Forensic Capability Network
Shaping forensics, together.

Supplementary Technical Notes for Cell Site Analysis for Geolocation

06/03/25

Version: 1.0 | Document Ref: FCN-DDD-GUI-0002 | Classification: OFFICIAL

Document Control

Document status	ACTIVE
Author	Jon Heathcote, Staffordshire Police

Update History

Version	Issue Date	Reason for Issue	Updated by	Reviewed by	Approved by
1	06/03/2025	To supplement the SFR process for Cell Site Analysis for Geolocation	Jon Heathcote, Staffordshire Police	Paul Roberts – Scientific Officer	Chris Davies – Quality Officer

Grey shaded sections will denote changes from previous version

Contents

1. Introduction

These guidance notes are intended to be used to supplement the production of an MG22 (SFR) form, such that the forensic result can be reported in the most clear and succinct way. The relevant version and section(s) of these supplementary notes should be quoted within the MG22 document produced by the person creating the report.

1.1 Definitions and Abbreviations

Abbr.	Meaning
CDR	Call Detail Record
CI	Cell ID
CSP	Cellular Service Provider
DDR	Device Detail Records
ECI	Enhanced Cell ID
GPRS	General Packet Radio Service
IMSI	International Mobile Subscriber Identity
LAC	Location Area Code
MMS	Multi Messaging Service
SAC	Service Area Code
SIM	Subscriber Identity Module
SFR	Streamlined Forensic Reporting
UE	User Equipment
Definitions	
Can	indicates a possibility or a capability
DNA-17	A DNA test that targets 17 areas of DNA plus a gender marker
May	indicates a permission
Shall	indicates a requirement
Should	indicates a recommendation

2. Cell Site Analysis for Geolocation

2.1 Overview

2.1.1 Cell site analysis for geolocation purposes, is a combination of forensic techniques, including call data analysis and radio frequency surveying (RF survey), which are used to geolocate a mobile device (or devices) to an approximate location, at a certain date and time.

2.1.2 These techniques are reliant on data recorded by the mobile network operators when a mobile device interacts with the network in a recordable event, which include voice calls, text messages and data sessions.

2.1.3 These records include user-initiated activities, such as calls made and text messages sent, as well as passive communications, like received text messages, unanswered calls, or automated data session activities.

2.1.4 The mobile telephone network infrastructure provided by the main service providers consist of large numbers of cell sites. Each site can consist of numerous individual transceivers (known as cells) each designed to cover a limited geographical area, which overlaps with the service areas of neighbouring cells.

2.1.5 Each cell is assigned a unique cell ID. When a mobile device user engages in a call, sends or receives a text, or uses data, the cell ID is captured, along with other data for the purposes of billing the subscriber for their use of the network resources. The billing records incorporating cell information are generally referred to as Call Data Records or Call Detail Records (CDRs).

2.1.6 A typical cell site consists of a mounting structure with one or more antennas and an enclosure that houses the necessary electronic equipment. Typically, the antennas at each cell site are configured in one of three ways:

2.1.7 Omnidirectional: transmitting and receiving radio signals in all directions (three hundred and sixty degrees) from the antenna site. Separate antennas at the same cell site may be similarly broadcasting in all directions at different frequencies for capacity or technology purposes.

2.1.8 It should be noted that some records show a cell on an omnidirectional cell site as having an antenna facing of zero degrees.

2.1.9 Sectorised: separate antenna transmitting and receiving radio signals in different directions from a common cell site. Commonly these are three sector sites, on which each antenna is configured to transmit and receive within an arc of just over one third of the circle. Other distributions of antennas and numbers of sectors exist. Additional antennas at the same cell site may be utilising the same sectorisation of the site to increase capacity or provide signal on other network technologies.

2.1.10 A two-sector cell site may be deployed to cover stretches of motorway or railway lines. The sectors may be configured to point in opposite directions, although this configuration may be adapted to better suit the route taken by the road or rail being serviced.

2.1.11 This is demonstrated in the following diagrams:

Figure 1: Omnidirectional Cell Site

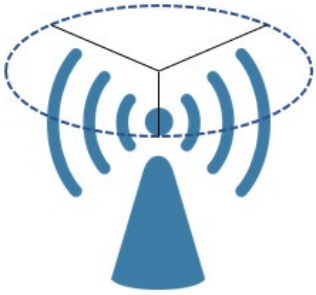

Figure 2: Sectorised Cell Site

2.1.12 The distribution of the most common sectorised cell site uses three directional antennas, each providing service over evenly distributed, theoretical one-hundred-and-twenty-degree arcs. The general direction, or bearing to which each antenna is orientated is known as the azimuth and is measured in degrees, clockwise from zero degrees for due north:

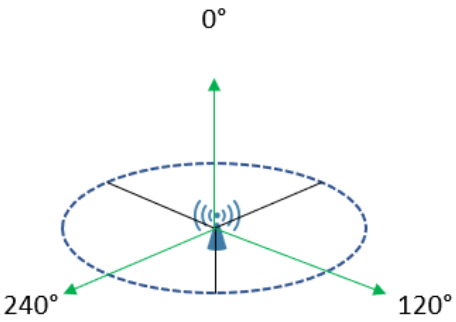

Figure 3: Example of sectors and azimuth

2.1.13 Rural areas will generally have fewer cell sites than in urban areas. This is because of differences in population density and a corresponding increase in demand for network services in the built-up area, together with the increase of man-made obstacles (clutter) that limit the potential range of cells in an urban environment. A rural cell site would usually exhibit greater coverage than a cell sited in an urban area. As illustrated by the following diagram:

