map presentations preserve aspect ratios (are not distorted) and include a scale that is unaltered by resizing maps. Those conducting CSA should follow their organization's quality standards, which may include peer review, to ensure validity of the work product and ensure that the analysis is both accurate and repeatable. Finally, those presenting CSA in a legal setting should coordinate with prosecutors before any court presentation of CSA.

## 7. Mapping the Data

### 7.1 Omni-Directional Cell Site vs. Sectorized Cell Site

Omni-directional cell sites transmit their radio frequency (RF) signals in all directions from a single antenna. The single antenna provides 360-degree coverage from the site. A direction from the cellular antenna (other than somewhere in the 360-degree area of estimated coverage) cannot be determined from an omni-directional cell site. A Distributed Antenna System (DAS) is a type of omni-directional cell site.

A sectorized cell site utilizes directional antennas oriented to provide coverage to a specific geographic area. The most common type of sectorized cell sites utilizes three (3) antennas to complete 360-degree coverage area from the tower.

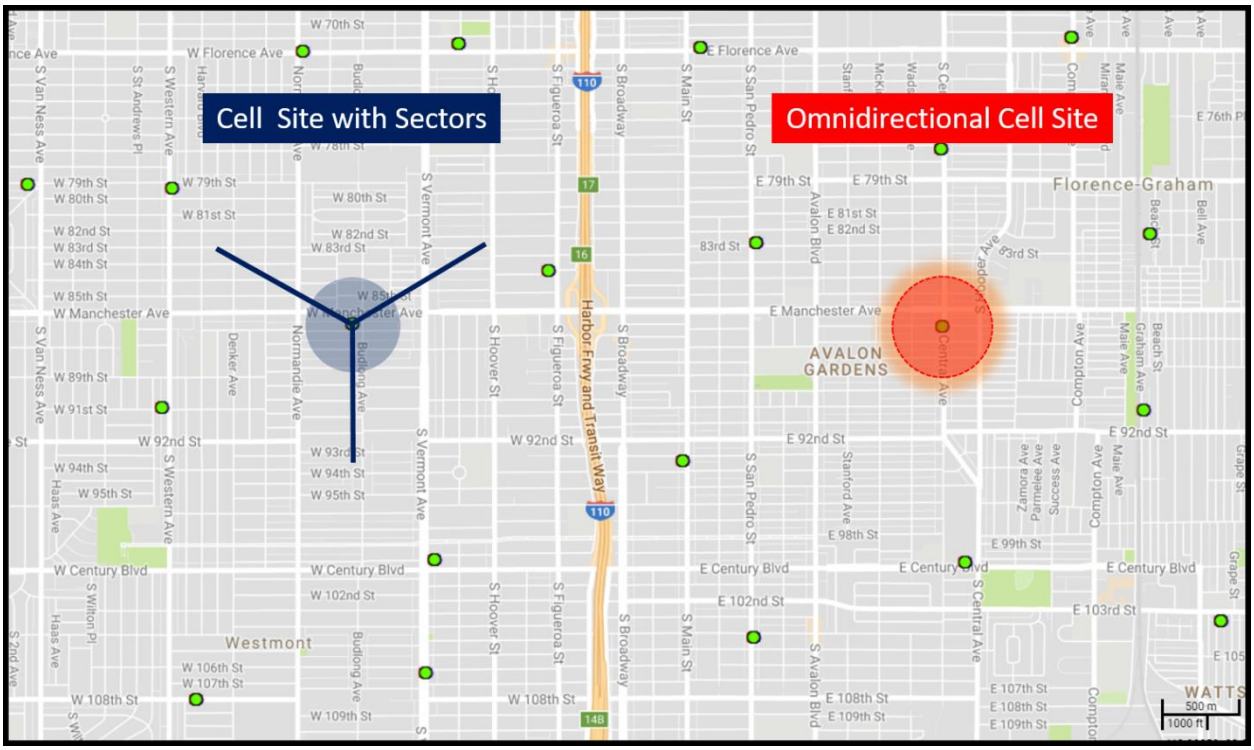


*Figure 1. Omni-Directional vs. Sectorized Cell Site Example*

## 7.2 Sectors

Cell Sectors are utilized by service providers to increase coverage and capacity within a specific geographic area. Sectors are oriented in a specific direction to provide coverage and limit interference from other sectors. The predominant configuration used by cellular providers are three (3) separate sectors, each providing 120-degree of coverage, and therefore provide 360-degree coverage around the cell tower. There are other configurations that may exist; for more information consult the carrier cell site list. Coverage area is not always uniform across all sectors and can vary from cell site to cell site.

