# Technical Briefing

## RFPS:

## Scanners vs Test Phones

01674-BRF

v2.0

September 2018

Martin Griffiths & Joe Hoy

Forensic Analytics

Communications Data Experts

# Contents

## 1. Executive Summary

RFPS (Radio Frequency Propagation Surveys) provide tangible evidence that quantifies the area in which a handset may have been located when a call data record was generated by the network.

Location surveys capture details of the cells that provide coverage at a significant location and usually attempt to determine which of those cells would be used by a phone making a call at that location. RF Surveys can also be used to show the service area of a cell, although it is worth acknowledging that RF survey data only provides evidence of the coverage provided by each surveyed cell on the date and at the time that the survey data was recorded.

RFPS test devices can be divided into two main types – test phones (or devices that emulate phones) and scanners.

A test device that emulates a 'normal' phone, or that is in fact a normal phone, operates using the same processes as a mobile phone – they take signal strength measurements of local cells and apply the same 'cell selection' algorithms (C1/C2 or S/R algorithms) on those measurements that a phone would apply. This means that a phone-based survey device is making the same types of cell selection decisions as the suspect mobile phones that are being investigated. Given that the role of an RFPS report is often, although not always, to answer the question 'could this call have been made from there?', then conclusions based on results that emulate the actions of the subject phone are going to be of more value than conclusions based on results obtained using other methodologies.

A scanner is generally a passive device which captures a wide area of radio spectrum, covering multiple radio bands and technologies, in one pass and measures the received signal strength of cells it detects in those bands. A traditional scanner, because it is merely detecting cellular signals and recording their strength, is therefore only gathering information about the detectability of surveyed cells and has nothing to say about their actual usability.

We were recently asked to provide an opinion in relation to RF Survey methodology and data interpretation in a case where the prosecution RFPS practitioner had used a 'phone emulator' type survey device and the defence expert had used a scanner-based device to undertake RF surveys. The resulting reports presented cellular service area maps which offered significantly different service areas to each other and we were asked to comment on the reasons for the wide disparity between the results.

In this report, we conclude that there is nothing inherently wrong with using traditional scanners as part of a validated RFPS survey methodology. Scanners have the potential to massively improve the speed and efficiency of RFPS surveys and will become invaluable survey tools as the range and complexity of the surveyed spectrum increases.

However, the interpretation of measurements obtained exclusively from traditional scanner-based survey devices, combined with an arbitrary 'minimal usable signal strength' level, to compile RFPS maps and reports which seek to show the serving potential of key cells, is a flawed methodology. If employed, this methodology has the potential to produce inaccurate and misleading results that can lead to similarly inaccurate and misleading conclusions.

## 2. RFPS: Scanners vs Test Phones

We were recently asked to provide an opinion in relation to RF Survey methodology and data interpretation.

The request related to a specific example in a case where the prosecution RFPS practitioner had used a 'phone emulator' type survey device and the defence expert had used a scanner-based device to undertake RF surveys. The resulting reports presented cellular service area maps which offered significantly different service areas to each other.

We were asked to comment on the reasons for the wide disparity between the results of the RF surveys undertaken by or on behalf of the prosecution using a 'phone emulator' and the RF surveys undertaken by the defence using a scanner.

RF Surveys provide tangible evidence that quantifies the area in which a handset may have been located when a call data record was generated by the network – this evidence is compiled on the basis of the cellular utilisation records combined with a set of RF Survey results. RF Surveys can also be used to show the service area of a cell, although it is worth acknowledging that RF survey data only provides evidence of the coverage provided by each surveyed cell on the date and at the time that the survey data was recorded.

It is always more helpful to the court if prosecution and defence can find common agreement on their RF Survey results. This is only possible however if the methodologies adopted by both parties are similar. Should the methodology or data interpretation employed by the two sides be significantly different, then common ground may not be achievable and the court will have to be furnished with the reasons for this.