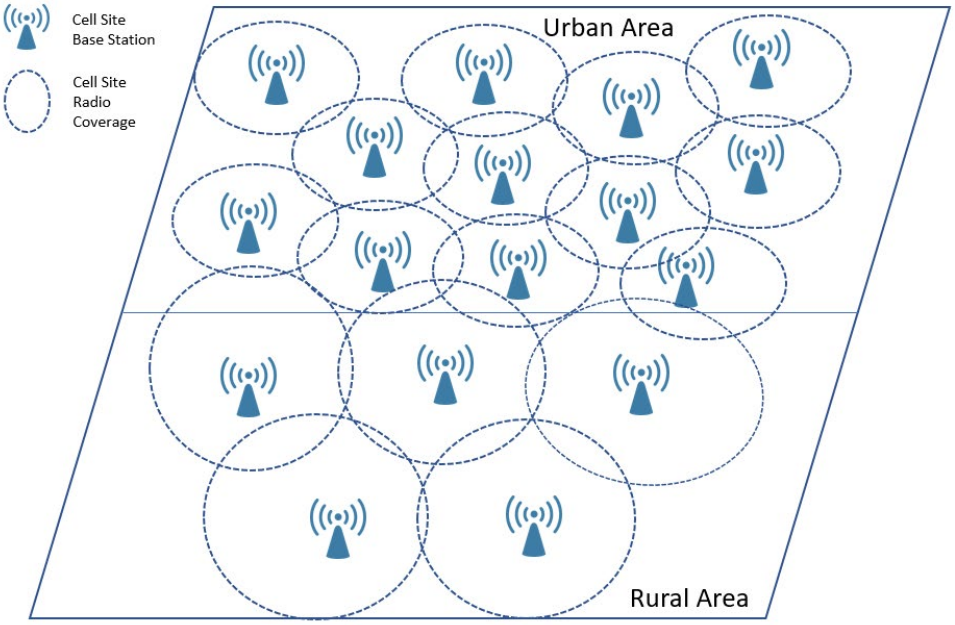

Figure 4: Example of urban and rural cell density

2.1.14 The cells that the mobile device connects to, would be referred to as a 'serving cell'.

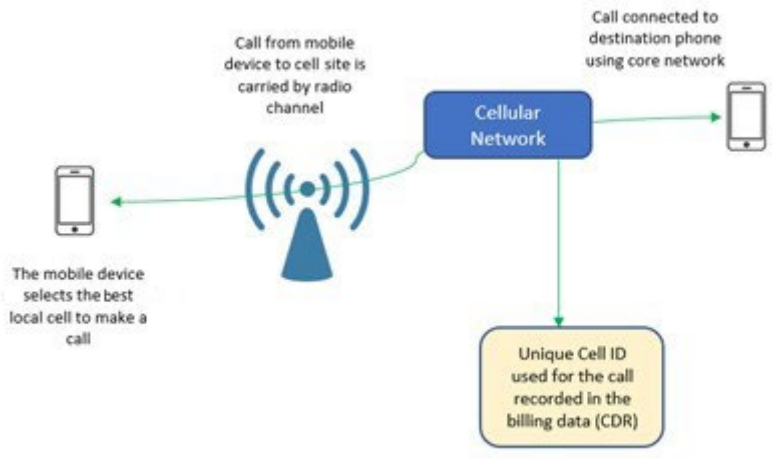

Figure 5: Basic cell selection and call process

2.1.15 Mobile phone network operators can, when the correct authority is provided, release details of calls, text messages, or data sessions, including the cell IDs that were used by a mobile device, which are recorded for engineering purposes and billing subscribers. This is provided in the CDRs as previously described.

2.1.16 Analysis of CDRs is useful to an investigator or a court, to determine what cells were used by the mobile device at or around a relevant date/time in the investigation. It is then possible to conclude that a mobile device used a cell covering the relevant location at the time of that call event, although it may have also been at other locations where the cell serves a usable signal.

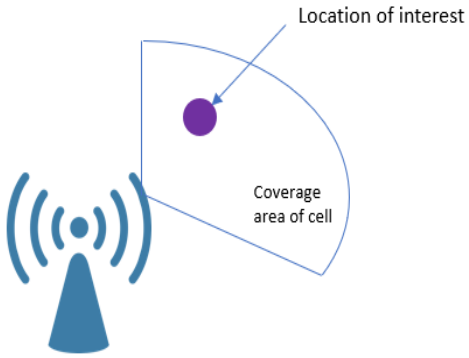

Figure 6: Example of coverage area of a cell

2.1.17 It is often assumed that a mobile device will use the nearest cell site, providing the strongest signal but this is often not the case. There may be instances when the line-of-sight between the device and the nearest cell site is obstructed, by a building or natural feature for example. In such cases, the device may be served by a cell that is not the closest or would ordinarily provide the best quality signal relative to the location of the device.

2.1.18 Additionally, the network operator can employ further factors in the evaluation of the best serving cell beyond the pure signal strength offered by the cells detected by the device. These considerations may result in the best cell not being the same as the strongest cell.

2.1.19 In a similar vein, because the cell sites are located to provide continuous coverage, there is overlap between neighbouring cells. When a device is in an area where there is overlap between two cells it does not necessarily follow that the device will be served by the nearest cell ID.

2.1.20 Furthermore, the cell used to service a particular event may also depend upon the generation of technology in use in an area, 2G (Global System for Mobile Communications or GSM), 3G (Universal Mobile Telecommunications System or UMTS), 4G (Long Term Evolution or LTE), or the currently evolving 5G (New Radio or NR), and the capabilities of the device.

2.2 RF Surveys

2.2.1 Conducting a Radio Frequency Propagation Survey (RF survey) can be used to assist in determining which cells provide service at a geographical location and can also show which cells are most likely to be used or have been used by a mobile device at that location.

2.2.2 There are two main types of surveying equipment used for evidential purposes in the United Kingdom - SIM based equipment and Software Defined Radios (SDR). A SIM based approach will generally measure signals using SIM cards that are each connected to a single network at a time. SIM based equipment is also usually capable of making test calls, texts or data connections. An SDR can be programmed to measure all cells on the air (all networks and technologies) and can provide more granular signalling information.

2.2.3 It is not the purpose of RF equipment (SIM based or SDR) to emulate a mobile device, only to measure the signals propagating from a cell(s).

2.2.4 There are benefits and limitations for each type of RF survey equipment. This document is not intended to list these, but an expert should be aware of the capability of any survey equipment they utilise to assist them in forming an opinion.

2.2.5 RF surveying equipment is essentially a sampling tool which takes measurements of signals being propagated from cells within a mobile network. These measurements are date and time stamped according to the time the signal was recorded along with the GPS location of where the survey equipment was situated when that recording was taken. The information recorded by the surveying equipment can assist the expert in assessing the likelihood of a particular cell providing coverage in a particular area.

2.2.6 The data recorded by the RF surveying equipment can be placed on a map to assist in visualising where the readings were taken of any given cell on a defined route. This process is to assist in presenting the data to a layperson rather than a requirement for the expert to form an opinion of whether a cell could provide service to a location or not. Therefore, it is not mandatory for an expert to include maps in all reports. The decision whether to do so will be made on a case by case basis.

2.2.7 While an RF Survey can confirm coverage in a particular area on the date of the survey, it's important to remember that the network is dynamic and may change over time. A time delay between date of any incident/event and the date of RF survey could mean that the survey measurements may not fully represent the state of the network at the time of the event. Therefore, any RF survey measurements are used, by the cell site expert, as one of a number of considerations when forming an opinion about the coverage of a cell or cells. A survey performed sometime after any critical event may not accurately represent the state of the network at the time of the event.