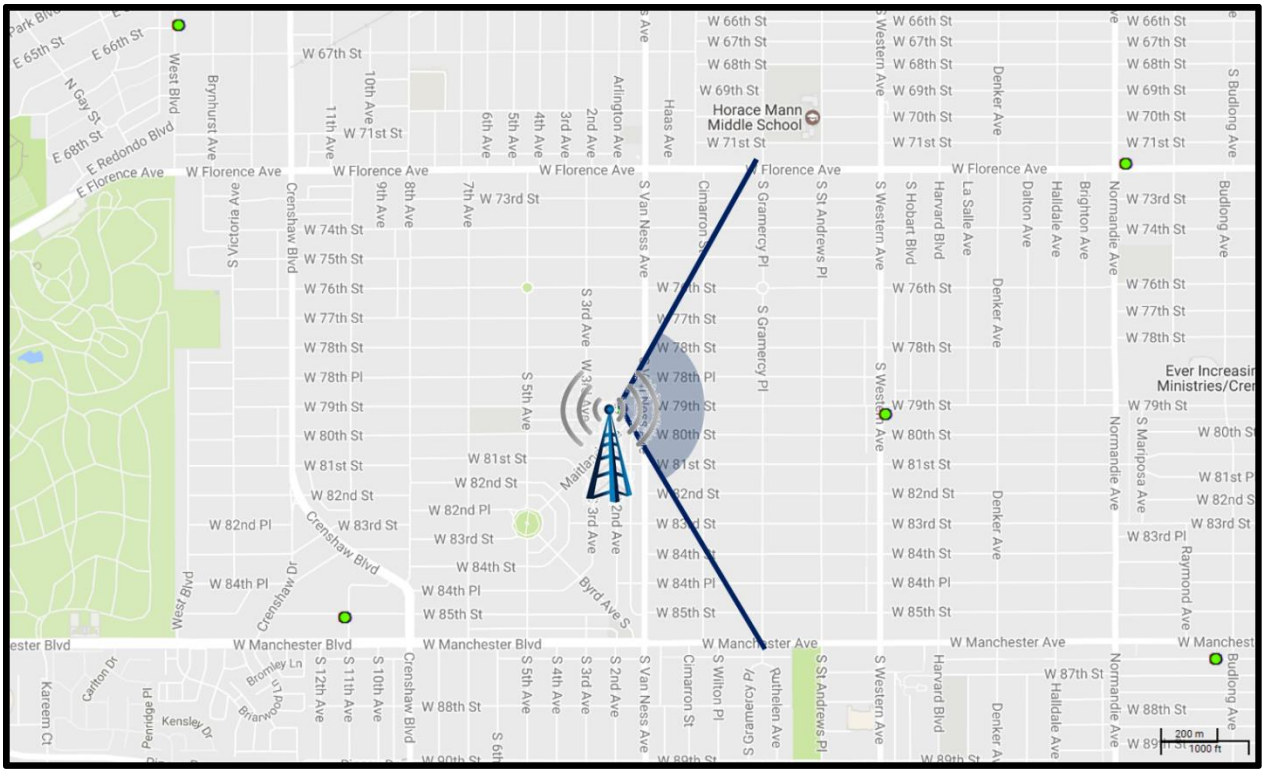


***Figure 2. Example of a Sector***

## 7.3 Azimuth and Orientation

The azimuth, also known as an orientation, is the direction representing the center of a sector's beamwidth. The azimuth bisects the sector's beamwidth and is represented in degrees. See Figure 3.

## 7.4 Horizontal Beamwidth (HBW)

This is the measurement of the angle of the sector, represented in degrees. Half of the beamwidth is on each side of the azimuth (counterclockwise and clockwise from the azimuth). Half Beamwidth is -3dB (half power) from the azimuth of the antenna. This should not be considered the absolute edge of the sector coverage. See ***Figure 3***.