### Survey Methodologies

RF Surveys can be undertaken in passive or active/connected modes.

Passive simply means that a mobile device is in an idle condition – passively measuring the signal strength and quality of the signals received from the network and recording them. If this test is undertaken by test equipment that is or that emulates a mobile device, then that device will be able to move around a network reselecting cells in the same way that a 'normal' mobile device would. This is how the test and monitoring equipment devices most commonly utilised by UK law enforcement (CSurv, Forensic Compass or NEMO) operate.

An active/connected mode survey requires the network monitoring equipment to generate a call, a text message or data traffic over a network connection and records which cell actually carried the traffic. Whilst there are arguments for and against active/connected mode surveys and test calls, in the opinion of many practitioners, a test call can be the acid test in determining which cell(s) would actually carry traffic at a specific location – something that Idle mode only surveys will often struggle to determine, especially at locations that enjoy strong coverage from several cells.

Tests calls aren't always required or appropriate, though, and their use often needs to be judged on a survey by survey basis.

We employ a mix of idle and connected mode survey techniques in our surveys – the mix of results obtained allows us to differentiate between the usable coverage 'service area' of a cell versus the much wider area of cell detectability. Both of these concepts are described below.

Service Area – the area within which a cell is detected as dominant over all others from the same network all or some of the time. It is the area within which that cell is likely to be selected as the cell a mobile device will attempt to use when asked to establish a connection.

Cell Detectability – an area within which a signal can simply be measured as providing a signal, whether that signal is the dominant one or not. This usually includes areas beyond the cell's service area in which it is still detectable but is not the strongest or 'serving' cell. Knowledge of the area within which a cell is detectable is of less evidential benefit than knowledge of the area within which that cell serves.

## Test phones vs scanners

RFPS test devices can be divided into two main types – test phones (or devices that emulate phones) and scanners.

A test device that emulates a 'normal' phone, or that is in fact a normal phone, operates using the same processes as a mobile phone – they take signal strength measurements of local cells and apply the same 'cell selection' algorithms (C1/C2 or S/R algorithms) on those measurements that a phone would apply. This means that a phone-based survey device is making the same types of cell selection decisions as the suspect mobile phones that are being investigated. Given that the role of an RFPS report is often, although not always, to answer the question 'could this call have been made from there?', then conclusions based on results that emulate the actions of the subject phone are going to be of more value than conclusions based on results obtained using other methodologies.

The cell selection algorithms enable a phone-based (phone emulator) survey device to determine which of the currently detectable cells should be classed as the 'serving' cell, and which should be classed merely as 'neighbour' cells. The serving cell is the cell a phone would choose to use if asked to establish a connection, a neighbour cell is any other that is currently detectable but hasn't been selected as the serving cell. The serving cell isn't always the strongest cell, as the subtleties of the selection algorithms allow some cells to be deliberately deprioritised as serving cells.

Test calls, as mentioned above, help to reinforce the evidence related to serving cells that is gathered from idle mode surveys – when asked to make a test call, a phone emulator survey device employs the same cell selection routines as a normal phone and chooses the cell that it calculates will provide the best service *at that point in time*. In areas where there may be a choice of serving cell, as there are several cells with roughly equal received signal strengths, a series of test calls can establish whether there is just one serving cell (an area of 'dominance') or several serving cells over time (an area of 'non-dominance'). This is particularly useful in areas where there are several strong cells, which *could* all serves, but where some of them have been deliberately deprioritised by the network and don't actually serve.

A scanner is generally a passive device which captures a wide area of radio spectrum, covering multiple radio bands and technologies, in one pass and measures the received signal strength of cells it detects in those bands. The 'generally' comment was inserted into the previous sentence because

there are now a growing number of 'hybrid' scanners, which can take cell selection algorithms into account and which will be described later in this overview.