2.2.8 It is therefore impossible for any survey to be able guarantee that the conditions under which the survey was conducted were also prevailing at the time any event of interest had occurred. This is particularly important to consider where there is a considerable passage of time between the significant events and the survey taking place as even routine maintenance of the equipment at a cell site, such as altering the power output of a transmitter, may have an impact upon the range and area covered by a particular cell.

2.2.9 The results from an RF survey can assist the geolocation expert in forming an opinion on whether a cell site could provide coverage at a given location. If a cell is not detected by an RF survey at a particular location, this does not necessarily mean that the cell did not provide coverage at the time of the incident. The geolocation specialist/expert can use knowledge or other factors to assist in forming this opinion.

3. Limitations of Cell Site Analysis for Geolocation

3.0.1 Geolocation analysis is a recognised and forensically accepted method of geolocating a mobile phone or device to an area.

3.0.2 When using historic call data records or findings from an RF survey as evidence in legal proceedings, it is important to consider the limitations. The findings can be used to show that a certain device, using the mobile telephone network, was in a general area that was capable of being served by specific cell id on that network at a certain point in time. If multiple cells are used within a short time frame, then the overlapping coverage of these cells can narrow down location uncertainty to smaller areas and in some cases this area can be defined to less than 100 metres. The findings can also be used to show that a device could not have been in a location at certain times.

3.0.3 Whilst the results of an RF survey help the expert form an opinion regarding the location of a device at a particular time, they should not be regarded to provide conclusive evidence that at phone could have been at that location. False negative results and both false positive results can arise from the sampling methods used by surveying equipment. As a result, the expert should use results along with experience, knowledge and other referenced material where applicable to help to draw an opinion.

3.0.4 Other, more traditional forms of evidence, such as fingerprints or CCTV evidence should be used to corroborate any conclusions or inferences drawn from the results of geolocation analysis.

3.0.5 It must be made clear to the Court that the arrows, pointers, markers, and other icons, that are used in the various diagrams accompanying cell site reports, are only indicators and not intended to show the precise location of a device that is the subject of any analysis or to infer a location thereof.

3.0.6 Geolocation analysis and RF survey data cannot normally geolocate a mobile phone or device to a specific property or exact location. Other corroborating evidence, for example ANPR, CCTV, Wi-Fi or DNA, can be used in the wider investigation to support a theory that a mobile device had been sited at a particular location.

3.0.7 When a mobile device uses the cellular network for a call, text message, or data session, it can be located anywhere within the service area of the cell. RF survey data can help determine whether a cell's coverage includes a specific location.

3.0.8 It is not the purpose of an RF survey to establish or attempt to establish the full coverage of any particular cell (unless specifically tasked) however the results may indicate the likely extent of coverage of a cell site along the survey route.

3.0.9 The probative value of an RF survey result should be considered when forming an opinion. For instance, a positive result of and RF survey of a cell site, with a notional coverage of 20kms will be of less probative value than a positive result in a cell site of a much smaller coverage area. Similarly, the use of multiple cells with overlapping or near overlapping service areas, within a short time may reduce the area within which a device is likely to have been located.

3.0.10 Geolocation analysis can assist with attribution of a device but cannot place a device in a person's hands or determine who had control at any point in time.

3.0.11 The timings of data connections are known to be ambiguous by nature, in that the time detailed in the CDR cannot always be relied on to be the exact time that a particular cell ID was used by a device. Data from different networks needs to be interpreted in the appropriate manner for the network used and the record format provided. Any report should highlight any instances where these timings create any ambiguity.

3.0.12 For the sake of clarity, only cells identified in the call data records will be commented on in a report, unless otherwise mentioned. Other cells may provide coverage in any of the locations reported on, but if they do not appear in the call data, they cannot be used to investigate the location of a mobile device.

3.1 Colocation & Non-Colocation Analysis

3.1.1 Colocation is a phrase that may be detailed in a report.

3.1.2 Although the word itself indicates that the things examined are together, in cell site analysis terms colocation analysis should be read to mean potential colocation analysis. An expert will also look at the alternative hypothesis in this scenario and consider whether it is more likely that the devices in question were co located or not co located at a specific point in time.

3.1.3 Co-locating devices is undertaken by conducting a series of observations upon the relevant call data records for the devices involved. It is essentially a statistical exercise based upon the timings of events and location of the relevant cells.

3.1.4 Colocation analysis provides an indication of times when two or more mobile devices were recorded as having connected to cells which provide coverage in a similar area, for connections which occurred at a similar time. The analysis does not provide proof that those devices were together only that they could potentially have been together. An indication of potential colocation should not be taken as proof on its own that selected devices were together.

3.1.5 The uncertainty associated with this analysis increases if the call data used includes data sessions, as the correlation between event start times and cell usage is less certain with this type of data.

4. Mobile Phone Networks

4.0.1 There are four licensed mobile network operators in the UK:

a) O2.

b) Vodafone.

c) Hutchinson 3G (Three).

d) EE

4.0.2 Each of these network operators manage cells on thousands of cell sites across the UK. Frequently, to overcome ecological or real estate difficulties, a single cell site location will be shared by cells belonging to more than one network operator.

4.0.3 There are a number of Mobile Network Virtual Operators which operate as separate providers to the consumer, but which use one of the four main operators listed above. The main network operators effectively sub lease their network to these companies, who maintain their own call data records. Examples of these companies include Lyca Mobile, Sky Mobile, Giff Gaff, Lebara, Tesco Mobile. This list is not exhaustive but provides examples of Mobile Network Virtual Operators

4.0.4 Network operators may de-commission a cell site or add a new site to their network. For network planning reasons they may change the cell IDs on an existing site. Additionally, a specific site or cell may be out of service on the day of survey.

4.0.5 The network operators do not automatically report these changes to Law Enforcement Agencies or other interested parties. It may not be apparent from CDRs that any changes have occurred.

5. Supplementary Data Records

5.0.1 In addition to the standard CDRs for calls, text messages and data sessions, O2 retains a further format of records, Device Data Records (DDRs). Vodafone also now provide sub record information.

5.0.2 Call Data Records capture details of billable events that utilise the circuit switched 2G and 3G networks. These consist of calls, text messages and simple multimedia messages (MMS).

5.0.3 Call Data Records also capture details of billable events that utilise the packet switched components of the network systems. These relate to data sessions which can be employed for internet and app activity but also includes Voice Over Internet Protocol (VoIP), Voice Over Long-Term Evolution (VoLTE) calls and Voice over New Radio (VoNR).

5.0.4 Device Data Records (DDRs) and sub records capture details of administrative contact between the device and the network, typically referred to as signalling messages. Signalling messages are generated by several means and offer a method of determining the approximate location of a device even when the device is not actively in use.