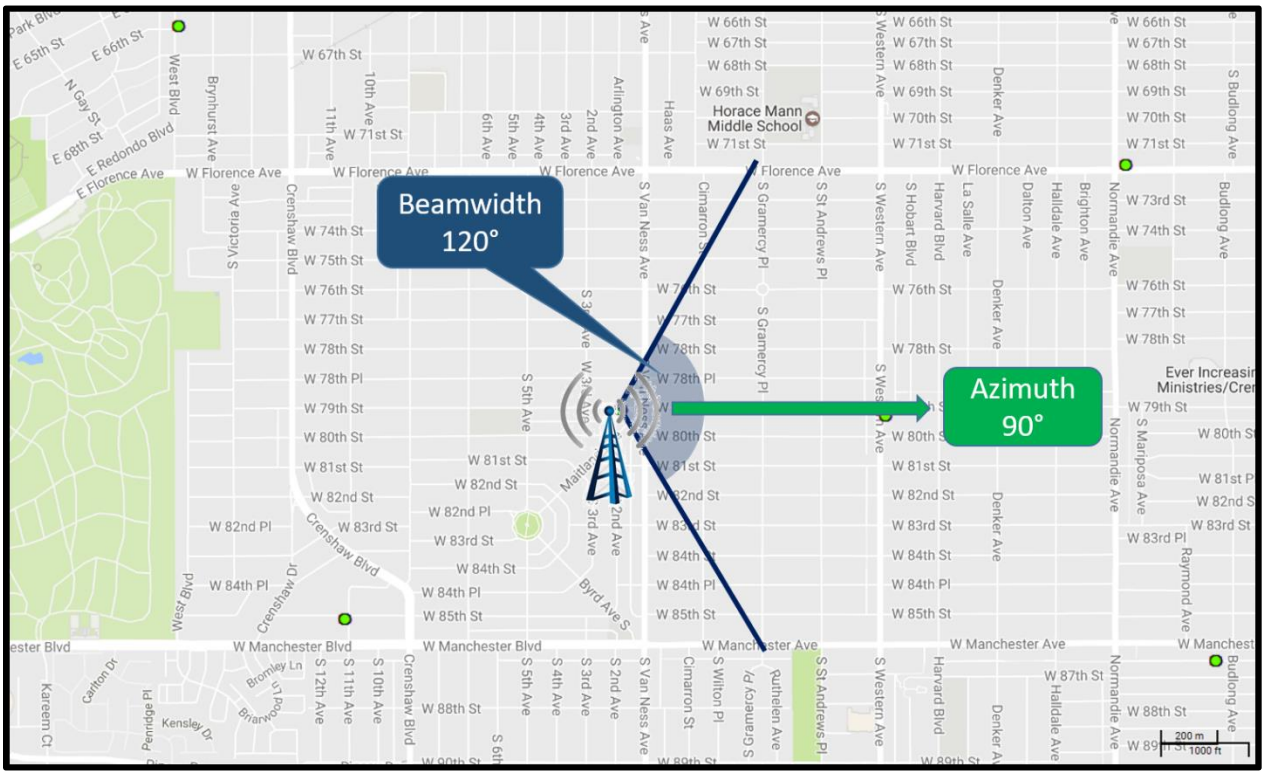


*Figure 3. Example of Azimuth and Beamwidth Measurements*

## 7.5 Optimal Beamwidth versus Actual Beamwidth

Optimal beamwidth (OBW), which is less degrees of coverage than the actual beamwidth, is the horizontal beamwidth that is often reported by the service provider and consists of the strongest area of coverage within the center of the sector's beamwidth of coverage. Actual beamwidth is the total geographic area of the sector in which there would be coverage. Cell site sectors' actual beamwidths typically cover 120-degrees. However, a beamwidth may vary and should be verified with service providers as needed. Caution should be utilized when working with optimal beamwidths and actual beamwidths to not underestimate a sector's actual coverage.

## 7.6 Neighboring Sectors and Cell Sites

Neighboring cell sites can be used for estimating the coverage area of the target cell site. Theoretically, the boundaries of a cell site's coverage area can be estimated by the proximity of neighboring cell sites. Generally, a cell site's coverage area will overlap with adjacent sectors.

## 7.7 Ranging Data

Cellular service providers often maintain ranging data for engineering and network optimization purposes through the normal course of business called Round Trip Delay (RTD). The retention for these types of records is relatively short, and, requests to preserve the records should be made as soon as possible after the incident. RTD provides an approximate distance of the mobile device from the cell site. RTD is the measurement of the time required for the signal to travel from the cell site to the handset and then back to the cell site. This type of data is non-technology specific and can be found in GSM, CDMA, and LTE networks and is commonly referred as Per Call Measurement Data (PCMD). In some cases, service providers also provide an estimate of the approximate location of the device via latitude and longitude with a margin of error. The coordinates provided in these types of records are generated from a proprietary algorithm and are not intended to provide an exact location of a device. As a result, it is recommended that ranging data be manually mapped at the listed ranges within the provided sectors.