Although traditional scanners may read the broadcast messages transmitted by cells, which enables them to capture the 'cell ID' for each surveyed cell to append the signal strength measurements to, they are generally not able to react to the content of those broadcast messages in the same way that a mobile device or the equipment that law enforcement utilise would. This is the fundamental difference, as the broadcast messages from the network play a part in determining the service area of a cell.

A traditional scanner, because it is merely detecting cellular signals and recording their strength, is therefore only gathering information about the detectability of surveyed cells and has nothing to say about their actual usability. There is nothing inherently wrong with this mode of operation, by the way – scanners are generally designed to be used by a network's test drive engineers to gather information about the geographical area that particular cells provide coverage over. Traditional scanners aren't designed to provide information about the geographical area in which a particular cell *serves*, which is the key difference between them and phone emulators or hybrid scanners.

The Rohde and Schwarz TSME drive test scanner, as an example, can record the signal strengths of the current strongest cell and up to 63 neighbours, whereas a mobile handset-based device will actively select a current serving cell and will monitor a varying number of neighbouring cells.

A Rohde and Schwarz TSME drive test scanner a scanner is unable to undertake active/connected mode surveys (e.g. it doesn't make test calls), and it is not equipped to decode or apply the cell broadcast selection/reselection parameters which are significant in determining the service coverage area of a cell. It is therefore only able to offer details of the area within which a cell can be detected, it cannot offer information about the 'serving' service area within each cell's detectability area.

This is not intended to be a criticism of the R&S kit or of traditional scanners, it's simply a reflection of the fact that these devices were designed to only capture cell detectability, which is not always the objective of an RFPS survey.

The issue that we're attempting to outline here isn't related to the use of scanners per se, it's related to the ability to interpret the results provided by scanners to infer whether cells serve or not.

It is important to understand that there is a role for scanners to play in RFPS surveying – in fact, as the number of cellular technologies and radio bands employed around the world continues to increase there's an argument to say that the use of scanners will become mandatory for RFPS surveyors in the next few years. Scanners are useful for capturing the whole set of detectable cells, of all technologies and on all channels, at a location very quickly – for example, at a location where there are 4 networks, 4 technologies (including WIFI) and 10 or 12 separate channel bands in use, it becomes economically unviable to undertake 'all technology' profiles using just phone emulators – the time taken to undertake all of those separate surveys using just one phone emulator would be measured in days. Whereas a suitably equipped scanner could complete the entire survey in minutes.

Scanners are also beneficial in detecting cells that have been deliberately configured not to serve. There are multiple reasons why operators might do this, but it generally comes down to the need to ringfence capacity – some cells are configured with reselection parameters that are so extreme that no phone would ever find them suitable to select as a serving cell. This means that these cells won't need to expend the overheads necessary to support 'camped on' phones (e.g. phones that have selected that cell a serving cell), this in turn means that all of the cell's capacity is available to carry call traffic. Some cells are preserved solely for carrying high-speed data traffic. In all of these cases, access to the 'hidden' cells is controlled by the network, using handover procedures, rather than being controlled by phones using cell selection techniques. Scanners detect all cells on all channels, if they're configured to, and will therefore capture the 'hidden' cells along with the more readily accessible ones. Crucially, though, as they haven't taken the cell selection parameters into account, results obtained by traditional scanners make it difficult to interpret whether a detected cells, even if it's the strongest cell, was capable of serving.

Recent years have seen the arrival of what we may term 'hybrid' scanners – such as the devices produced by the US firm QRC. A hybrid scanner undertakes a wide-band survey that captures details of multiple cells and channels simultaneously, like a traditional scanner, but also captures and applies cell selection parameters to the measurements for each cell, like a phone emulator. This means that the results from hybrid scanners provide the ability to infer cell usability as well as cell detectability whilst at the same time providing the productivity and efficiency boost that made scanners attractive in the first place.