5.0.5 For signalling messages to be relayed between the network and the device it is necessary for the device to be switched on and, for those records to be available for analysis, connected to the O2 (DDR) or Vodafone (sub records) networks.

5.0.6 Irrespective of network used, the operation of devices connected to a cellular network is controlled via the exchange of signalling messages. These are administrative messages that allow the device to make connectivity requests and the network to allocate resources for calls, text messages and data sessions.

6. Network Changes

6.0.1 At the time of writing, there are extensive network alterations taking place associated with the installation of cells necessary for the implementation of 5G services and the nationwide removal of cells providing 3G services. For this reason, it is important to highlight the limitations on cell site analysis and RF survey results resulting from these changes.

6.1 Time Elapsed

6.1.1 Any time that has elapsed between the date of the event or offence being considered and the survey undertaken provide the opportunity for network changes to have taken place.

6.1.2 The network operator may change or update the infrastructure of the equipment employed on the network over time. These changes to infrastructure are more likely to occur during the period of transition to a more 5G dominated network with extensive alterations to the available 5G and 3G cells.

6.1.3 One form of maintenance is optimisation and is designed to use minor alterations to the configuration of a cell, to improve the service provided by cells associated with that site. It may also include more extensive changes to the physical properties of a cell, with antenna being replaced, removed, or reorientated to face in a different direction. Research suggests that over a 3 year period a 4G cell site coverage area varies by less than 20% and the majority of this variation is at the cell edge, with the cells inner coverage remaining largely the same.

6.1.4 If changes take place between the time of the event but before the RF survey has been conducted, then the results of the survey may not match the service provided at the time of the event. It is therefore recommended that any proposed survey should be conducted as close to the date of the event as possible.

6.1.5 Although no changes may have been made to the configuration of the cell of interest, the commissioning or decommissioning of other cells in the area may have an effect on the service areas of other cells, possibly including the cell of interest.

6.2 Spectrum Refarming

6.2.1 Differences in the operation of the network may have occurred between the time of the event of interest and the Radio Frequency Survey measurements being generated. These are primarily the result of technology advances and network capacity.

6.2.2 With the limitations on the available frequency spectrum for the broadcast of signals associated with mobile network communications, the provision of sufficient capacity for users on 5G has required the re-appropriation of bands of spectrum previously utilised for other technologies, specifically 3G. This process of reassigning spectrum bands for the use by newer technologies to provide users with a high-capacity faster network experience is termed spectrum refarming.

6.3 Topography

6.3.1 Changes to the landscape in the area are likely to affect signal propagation and therefore the coverage of cells. New buildings, structural or environmental changes (clutter) in the area over time may generated the following effects:

a) Shadowing: Terrain or buildings partially reducing signal.

b) Attenuation: Signal strength reduction resulting from passing through a building or similar structure.

c) Diffraction: The limited bending of the path of a signal around an object that may result in signal at locations that are not in the line-of-sight from the cell.

d) Reflection: Generates interference patterns that may reinforce or reduce signal strength at points within the service area.

6.4 Network Users

6.4.1 Over time a larger number of people may utilise the network within a specific area, or increased numbers of devices may increase the traffic on the network in an area.

6.4.2 Increases in traffic will impact the capacity of cells on the network and the network operator may respond by controlling the throughput of a cell by making alterations that reduce the service area of the cell.

6.5 Serving & Neighbour Cell Considerations

6.5.1 At any point a mobile device in idle mode will only select one serving cell for paging and connectivity. The cell used is influenced by the number of detected cells, strength and quality of their signals and network-defined offsets.

6.5.2 Neighbour cells can be included on survey files of the main hardware providers of surveying equipment. They are usually ranked in the order in which they can be selected by the device.

6.5.3 Taking into consideration signal strength and more importantly signal quality, a cell ranked as the first neighbour (N1), or lower ranks in some cases, may have the capacity to be a serving cell at that location at specific points or in the absence of the detected serving cell.

6.5.4 The Neighbour Cell List (NCL) is used to control cell measurements by mobile devices to enable efficient use of network resources and allow connection continuity when cells are reselected during move in connected mode. Reselection, especially when the device is utilising network resources, is known as handover.

6.5.5 The list of neighbour cells is provided by the network and used by the device to monitor the signal quality of potential handover candidates and preferentially rank them according to suitability. This ensures that any mobile in the serving cell area can find one or more alternative cells that can be used when the serving cell signal deteriorates.

6.5.6 The resulting mobility performance is used to avoid calls being dropped and to limit periods where the device has no service.

6.5.7 During a call, the mobile device will report back to the network the neighbour cell calculations. This enables the network operator to ensure the best cell can be allocated for handover during a call, both to ensure the continuation of the connection and to balance the distribution of traffic load across the network resources.

7. Theoretical Cell Ranges

7.0.1 There are many factors that can affect the coverage of a specific cell.

7.1 2G

7.1.1 The maximum theoretical range of a 2G cell is thirty-five kilometres. In theory, a cell in a rural setting with no obstructions, man-made or natural may be detected at that extreme distance but other cells would be expected to provide better service, and this range would not be seen in the field.

7.1.2 Communications beyond thirty-five kilometres would be prevented as timing issues would make it impossible to synchronise communications between the phone and the cell site, unless the cell site was deliberately using double-length timeslots associated with an extended range cell site.

7.1.3 Extended range 2G cells were originally employed to provide offshore service in coastal areas where the lack of landmass, and relatively low network traffic, made the deployment of additional cell sites impractical.

7.2 3G, 4G & 5G

7.2.1 The range of cells on more recent technologies, 3G, 4G and 5G are not, generally, limited to a physical distance by the timeslots employed in 2G network implementation.

7.2.2 This infers that, assuming a sufficiently high-powered antenna and the absence of any obstructions, these cells would be able to provide service over any range. Practically however, the power output and level of network traffic (noise) make the use of smaller cells more appropriate, and, with each generation of network technology, the typical range of cells has reduced.

7.3 General

7.3.1 The range of a cell is directly related to the number of cell sites deployed in that area which, in turn, is related to the volume of mobile device traffic expected in that area.

7.4.2 A single powerful cell in a dense urban area could be set-up to attract all devices on the network in the area to connect to it. This would result in the capacity of that cell being reached and further users being unable to obtain the quality of service necessary to utilise their devices.

7.4.3 Therefore, network operators deploy more cells over areas of dense population or high network traffic and reduce the power of individual cells to provide a better quality of service over the area through multiple cells with smaller individual ranges.