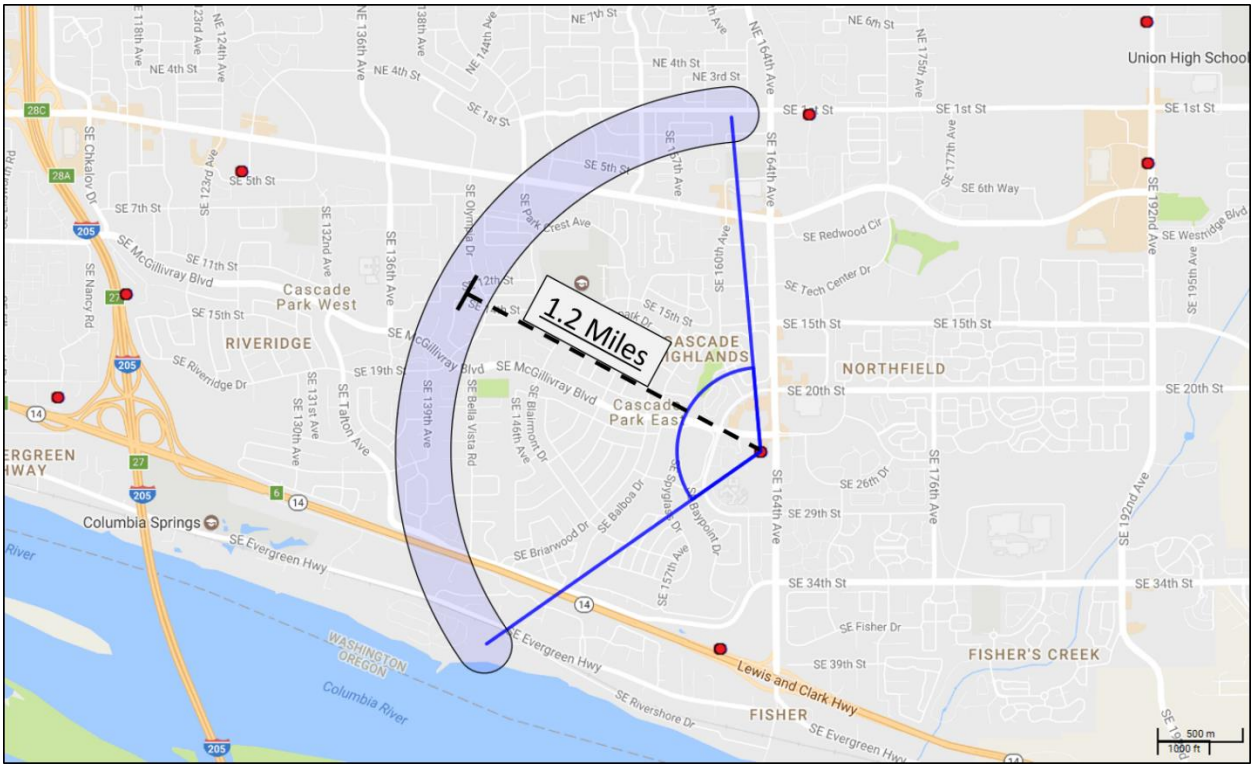


***Figure 4. Example of Cell Site Coverage Area with Per Call Measurement Detail (PCMD) Included***

### 7.8 Precision Geolocation Information

Geolocates are real-time, precision location requests by the network from the device. Geolocates are commonly referred to as "pings" and will normally report a latitude and longitude along with a certainty factor or margin of error from that point. It is extremely important to map the certainty factor, or radius, that is reflected in the geolocate data. Simply mapping the latitude and longitude commonly will not provide a valid result on its own. Further, geolocate data is not kept in the normal course of business and is typically not obtainable from the service providers as official business records.


*Figure 5. Example of Geolocates*

## 8. Validation

Those conducting CSA should be able to validate their results by using alternate automated tools or manual mapping techniques. When using automated tools or software to plot and report the location data for formal legal proceedings, those conducting the analysis should be able to explain how the software or tool works and be able to validate the accuracy of the final results by mapping manually. Validation should also be conducted when new software or tools are utilized. A secondary validation is encouraged following organizational peer-reviewed processes or policies.

## 9. Presenting the Data in Legal Proceedings

CSA practitioners should properly represent map data by providing legends or distance scales and presenting proportionally-accurate maps. In addition, practitioners should consult and coordinate with their appropriate legal counsel.

As a general rule, courts require the witness presenting HCSLI to be admitted as an expert witness. The witness needs to have significant knowledge, training, and experience interpreting CDRs. Those conducting CSA should be prepared to present a thorough CV detailing this relevant knowledge, training, and experience. Legal considerations such as Daubert and Frye standards, or any other applicable expert witness legal requirements, may apply.

Knowledge, training, or experience conducting cellular or mobile device or computer forensics (e.g., use of a forensic extraction tool) does not equate to having adequate training, knowledge, and expertise to conduct CSA.

## 10. Considerations

CSA only demonstrates the specific cell site and sector (if applicable) used by a specific cellular device at a specific date and time. CDRs, in and of themselves, do not conclusively indicate specifically who was using a device, but can be used to establish patterns of use. Furthermore, cell site and sector information in CDRs do not allow for the identification of an exact location of a device at a specific date and time (e.g., a specific intersection, address, etc.).