It is the Forensic Science Regulator's view that any measurement or analytical techniques employed to produce technical evidence must have been thoroughly validated by the practitioner so that the results can be shown to be demonstrably and repeatably accurate. Results provided by phone emulator type devices (CSurv, Forensic Compass, NEMO, TEMS, etc) that seek to show cell usability have undergone success validation numerous times (not least as part of the national ISO17025 trial a few years ago). We're not aware of any published validation results that show that the use of traditional scanners *on their own* to determine cell usability are accurate and as we'll outline below, we'd be extremely sceptical of any results that claimed to be able to provide such validation.

So, to summarise: phone emulators, scanners and hybrid scanners all have a role to play in the collection of RFPS survey data. As long as the methods employed using those devices have been validated and are appropriate for the form of analysis that is being undertaken, there is no issue with the use of any of them. The key to deriving appropriate conclusions from RFPS data lies in the interpretation of that data.

## Data Interpretation

If the equipment used to undertake a survey emulates (or is in fact) a mobile device, the survey results will reveal the service coverage area of a cell. This is consistent with the methodology and the interpretation of survey data taught on the College of Policing RF Surveyors course and the RF Propagation Surveyors course delivered by Forensic Analytics Limited, which are the only two courses available within the UK dealing with this discipline.

The use of a traditional scanner, measuring only the signal strength of surveyed cells, is acceptable if the objective is to either obtain a list of the cells that can be detected at a location or to obtain a plot

of the geographical area over which a cell can be detected. This is acceptable usage as it isn't open to alternative interpretations – either a cell was detected or it wasn't detected.

However, the use of a traditional scanner may not always be an acceptable method if the objective is to attempt to determine the set of serving cells at a location or to determine the serving service area of a cell. This is because the determination of whether a cell serves is based on knowledge of more than just it's signal strength and is therefore a matter of interpretation.

In short; a method that uses signal strength only to determine useful service coverage area is a flawed methodology and will lead to great disparities between surveys conducted using this method and surveys conducted using phone emulator techniques.

The disparity is born out of the fact that the service area that a phone emulator will have determined for cells, based on using a phone-like survey device and taking account of cell selection algorithms, is likely to be much smaller than the detectability area for those cells identified by a survey that used a traditional scanner.

Surveys conducted with traditional scanners are likely to indicate that a cell could be used over a much greater area than is in fact the case.

Surveys based on signal strength alone are not able to shed light on the usability of a specific cell in areas where there is competition from multiple other cells. For example, knowing that Cell A has a signal strength of, say -70dBm (which is a comparatively strong signal) does not tell us whether that cell would actually be used by a phone at the measurement location. In isolation we can say that a signal of -70dBm is more than capable of carrying a high-quality call, but Cell A wouldn't be selected as the serving cell by a real mobile device at that location if the phone was also receiving a signal with a strength of -50dBm from Cell B. In this scenario, the phone would choose Cell B as it had a much stronger signal (100x stronger, in fact).

In the case we were asked to comment on, the defence expert had determined that a received signal strength of -100dBm should be sufficient to maintain a successful 2G GSM connection. This in itself isn't contentious, GSM connections should work over signal strengths as low as -110dBm. However, the defence expert then went on to conclude that any location at which a given cell was detected with a signal strength of greater than -100dBm was a location at which that cell could be used to make a call and therefore was within the cell's usable service area, and this is contentious.

Determining the usability of cell based on its signal strength in isolation, without reference to any other cells that provide coverage in the same area is a flawed methodology as it fails to take into account the cell selection algorithms applied by mobile devices. In 2G GSM networks, which was the network type relevant in that case, a mobile device selects a serving cell on the basis that it is the strongest cell in that area at that point in time, it doesn't select the first cell that happens to be strong enough to carry a call. 3G and 4G networks operate slightly differently, in that a cell can be selected to serve if it is 'strong enough', meaning that it is stronger than a broadcast minimum value. This means that in 2G mode a phone will always choose the strongest cell (with caveats) whereas a 3G/4G phone will choose the strongest or one of the strongest cells.