7.4 Typical Cell Ranges

7.4.1 There are four main cell types and one emerging cell type employed by the network operators and the coverage capabilities of these vary widely:

a) Femtocells: The appearance of a femtocell is often like a Wi-Fi router or signal booster plug. Generally, they are deployed indoors, however they may be deployed outside if required. A typical range would be ten to twenty metres.

b) Picocells: If deployed indoors, picocells can be found in shopping centres, airports etc. and have a typical range radius of twenty to thirty metres. Their appearance is like an industrial Wi-Fi extender and normally found on ceilings or other elevated structures. Outdoor picocells can provide coverage up to around five hundred metres.

c) Microcells: Deployed at outdoor sites, these typically have a coverage area of five hundred metres to one kilometre and normally deployed to cover a particular area of high network traffic.

d) Macrocells: Deployed at outdoor sites. Coverage and range vary widely and is dependent upon many factors. It can be as little as half a kilometre but can be significantly more in a rural area and includes the largest cells deployed on the network.

e) 5G small cells: These are beginning to emerge in the network and will become more prevalent as the national rollout of the 5G network.

7.4.2 It is impossible to specify, or predict, the precise range that any cell may cover, or have covered, at any time based upon any knowable, tabulated characteristics of that cell, but a very broad and very general guideline may be assumed:

a) Macrocell 1-20 kilometres.

b) Microcell: 500 metres to 1 kilometre.

c) Picocell: 20 to 500 metres.

d) Femtocell: 10 to 20 metres

e) 5G small cells: Small cell coverage is likely to support coverage between 10 metres and 500 metres, but typically will support shorter ranges (sub 100 metres).

7.4.3 These ranges are typical examples and examples have been surveyed of cells that provide service at distances away from the respective cell site in excess of those indicated and cells that failed to provide service at the distance indicated despite expectations.

7.5.4 These ranges are an approximate guide and should not be referred to in evidence.

8. Change in Cell During a Call

8.1 When a device is in idle mode, a state where the device is not actively engaging in any user activity, such as a call, it will monitor the network.

8.2 With 2G, the device will be aware of the strongest cell, subject to network operator offset factors, and the next best six neighbouring cells.

8.3 With 3G, the device will be aware of the most favourable signal but not necessarily the strongest. This is due to 3G being designed to use a signal that will provide the best quality of service for the device.

8.4 When a mobile device is used, either to send or receive a call or text message, or connects for a data session, it must send a signal request to the network. This is a validation process designed to take place between the device and the network and ensures there is a good path for communication.

8.5 For the purposes of call data records, the start cell ID will be recorded at this point, except for data session records on the O2 and EE network.

8.6 In Call Data Records (CDRs) for voice calls it is not uncommon for the record to include a start cell ID and an end cell ID. On occasion these will be the same but at other times they will differ and there are several reasons why this may occur. The following are typical examples:

a) The device has moved, due to the user being in a vehicle or travelling on foot, over a distance that cannot be covered by the start cell ID. The call is handed over to a different cell one or more times as the journey progresses. Only the start and end cell IDs will be recorded in the CDRs.

b) The device remains stationary, but changes in external factors, such as moving objects blocking the signal or changes in device orientation, cause a significant difference in signal quality, making another cell preferable for the connection.

c) The start cell ID is near to or has reached its capacity and the network determines the need to hand the call to another cell, which then appears as the end cell ID in the call data records.

8.7 These are typical examples and in reality, once connected, the network largely controls the traffic and cells utilised by mobile devices at times using proprietary algorithms which are not known.

8.8 In general, networks look to avoid handing off calls as this will increase the possibility of poor quality of service and potentially dropped calls. The networks will continue to monitor cell usage and if a cell nears capacity, they will transfer users to other cells or technologies on the same cell site or identify cells that are suitable candidates for the early hand-off of users.

8.9 Large scale events, for example festivals, pop concerts and sporting events, can also cause a rise in demand for the network and hand-offs may occur more frequently. In the case of such events where it is possible to predict a temporary increase in network activity, the networks may install temporary cells on wheels (COW) that will increase capacity in the area during such events.

8.10 As the circumstances dictating when a hand-off may occur are unpredictable, and not recorded in the call data records, RF Surveys can potentially determine where geographically a handover point may be but will not be able to discriminate when this occurred.

8.11 4G technology works in a very similar way as 3G as it will select a cell based on signal quality, however it uses different measurement criteria. The device will search for the strongest cell initially and select it, but when one or more cells have been detected it will choose the cell with the highest quality signal. Reselection of a cell is triggered when the cell drops below the broadcast minimum value, for example as the device is moving around an area.

8.12 Both 3G and 4G technologies utilise a system called an active set. Rather than the hand-off being a clean switch from one cell to another, the device will utilise signal from multiple cells to retain service quality while in the hand-off process. If a call is terminated while in the active set state, only the primary cell, typically the cell in use before entering the active set state, will be recorded in the CDRs and there will be no means of identifying the active set state of the connection.

9. Topography

9.0.1 The radio frequencies associated with mobile networks and mobile devices are generally accepted as travelling in straight lines, so topography and the line-of-sight of a cell site will have some effect the coverage of a cell.

9.0.2 Any elevation profiles included in the accompanying report are based upon the ground-level. This does not include other obstacles, natural and man-made, that might interfere with the signal path.

9.1 Buildings / Man-Made Structures

9.1.1 If a radio signal is obstructed by a building, and dependent upon the constitution of the building, some of the signal energy will be absorbed by the building resulting in attenuation of the signal.

9.2.2 Despite the network signal being attenuated by buildings, servicing coverage can still be achieved, if a signal is strong enough to maintain quality. Other factors such as refraction and reflection also help to achieve serving coverage within buildings.

9.2.3 A sufficiently strong signal may be attenuated by a building and still provide usable signal beyond the far side of that building.

9.2.4 Additional signal energy may be reflected by the building causing multipath propagation.

9.2.5 Multipath propagation may lead to constructive and destructive interference:

a) Constructive interference will enhance the signal and may result in hotspots of service.

b) Destructive interference will erode the signal and may cause black spots within the service area of the cell

9.2.6 Signal reflection may also enable the signal to travel round corners creating areas of service that are not in the line-of-sight of the cell site.

9.2.7 In some cases, a location of interest may be at elevation, such as an apartment on an upper storey of the building. On these occasions, it is preferable for the surveyor to have obtained access to those elevated areas as the survey measurements may identify additional or different cells than those observed by ground level surveying.

9.2.8 A typical one or two storey building would see little change in cells surveyed compared with survey measurements generated outside the property.

9.3 Changes

9.3.1 There can be changes to the man-made aspects of the topography between the time of the incident and the date of the survey.