Further, an advanced method of CSA not detailed in this document includes the utilization of RF survey equipment to establish detailed cellular signal propagation estimates. These more detailed RF estimates may be displayed on RF propagation maps (i.e., frequency-coverage heat maps).

## 11. Future Considerations

This document was prepared with the resources available at the time of publication. As with all technology, CSA is a constantly evolving discipline with frequent implementation of new features and innovations. Notably, while much of the voice traffic of cell phones in the United States still utilizes second generation (2G) or third generation (3G) cellular technologies, the United States cellular industry is already using rapidly expanding the use of fourth generation (4G) cellular systems. When 4G systems are fully implemented, all cellular network traffic will be transmitted via internet protocol (IP) standards. Additionally, fifth generation (5G) systems are already being tested. As time progresses, the data available from cellular providers will change, as will the formats in which the available data is provided.

## 12. Additional Resources

[1] United Kingdom Accreditation Service (UKAS), "ISO/IEC 17025 Accreditation for Forensic Cell Site Analysis – An Overview – Pilot Update July 2016," May 5, 2016. Available: https://www.ukas.com/download/development_pilot_programmes/Cell Site Analysis Project - ISO17025 Accreditation of Cell Site Analysis - An overview(2).pdf.

[2] CSIR Built Environment, "Analysis and Mapping of Cellular Telephone Usage. Contract Report: Sea Point CAS," Pretoria, South Africa, June 14, 2009.

[3] P. Schmitz, A. Cooper, A. Davidson and K. Roussow, "Breaking Alibis through Cell Phone Mapping," *Crime Mapping Case Studies: Successes in the Field, Volume 2,* pp. 65-72, 2000. Available: https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=183202.

[4] "Cell Phone Analysis," *ESRI ArcGIS for Local Government*, 22 April 2017. [Online]. Available: http://solutions.arcgis.com/local-government/help/cell-phone-analysis/.

[5] E. Sanow, "Cell Phone Analysis: Part 1," *Law and Order Magazine,* November 2012. [Online]. Available: http://www.hendonpub.com/law_and_order/articles/2012/11/cell_phone_analysis_part_1.

[6] E. Sanow, "Cell Phone Analysis: Part 2," *Law and Order Magazine,* December 2012. [Online]. Available: http://www.hendonpub.com/resources/article_archive/results/details?id=4900.

[7] A. Edens, Cell Phone Investigations: Search Warrants, Cell Sites and Evidence Recovery, Police Publishing, ISBN: 978-1-63180-006-1, 2014.

[8] K. Metcalf, Cell Phones in Criminal Investigations: Basic Preparation, Analysis, and Mapping of Cellular Data, Amazon Digital Services LLC, 2016.

[9] "Cell Site Analysis and Mapping," *Forensic Magazine*, 23 January 2013. [Online]. Available: http://www.forensicmag.com/product-release/2013/01/cell-site-analysis-and-mapping-0. [Accessed 22 April 2017].

[10] G. Smith, "Checking Masts – Cell Site Analysis (CSA)," *Forensic Focus*,15 July 2011. [Online]. Available: https://articles.forensicfocus.com/2011/07/15/checking-masts-cell-site-analysis-csa/. [Accessed 19 June 2017].

[11] "Appendix: digital forensics: cell site analysis. Part of: Forensic science providers: codes of practice and conduct," Forensic Science Regulator of United Kingdom, Ref: FSR-C-135, 9 June 2016. [Online]. Available: https://www.gov.uk/government/publications/cell-site-analysis.

[12] P. Schmitz, C. Eloff, R. Talmakkies, C. Linnen and R. Lourens, "Forensic mapping in South Africa: four examples," *Cartography and Geographic Information Science,* vol. 40, no. 3, pp. 238-247, May 2013. [Online]. Available: http://dx.doi.org/10.1080/15230406.2013.800273.

[13] J. Hoy, Forensic Radio Survey Techniques for Cell Site Analysis, West Sussex: Wiley, February 23, 2015.

[14] R. Ayers, S. Brothers and W. Jansen, "Guidelines on Mobile Device Forensics," *NIST Special Publication 800-101*, pp. Section 6.3, pages 52 through 54, May 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

[15] M. Tart, I. Brodie, N. Gleed and J. Matthews, "Historic cell site analysis – Overview of principles and survey methodologies," *Digital Investigation*, vol. 8, no. 3-4, pp. 185-193, February 2012.