Using this flawed methodology, the defence expert had simply mapped the area in which each surveyed cell was theoretically strong enough to carry a call but hasn't tested to make sure that the

cell could actually carry a call – either by referring to the relative usability of the cell compared to its neighbours and/or by making test calls. This is a failure of interpretation and also indicates that the methods being used in this example hadn't been validated.

Any 'cell coverage' maps produced using this flawed methodology will show only where the target cell was detected, not necessarily where is was serving. This is absolutely critical as cells can usually be detected some way beyond the area within which they are able to provide service. Ultimately, were results obtained using this methodology to be accepted by a court, they would provide inaccurate and grossly misleading indications of the 'usable' coverage area of those cells, which would inflate the area within which a phone using those cells could have been located when calls of interest were made.

In circumstances in which the prosecution were attempting to use cell site evidence to show that a suspect's calls could have been in an area that includes a significant address, maps produced using this flawed methodology would provide a much greater 'area of uncertainty' regarding the phone's possible location – they could erroneously claim to show that the phone could have been located a much greater distance away from the significant address than may in fact have been the case.

## Conclusion

There is nothing inherently wrong with using traditional scanners as part of a validated RFPS survey methodology.

Scanners have the potential to massively improve the speed and efficiency of RFPS surveys and will become invaluable survey tools as the range and complexity of the surveyed spectrum increases.

Scanner results in combination with test calls and phone emulator survey data or results obtained from hybrid scanners provide enough context to allow accurate interpretations of that data to be made.

Scanner results that merely seek to show the detectability of a cell or the range of cells that were detected at a location, without attempting to interpret the usability of those cells from that data, are also perfectly acceptable.

However, the interpretation of measurements obtained exclusively from traditional scanner-based survey devices, combined with an arbitrary 'minimal usable signal strength' level, to compile RFPS maps and reports which seek to show the serving potential of key cells, is a flawed methodology. If employed, this methodology has the potential to produce inaccurate and misleading results that can lead to similarly inaccurate and misleading conclusions.

This flawed methodology is only capable of reporting on the 'detectability' of surveyed cells and is unable, with any degree of accuracy, to report on the 'usability' of those cells.

In our opinion, and in the opinion of several experienced and respected cell site and RFPS practitioners with whom we have consulted in the process of producing this report, results obtained exclusively from traditional scanners in idle mode that seek to show the serving potential of key cells are flawed and will provide an inaccurate impression of a cell's coverage area.

**Acknowledgements**

This briefing was originally complied in relation to a specific case, but we consulted in a limited way within the cell site and RFPS community to gauge opinion and we amended some of our original text in response to comments received. We also then circulated the original report much more widely within the community and received a lot of very pertinent and sage feedback, which we have incorporated into the published version.

We would like to thank the following colleagues for their comments, feedback and input:

- Andy Dampier (Kent Police)
- Ash Waller (South Yorkshire Police)
- Phill Gardiner (First Forensic Solutions)
- Lester Wilson (3G Forensics)
- Dave Cutts (Forensic Analytics)
- Iain Brodie (CCL Group)
- Matt Tart (CCL Group)
- Dominic Kirsten (MASS)
- Richard Baxter (MASS)
- Stuart Banks (DFC Ltd)
- Darran Fletcher (Nottinghamshire Police)
- Joe Crocker (Avon & Somerset Police)
- Jim Ariss (EMSOU)

We'd be very interested in any further comments or feedback, contrary opinions or examples of the use of scanners vs test phones or anything else you feel like contributing – if you'd like to comment please email us at:

enquiries@forensicanalytics.co.uk

NOTES

CSAS Desktop | CDAN Indexer | CSAS Parsing API | Cell Site Analysis | Training Services

Forensic Analytics Ltd

Registered in England and Wales. Company No: 08606475

Pixmore Centre
Pixmore Avenue
Letchworth
SG6 1JG

+44 800 158 3830
www.forensicanalytics.co.uk