9.3.2 The most obvious to observe, and most likely to influence cell service areas, is the construction or destruction of a building around the area of interest.

9.3.3 Scaffolding may generate signal reflections that differ between the incident and survey if it has been installed or removed in the meantime.

9.3.4 Cranes and their orientation on the skyline may alter the service areas associated with cell sites at elevation in the area.

9.3.5 A large vehicle, such as a double decker bus or a lorry, may obstruct cell signals. Under normal circumstances, the survey will occur over a sufficiently long time to generate measurements after the vehicle has moved, unless parked. However, an obstruction present at the time of the incident cannot be identified or replicated in the survey measurements.

9.4 Natural

9.4.1 Foliage on trees in a wooded area may seasonally affect the coverage of cell depending upon the frequency utilised by the cell. This may be a consideration depending on the locations of interest and the time of any associated event.

9.4.2 Precipitation, either rain or snow, may create reflective surfaces that could have a limited effect on the service area of cells.

10. Call Forwarding & Voicemail

10.0.1 When a device is unable to receive a call, this may result in the call being diverted to Voicemail. There are several reasons why this may occur including, but not necessarily limited to:

a) The receiving device is on another call.

b) The receiving device is in an area with no coverage.

c) The receiving device is switched off.

d) Divert is enabled on the receiving device.

10.1 Call Forward

10.1.1 Outgoing calls from the calling party will only show as a Call Forward if the called party is on the same network as the calling party.

10.1.2 The CDRs for the outgoing party will show the outgoing call and a Call Forward record, although these may be combined into a single line in the CDRs. This is due to the call being captured by both the billing system and the Voicemail platform of the common network operator.

10.1.3 However, should an outgoing call be made to a number on a different network there will only be an outgoing call recorded in the CDRs.

10.1.4 Zero second calls shown within CDRs are usually the result of the calling party disconnecting the call without leaving a message.

10.2 Voicemail

10.2.1 The records for the recipient of the diverted will identify the event with a Divert/Voicemail record.

10.2.2 CDRs may identify the telephone number or service number associated with the target of the re-direction of the call. This may be the Voicemail service but may also be another telephone number assigned by the user, such as a number associated with a secondary phone.

10.2.3 Should it be important to establish if a call was diverted to Voicemail, then it would be necessary to apply for CDRs for the recipient of the call that include details of the target of the diverted call.

11. Data Sessions

11.0.1 Devices that can connect to the internet do so with or without any interaction from the user.

11.0.2 Activity without user interaction can occur through notifications, automated app updates and other data communication to the device. The device may also be set-up to make requests to the network, such as hourly email checks, that occur without the interaction or presence of the user.

11.0.3 General Packet Radio Service (GPRS) is a term used to refer to a data communication session used by a device on a mobile communications network using 2G or 3G technology. As mobile networks evolve to purely IP networks in 4G and 5G these data communications are now referred to as data sessions or IP sessions.

11.0.4 Most mobile phones in use in the UK today are smartphones which can run advanced services utilising data connections. This type of connection relates to data connectivity for devices which are browsing the Internet, connecting to an email service, or carrying out some other function which involves a data connection.

11.0.5 A data session differs from a voice call in that the network does not set-up an exclusive end-to-end physical connection for a timed period as the user is generally charged by the amount of data they have used and not for the duration of the call.

11.0.6 This connectivity creates a virtual data pipe between the network and the device and is frequently in an always-on state. So, the connection to the internet and network functions is maintained even when the device is not performing any specific action.

11.0.7 This always-on data pipe enables applications such as email programs to query the network for incoming emails at regular intervals or allows for instant messaging clients on the device to receive incoming messages.

11.1 GPRS and Data Session Records

11.1.1 Due to the way in which a data event occurs, GPRS and data session records need to be interpreted differently to voice call and text message records. With a voice call or a text message, the time in the call data record shows the time at which the event happened, and the corresponding cell used at that start time, and end time with respect to calls.

11.1.2 GPRS and data session records are not generated in the same way and often multiple records relate to a single ongoing data connection.

11.1.3 An ongoing data connection is frequently identified through the duration timings of the individual records. A record starting at or within a couple of seconds of the termination time of a previous entry can be the continuation of the same network connection.

11.1.4 Additionally, some records include a session charging ID which remains consistent across all records relating to the same continuous data session.

11.1.5 Depending upon the location of the cell and duration of the record, there may be the opportunity for extensive movement of the device from the service area of the cell shown by the time of the record.

11.1.6 The exact method of generating records for GPRS or data sessions, vary between network operators and can vary over time for a single operator.

11.1.7 The following sections details the network operators and the accurate interpretation of GPRS records generated by their systems.

11.2 Vodafone and Three

11.2.1 The time shown for each record indicates the generation of a new record on the network database. This record may be the initiation of a new data session connection or the continuation of an ongoing session.

11.2.2 The cell shown in relation to each record is recorded at the time the record starts. This may not be a cell associated with the location of the device at the time of the record, merely the last cell used by the device for data transfer prior to the start time recorded.

11.2.3 Depending upon the cause of the creation of the new records, the cell usage may coincide with the timing of the GPRS or data session record.

11.2.4 The following wording should be generically used in relation to the association between the timing of GPRS or data session records and cell information provided:

a) The device was within the service area and connected to the cell at or before the time of the record and after the start time of the ongoing connection entry with a different cell. This can also be simplified for ease of understanding to simply read ‘At some point between time x and time y.’ The concept from above is still the same.

11.2.5 Where the record is the first or only record for a continuous data session this equates to at the time of that record. This may be determined either by a new charging ID or a significant gap, about ten seconds or more, since the termination of all ongoing session records.

11.2.6 Additionally, when the connection to the network systems switches between technologies, typically 3G to 4G or 5G to 4G and visa-versa, the retuning of the transmitter in the device means that the new cell could not have been connected to prior to the timing of the new record. As a result, a change of technology is another example of an occasion when the terminology at the time of the record can be used.

11.3 O2 and EE

11.3.1 Despite referring to the cell associated with a GPRS or data session record as being the start cell, O2 and EE records indicate the last cell utilised during the part session recorded.

11.3.2 The following wording should be generically used in relation to the association between the timing of GPRS or data session records and cell information provided:

a) The device was within the service area and connected to the cell at or before the end time of the record and after the start time of the first consecutive ongoing connection entry with the same cell. Again, this can also be simplified for ease of understanding to simply read ‘At some point between time x and time y.’ The concept from above is still the same.

11.3.3 Where the record is the first or only record for a continuous data session this equates to at or before the end time of the record and after the start time of that record.