[16] B. Siuru, "How Can Cell Phone Records Help to Solve Crimes?," *Police and Security News*, pp. 44-46, September/October 2014. [Online]. Available: https://policeandsecuritynews.com/imgs/archives/2014/digital/SeptOct2014.pdf.

[17] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, "Investigative Uses of Technology: Devices, Tools, and Techniques," *NIJ Special Report*, pp. 11, 13, 17, 31, 33, and 102, October 2007. [Online]. Available: https://www.ncjrs.gov/pdffiles1/nij/213030.pdf.

[18] P. Schmitz and A. Cooper, "Mapping Crime Scenes and Cellular Telephone Usage," South Africa)., 2000. [Online]. Available: http://hdl.handle.net/10204/2788.

[19] P. Schmitz, A. Cooper, T. De Jong and D. Rossmo, "Mapping Criminal Activity Space," *Journal of Intelligence and Analysis*, vol. 22, no. 3, pp. 67-94, December 2015.

[20] C. Miller, " The Other Side of Mobile Forensics," *Officer.Com*, 1 July 2008. [Online]. Available: http://www.officer.com/article/10248785/the-other-side-of-mobile-forensics.

[21] T. O'Connor, "Provider Side Cell Phone Forensics," *Small Scale Digital Device Forensics Journal*, vol. 3, no. 1, June 2009. [Online]. Available: http://ctfdatapro.com/pdf/celltower.pdf.

[22] H. B. Dixon Jr., "Scientific Fact or Junk Science? Tracking a Cell Phone without GPS," *The Judges' Journal*, vol. 53, no. 1, 2014. [Online]. Available: https://www.americanbar.org/publications/judges_journal/2014/winter/scientific_fact_or_junk_science_tracking_a_cell_phone_without_gps.html.

[23] I. Ajala, "Spatial Analysis of GSM Subscriber Call Data Records," *Directions Magazine*. 8 March 2006. [Online]. Available: http://www.directionsmag.com/entry/spatial-analysis-of-gsm-subscriber-call-data-records/123196.

[24] A. Cooper and P. Schmitz, "Tactical Crime Mapping in South Africa," *Networks and Communication Studies, NETCOM*, vol. 17, no. 3-4, pp. 269-279, 2003. [Online]. Available: https://www.researchgate.net/profile/Antony_Cooper2/publication/228410584_Tactical_Crime_Mapping_in_South_Africa/links/00b49527b96fdd8e6f000000.pdf?origin=publication_detail.

[25] P. Schmitz, S. Riley and J. Dryden, "The Use of Mapping Time and Space as a Forensic Tool in a Murder Case in South Africa," in *Proceedings of the 24th International Cartographic Conference*, Santiago de Chile, Chile, November 19 2009. [Online]. Available: http://icaci.org/files/documents/ICC_proceedings/ICC2009/html/refer/20_5.pdf.

[26] T. O'Malley, "Using Historical Cell Site Analysis Evidence in Criminal Trials," *United States Attorneys' Bulletin,* vol. 59, no. 6, pp. 16-34, November 2011.

## 13. Definitions

*The following definitions are provided to assist with interpreting this document. They are written in lay terms to the extent reasonably possible. For further details, readers may refer to more technical resources defining these terms, such as Cellular Telecommunications Industry Association (CTIA) (http://files.ctia.org/pdf/Telecom_Glossary_of_Terms.pdf), Third Generation Partnership Project (3GPP) (http://www.3gpp.org/technologies/95-keywords-acronyms), and European Telecommunications Standards Institute (ETSI) (http://webapp.etsi.org/Teddi/).*

**4G, LTE** – Fourth generation Long Term Evolution (LTE) is a standard for wireless communication of high-speed data for mobile phones and devices. All cell phone companies in the United States have deployed, or will deploy, 4G cellular systems.

**Actual Beamwidth (ABW)** – The coverage that is not always reported by a cellular provider for a cell site sector's coverage, but is the actual beamwidth that the cell site sector actually covers. This is also known as total coverage area.

**Addressing and Routing Data** – Data that represents the transactional data of an electronic communications event. This data includes such items of data as the phone numbers dialed, durations of phone calls, phone numbers involved in text messages, Internet Protocol (IP) addresses involved in data transactions, etc. This data does not include the contents of any electronic communications.

**Antenna** – An electrical device which converts electric power into radio waves, and vice versa. It is usually with a radio transmitter or radio receiver and can be mounted on various structures including poles, masts, towers, etc.

**Automated Cell Site Analysis Program** – An analysis program providing analysis or mapping of cell site data which is designed for practitioners and law enforcement investigators to automate the mapping of CDRs from cell phone companies.

**Azimuth** – The direction an antenna is pointed in degrees where zero is north. With a cell site sector, the azimuth represents the center of the cell site's coverage. Azimuth is also known as orientation.

**Base Transceiver Station (BTS)** – A piece of equipment that facilitates wireless communication between user equipment (UE) and a network. UEs includes devices such as mobile phones (handsets) or computers with wireless Internet connectivity. The network can be that of any of the wireless communication technologies like GSM, CDMA, wireless local loop, Wi-Fi, or other wide area network (WAN) technology.

**Beamwidth** – The radio frequency arc of coverage of an antenna measured in degrees. With a cell site sector, half of the beamwidth is represented counterclockwise and the other half of the beamwidth is represented clockwise from the azimuth. Beamwidth in cell site analysis typically represents the horizontal beamwidth (HBW) of coverage of a sector. Vertical beamwidth (VBW) can represent antenna's uptilt or downtilt.

**Call Detail Record (CDR)** – Records maintained by the service provider capturing information typically needed to accurately bill a subscriber or, in the case of a prepaid service plan, debit the balance. This information typically includes the date, time, duration, source identifier, destination identifier, or, the amount of data transmitted or received.

**Cell Site** – A cell site is a physical location that is comprised of the equipment needed to receive and transmit radio signals for cellular voice and data transmission that may consist of equipment from one or more cellular telephone companies. Cell sites are designed to provide radio frequency coverage over defined geographic areas.

**Cell Site Analysis (CSA)** – The analysis of historical records provided by the cellular companies, or other geographic data, in order to place a particular cellular device within an approximate, and possibly even fairly-specific, geographic area during a specified date and time.

**Cell Site List** – The list of all cellular system antenna with sector information that is retained by a cell provider. Cell site lists typically contain the latitude and longitude of cell sites as well as specific sector information including the azimuths and beamwidths of sectors.

**Cell Site on Wheels (COW)** – A portable mobile cellular site that provides temporary network and wireless coverage to locations where cellular coverage is minimal, compromised, or there is an increase in users for a specified event. Cell sites on wheels can also be known as Repeaters and Trailers (RATs).

**Cellular Network Operator** – A cellular network operator is a wireless communications service provider that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure (antennas and switches), backhaul infrastructure, provisioning computer systems and repair organizations. Examples of cellular network operators are AT&T, Sprint, T-Mobile, and Verizon Wireless.

**Cellular Radio Frequency (RF) Coverage Estimate** – The theoretical estimation of the geographic coverage of a particular cell site or sector.

**Code Division Multiple Access (CDMA)** – A spread spectrum technology for cellular networks based on the Interim Standard-95 (IS-95) from the Telecommunications Industry Association (TIA).

**Distributed Antenna System (DAS)** – A network of relatively-small antennas within a geographic area or structure.

**DRAS** – Dialing, Routing, Addressing, and Signaling information of electronic communication events including phone calls, text messages, data transactions (i.e., IP), etc.

**Drive Test** – (see Radio Frequency Survey)

**Geolocate** – Real-time, precision location requests from the device in a surveillance capacity. Geolocates are commonly referred to as "pings" and will normally reflect a latitude and longitude along with a certainty factor. Geolocates may be produced through various means and several major cell phone providers can provide law enforcement geolocates on a target pursuant to appropriate legal authority. A geolocate may also require some form of legal process.

**Global Positioning System (GPS)** – A system for determining position via latitude and longitude by comparing radio signals from several satellites.

**Global System for Mobile Communications (GSM)** – A set of standards for second generation, cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP).

**Heat Map** – A geographical representation of RF coverage where the individual signal strengths are represented as colors.

**Historic Cell Site Location Information (HCSLI) –** The historical communications data contained within a Call Detail Record (CDR).

**Internet Protocol (IP) –** The principal communications protocol used to move data across the Internet, and most Intranets, via packets of data.

**Latitude and Longitude** – A coordinate system that enables every location on the Earth to be specified by a set of numbers.

**Micro Cell** – A cell in a mobile phone network served by a low power cellular base station, which covers a limited area such as a mall, a hotel, or a transportation hub. A microcell is usually larger than a pico cell, though the distinction is not always clear.

**Mobile Virtual Network Operator (MVNO)** – A wireless communications services provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a cellular network operator to obtain bulk access to network services at wholesale rates, then sets retail prices independently.

**Neighboring Cell Sites** – Cell sites that are in close proximity to the target cell site. Neighboring Cell Sites can affect the outer boundaries of a target cell site's coverage area.

**Network Extender** – Any device used to extend a network segment beyond its inherent distance limitation. These devices employ a variety of transmission technologies and physical media (wireless, copper wire, fiber-optic cable, coaxial cable) to access the cellular networks.