11.3.4 Historically EE did report in the same way as Vodafone and Three in as much as it recorded start times and start cells for data sessions. This changed to end time and end cell recordings, due to hardware replacement which was completed in early 2024. As a result historic CDR records for EE may need closer inspection to ensure the correct cell and time is being reported.

12. Stacked Cells

12.0.1 Two or three cell IDs on the same cell site are often used to provide service in the same area, allowing many phones to access the network simultaneously. They all share the same antenna orientation, frequency band, technology and provide similar coverage.

12.0.2 These are often called stacked cells and each cell in the stack has a separate cell ID.

12.0.3 A device will only access one cell, or member of a group of stacked cells, at any one time. It is therefore possible for a device to use different cells within the stack on different occasions when at the same location.

12.0.4 This means it is possible for some Radio Frequency Survey equipment to select a different cell in the stacked group to the cell ID shown in the Charging Detail Records (CDR). This is prevalent when using SIM based equipment.

12.0.5 When the Radio Frequency Survey equipment has measured multiple cells from a stack, each cell ID will be listed individually in the report. When the Radio Frequency Survey equipment only measures one of the cells from a stack and a different cell appears in the CDR, it may be inferred that those stacked cells would be expected to have similar service areas.

12.0.6 CDRs for the O2 network occasionally include Service Area Code (SAC) values instead of cell IDs.

12.0.7 A SAC value is used to denote the use of one of the cells associated with that stack. A SAC will relate to 3G cells and typically is associated with a stack of two cells, although examples with other numbers of cells are not uncommon, including occasions where a single cell has become the only cell connected to a SAC.

12.0.8 O2 are unable to determine which cell, of those associated with the SAC, was used for the record. However, they maintain a database, accessible to specific members of Law Enforcement Agencies, called SortCeller that enables the user to query the O2 network setup. This includes input of the Location Area Code (LAC) and SAC provided in the CDRs to determine the cell IDs of the cells associated with the stack.

12.0.9 The cell IDs associated with each SAC need to be obtained from O2 for survey and reporting purposes and are shown together in the report. Where there are two cells associated with a SAC value they can be written as cell IDs 11111 and 22222 or cell ID 11111_22222.

12.0.10 Unless there is information to suggest to the contrary, it is deemed acceptable by experts that stacked cells in the same frequency band, transmitted from the same site and sharing the same azimuth will provide similar coverage. It should be noted that each technology, 2G , 3G , 4G and 5G , has multiple frequency bands that may be available for use by the networks, so cells on a common technology from the same site and azimuth may provide significantly different coverage.

13. Glossary

2G – Global System for Mobile Communications – Mobile phone system used primarily for calls and text messages. Capacity was reduced to enable frequencies to be used for later generations of technology, primarily 3G. Cell IDs limited to sixteen bits, equivalent to four hexadecimal characters or decimal values between 0 and 65535.

3G – Universal Mobile Telecommunications System – Third generation mobile telephone technology introduced for better data handling capabilities than previous system. Introduced the concept of utilising packet switched data handling for calls in the form of VoIP. Cell IDs limited to sixteen bits, equivalent to four hexadecimal characters or decimal values between 0 and 65535.

4G – Long Term Evolution – Cells referenced by combining the ENodeB and Cell ID or ECI format. Enhanced Cell IDs of up to twenty-eight bits, equivalent to seven hexadecimal characters or decimal values between 0 and 268435455.

5G – New Radio – The most recent generation of telephone communication technology with the highest data throughput rates. Implementation means that data combines 4G and 5G cells simultaneously. Currently, the primary cell in this process is an 4G cell and this cell is detailed in the CDRs. As 5G NSA continues to be rolled out, 5G cells will become more prevalently recorded in CDRs.

ARFCN (Absolute Radio Frequency Channel Number) - In 2G cellular networks, an absolute radio-frequency channel number (ARFCN) is a code that specifies a pair of physical radio carriers and channels used for transmission and reception.

Attenuation - The decrease in the strength of a signal due to absorption and the redistribution of energy by objects i.e. buildings

Azimuth – Direction an antenna is pointing, displayed in degrees, clockwise from due north. Figure 3, in Section 1 of this technical appendix, illustrates this.

Base Station – The equipment housed at a cell site that enables connection through a network utilising the 2G technology. Analogous to a NodeB and eNodeB on 3G and 4G networks respectively, although the technical processes undertaken by the different equipment types varies significantly.

Call Detail Record (CDR) – A record of circuit switched usage provided by the network operator, originally maintained to bill the customer for the number of text messages sent and the minutes of call time used. It records details of the usage of a specific mobile device.

b) A record of packet switched usage provided by the network operator, maintained to bill the customer for the volume of uploaded and downloaded data used. It records details of the usage of a specific mobile device.

Call Event – An event that had triggered an entry in the CDR.

Cell Global Identifier (CGI) – The CGI provides each cell with a fully unique global ID. This allows an individual cell to be identified across all technologies globally. The structure of the CGI differs for each mobile technology: 2G CGIs consist of MCC-MNC-LAC-CI, 3G CGIs consist of MCC-MNC-RNC-CI and 4G CGIs consist of MCC-MNC-eNB-CI.

Cell ID (CI) – An identifier given to a cell by the network, unique within the grouping area. It is normally presented as a decimal value. The range of cell ID values depends upon the technology utilised with technically fewer values available for 4G cells, although the Enhanced Cell ID is referred to as the cell ID in most cases. Some cell IDs may be reserved for specific network usage rather than relating to physical cell installations.

Cell Site (or Cell site)– A location owned or rented by a network operator to place their equipment. Within the network architecture, the cell site is the location of the equipment named the Base Station, NodeB or eNodeB depending upon whether considering a 2G, 3G or 4G system respectively.

Cellular Service Provider (CSP) – Formal term for the network provider, includes MNOs and MVNOs.

Circuit Switched – A network that creates a dedicated resource that connects two devices, typically for a call between the parties. The data transmission rate is fixed, and the resource cannot be shared by multiple users or functions. Utilised in 2G communications.

Connected Mode – The state a mobile device is in when a connection has been established to a base station and traffic flow is possible. Device not in Idle Mode.

Dedicated Mode – Original term for Connected Mode used in 2G.

Device Detail Records (DDR) – A record of data produced by the network operator relating to non-billable paging and events. Suitable database only maintained by O2.

Enhanced Cell ID (ECI) – Format of cell ID employed on 4G networks. Consists of the eNodeB and Cell ID components of the CGI.

eNodeB (eNB) – The equipment housed at a cell site that enables connection through a network utilising the 4G technology. Analogous to a Base Station and NodeB on 2G and 3G networks respectively, although the technical processes undertaken by the different equipment types varies significantly. A component of the CGI on 4G networks.