**Omni-Directional Cell Site (AKA Omnipole)** – A cell site that contains only one sector with 360° of coverage.

**Optimal Beamwidth (OBW)** – The coverage that is reported by a cellular provider that reflects the best, or optimal, coverage area of a particular sector. Optimal beamwidth does not typically reflect the absolute coverage area of a particular sector.

**Orientation** – The direction an antenna is pointed in degrees where zero is north measured in degrees out of 360. With a cell site sector, the orientation represents the center of the cell site's coverage. Orientation is also known as azimuth.

**Pen Register** (related Trap and Trace) – A law enforcement surveillance technique that monitors and records, in real time or near real time, the outgoing destination identifiers (i.e., dialed phone numbers) of a target's phone calls, text messages, data transactions, or other electronic communications. Pursuant to appropriate legal authority with cellular telephones, pen registers also provide the cell site and sector location data for these communication events.

**Pico Cell** – A small mobile phone base station connected to the cellular network via the Internet that is typically used to improve mobile phone reception indoors and considered to be smaller than a microcell.

**Radio Frequency (RF)** – Any of the electromagnetic wave frequencies that lie in the range extending from around 3 kHz to 300 GHz, which include those frequencies used for communications or radar signals. RF usually refers to electrical rather than mechanical oscillations.

**Radio Frequency (RF) Survey** – A survey of radio frequency signals using sophisticated equipment and antennas. This provides a detailed map of the radio frequency coverage for a specific geographic area.

**Ranging Data** – A measurement of the time it takes for a signal to be transmitted from the base transceiver station (BTS) at the cell site to a remote cellular device and back to the BTS. Ranging data may also be reported as Range to Tower (RTT), Round Trip Delay (RTD), Real Time Tool (RTT), Per Call Measurement Data (PCMD), Reveal Data, Timing Advance, etc. Ranging data provides distance-from-antenna estimates along an arc within sectors.

**Repeater and Trailer (RAT)** – A portable mobile cellular site that provides temporary network and wireless coverage to locations where cellular coverage is minimal, compromised, or there is an increase in users for a specified event. Cell sites on wheels can also be known as Repeaters and Trailers (RATs).

**RF Propagation Map** – A geographical representation of RF coverage, not necessarily including signal strengths, which displays the approximate boundaries of a cell site.

**Roaming** – The ability to make and receive voice calls, send and receive data, or access other services, when travelling outside the geographical coverage area of the home network, by means of using a roaming network.

**Sector** – The section of a cell site that covers a specified geographic area.

**Sector Line** – The line that is drawn to establish the approximate outer clockwise and counterclockwise boundary of a sector measuring in degrees from the azimuth. This is also known as the edge of the sector and is determined by the azimuth and beamwidth.

**Survey** – see Radio Frequency Survey.

**Tower** – A cellular telephone site where an antenna and electronic communications equipment are placed on a radio tower mast to create a cell site(s) in a cellular network.

**Trap and Trace** (related Pen Register) – A law enforcement surveillance technique that monitors and records, in real time or near real time, the incoming origination identifiers contacting a target. This can include incoming telephone numbers involved in phone calls, text messages, data transactions, or other electronic communications. Pursuant to appropriate legal authority with cellular telephones, trap and trace devices also provide the cell site and sector location data for these communication events.

**Walk Test** – A survey of radio frequency signals using sophisticated equipment and antennas by walking around with test equipment in the target area. This provides a detailed map of the radio frequency coverage for a specific geographic area.

# SWGDE Recommendations for Cell Site Analysis

## History

| Revision | Issue Date | Section | History |
|---|---|---|---|
| 1.0 DRAFT | 2016-09-15 | All | Initial draft created and SWGDE voted to release as a Draft for Public Comment. |
| 1.0 DRAFT | 2016-10-08 | All | Formatting and technical edit performed for release as a Draft for Public Comment. |
| 1.0 DRAFT | 2017-01-12 | All | Full rewrite performed on the initial draft; title changed to remove “Forensic” before “Cell Site Analysis.” SWGDE voted to re-release as a Draft for Public Comment. |
| 1.0 DRAFT | 2017-02-21 | All | Formatting and technical edit performed for re-release as a Draft for Public Comment. |
| 1.0 DRAFT | 2017-06-22 | All | Additional revisions were made to all sections for finalization. SWGDE voted to re-release as a Draft for Public Comment. |
| 1.0 DRAFT | 2017-07-11 | All | Formatting and technical edit performed for re-release as a Draft for Public Comment. |
| 1.0 | 2017-08-24 | All | SWGDE voted to publish as an Approved document (Version 1.0). |
| 1.0 | 2017-09-25 | | Formatted and published as Approved Version 1.0. |