FDMA (Frequency Division Multiple Access) - FDMA gives users an individual allocation of one or several frequency bands, or channels. Multiple Access systems coordinate access between multiple users. The users may further share access via additional methods such as TDMA.

General Packet Radio Service (GPRS) – A packet switched mobile data standard used in mobile communication networks. GPRS was established by European Telecommunications Standards Institute in response to the earlier, less efficient, standards for mobile data communication networks.

Handover – The process of passing the active connections for a mobile device in Connected Mode from one cell to another.

Idle Mode – The state where a mobile device is powered on and attached to a network but has no active control or traffic connections. Device not in Connected Mode.

Integrated Circuit Card Identifier (ICCID) – The identifier of the Universal Integrated Circuit Card (commonly known as the SIM card). This card holds the Subscriber Identity Module (SIM) software and it typically also engraved or printed on the SIM card body.

International Mobile Equipment Identity (IMEI) – 15-digit electronic serial number which is held in the memory of a mobile device. This is displayed in the call data records or billing data and is a digital identifier for a mobile device.

International Mobile Subscriber Identity (IMSI) – A unique number identifying a subscriber. This number is stored on the SIM and allocated to the subscriber when that SIM is purchased. It is used to identify the subscriber by the CSP and differs from the MSISDN.

Location Area Code (LAC) – A component of the CGI on 3G or circuit switched networks. This code assists with network management and reduces the area within which a paging message is broadcast with the network needs to contact the device. This value is a five-digit number.

Mobile Country Code (MCC) – A component of the CGI in all technologies. Identifies the country of the network upon which a cell is located. In the United Kingdom, the value is 234.

Mobile Network Code (MNC) – A component of the CGI in all technologies. Identifies the MNO that maintains the cell site associated with the cell. In the United Kingdom, this value is a two-digit number.

Mobile Network Operator (MNO) – A CSP that provides connectivity to subscribers through cell sites maintained by that network operator. The four MNOs in the United Kingdom are O2, Vodafone, Three and EE.

Mobile Station – Cellular device, typically a mobile phone, used by subscribers to connect to the mobile network. This is the terminology used for a 2G network. On 3G and 4G systems the term User Equipment is used.

Mobile Station International Subscriber Directory Number (MSISDN) – This is a number used to identify a mobile phone number internationally. Formal name for the telephone number. Some mobile phones enable a value stored under the name MSISDN to be changed. Changing this stored value on the handset has no effect on the actual MSISDN.

Mobile Virtual Network Operator (MVNO) – A CSP that does not own the network infrastructure used to provide service to customers. Utilises the infrastructure of an MNO to provide services to subscribers. Examples in the United Kingdom include giffgaff, Lycamobile, Virgin Mobile and Tesco Mobile.

Multi Messaging Service (MMS) - Also referred to as picture messaging, MMS works much like text messaging but with a greater capacity so you can send larger quantities of text as well as attaching images and audio files from your phone.

NodeB – The equipment housed at a cell site that enables connection through a network utilising the 3G technology. Analogous to a Base Station and eNodeB on 2G and 4G networks respectively, although the technical processes undertaken by the different equipment types varies significantly.

Packet Switched – A network that groups and sends data in the form of small packets. It enables the sending of data or network packets between the mobile device and the other party, either a recipient device or the internet, over a resource that is potentially shared between multiple users. Utilised for data communications.

Radio Network Controller (RNC) – A component of the CGI on 3G networks. This code assists with network management and reduces the area within which a paging message is broadcast with the network needs to contact the device. This value is a five-digit number.

Roaming - If you use your mobile outside your network operator's local coverage area, you are said to be 'roaming'.

Received Signal Code Power (RSCP) - Indicates the RF signal strength of the pilot channel measured at a receiver. This value is typically displayed as a negative value and in decibel Milliwatts (dBm). 3G signals are measured using RSCP.

Reference Signal Receive Power (RSRP) - Indicates the average RF signal strength of the Resource Elements (RE) measured at a receiver. This value is typically displayed as a negative value and in decibel Milliwatts (dBm). 4G signals are measured using RSRP.

Received Signal Strength Indicator (RSSI) - Indicates the RF signal strength of the beacon signal measured at a receiver. This value is typically displayed as a negative value and in decibel Milliwatts (dBm). Both 2G and Wi-Fi signals are measured using RSSI.

Synchronisation Signal Reference Signal Receive Power (SS-RSRP) - Indicates the average RF signal strength of the secondary synchronisation signals measured at a receiver. This value is typically displayed as a negative value and in decibel Milliwatts (dBm). 5G signals are measured using SS-RSRP.

Service Area Code (SAC) – A system available within the network operation specifications to group multiple 3G cells with a common cell site and azimuth. Only utilised by O2.

Subscriber Identity Module (SIM) - The SIM is software which is held on the Universal Integrated Circuit Card (commonly known as the SIM card). It identifies the user account to the network, handles authentication and provides data storage for basic user data and network information.

Short Message Service (SMS) - Text messages of up to 160 characters to be sent and received via the network operator's message centre to a mobile handset

SortCeller – Cell ID location report and electronic database used to identify and obtain additional information about O2 cells. Primarily used to identify the cell IDs associated with a SAC and the corresponding LAC.

Stacked Cells – Typically, two or more overlapping cells on the same technology, 2G, 3G, 4G or 5G, and providing coverage to similar areas using the same power level and transmitted via the same antenna, resulting in the same azimuth. Used to increase network capacity.

Sub Records – A record of paging and signalling messages relating to 4G data sessions in the Vodafone network.

User Equipment (UE) – Any device used directly by a network user to communicate over that network. It can be a mobile phone, a cellular capable tablet, or any other device using a SIM card to provide a data connection. On 2G systems the term Mobile Station is used.

Wideband Code Division Multiple Access (W-CDMA) - The underlying air-interface within a 3G system, using a pair of 5 MHz-wide radio channels for uplink and downlink transmission. W-CDMA supports voice, very high-speed multimedia services such as full-motion video, Internet access and video conferencing. W-CDMA transmits on a pair of 5 MHz-wide radio channels

14. Reference Documents

Document Name	Document Number	Responsible Department
MG22A	SFR MG22A	FCN Science Directorate
MG22B	SFR MG22B	FCN Science Directorate
MG22C	SFR MG22C	FCN Science Directorate
MG22D	SFR MG22D	FCN Science Directorate
SFR Annex	SFR2 Annex	FCN Science Directorate
Case Management Risk Form	SFR Case Management Risk Form	FCN Science Directorate
National Guidance for Streamlined Forensic Reporting	FCN-MGT-GUI-0003	FCN Science Directorate