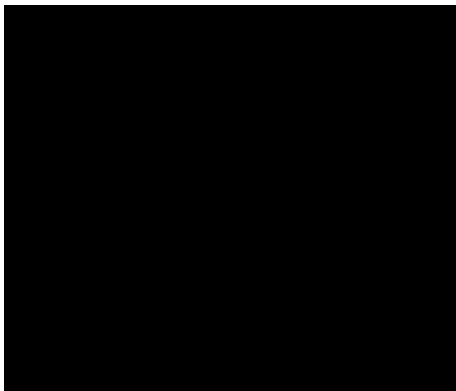
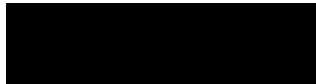

ICC v YEKATOM & NGAÏSSONA

Interpretation and Limitations of Call Data Records (CDRs)

Duncan Brown
23rd November 2023

Exhibit:



On instructions of:
NGAÏSSONA defence team

Subject matter:
CDR considerations

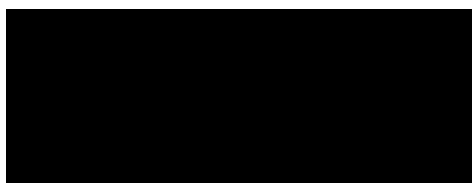
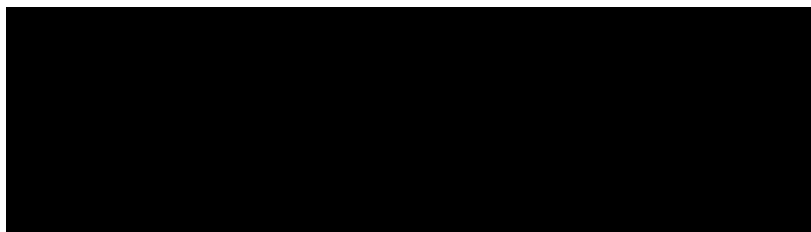


Table of Contents

1	SUMMARY	3
1.1	Case outline	3
1.2	Summary	3
2	INTRODUCTION	5
2.1	Report	5
2.2	Formal Details	5
2.3	Synopsis	6
2.4	Instructions	6
2.5	Disclosure of Interests	7
3	BACKGROUND	8
3.1	Information provided:	8
3.2	The Issues to be Addressed.	8
3.3	Background Information	9
3.4	Exhibits	9
4	CALL DATA RECORDS	10
4.1	Introduction to Call Data Records	10
4.2	Content of Call Data Records	10
4.3	Collection of Call Data Records	12
4.4	Preparation of CDR Extracts for Law Enforcement	12
4.5	Analyst Processing of Call Data Records	13
4.6	Interpretation of Call Data Records	14
4.7	Limitations of Call Data Records	14
4.8	Limitations of Call Records for Data Sessions (GPRS)	15
4.9	General Limitations of Cell-Site Evidence	16
4.10	Limitations of Attribution	17
5	QUESTIONS ARISING	19
5.1	Introduction	19
5.2	Questions emerging from proceedings and disclosed material.	19
5.3	Questions arising from conclusions of the Swiss police analyst report.	23
6	EXPERTS DECLARATION	27

1 Summary

1.1 Case outline

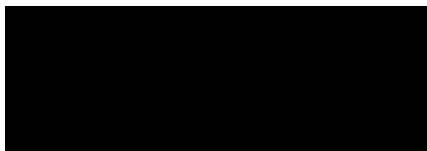
- 1.1.1 The Office of the Prosecutor at the International Criminal Court ('ICC') has brought war crimes and crimes against humanity charges against Mr Ngaïssona that relate to events which occurred in the Central African Republic ('CAR')
- 1.1.2 The Prosecution evidence includes Call Data Records obtained from various telecommunication providers and which they have suggested show patterns of contact relevant to their case.
- 1.1.3 I have been instructed by the defence team for Mr Ngaïssona to consider samples of that evidence and comment on the interpretation CDRs and the conclusions that can and cannot be drawn for such material.

1.2 Summary

- 1.2.1 CDRs (Call Data Records) are produced by Mobile Network Operators for billing and network management purposes. It is normally a requirement of the Operators' licenses that they achieve a high level of accuracy for their billing records, and it is in the companies' financial interest to record every chargeable connection. The CDRs may not capture every detail of every transaction but the information that is recorded is considered reliable.
- 1.2.2 'CDR Extracts' can be very useful to law enforcement agencies to attribute the phone to a named individual as a primary user or to provide evidence of contact or patterns of contact between parties.
- 1.2.3 When combined with cell-site information geo-location analysis can be used to establish location and movements of a mobile.
- 1.2.4 The reliability and usability of CDR Extracts depends on the careful definition of what data should be extracted and the operators' staff performing the extraction queries consistently.



- 1.2.5 The resulting CDR Extract files must be correctly managed to ensure any subsequent analysis can be completed to evidential standards. Any analysis products created for a prosecution must be repeatable for defence verification purposes.
- 1.2.6 CDR Extracts cannot identify who was using the mobile at a specific time nor confirm an accurate location beyond an area of likely coverage from the antennas used.



2 Introduction

2.1 Report

- 2.1.1 This document is the record of my investigative methodology and analysis, including my findings and conclusions.
- 2.1.2 To assist the reader, I have prepared a second document containing four annexes.

2.2 Formal Details

- 2.2.1 My name is Duncan Brown. I am a director of and expert witness for [REDACTED] [REDACTED] specialising in cell-site analysis, telephone attribution and related topics.
- 2.2.2 Having qualified as a Chartered Surveyor in 1983 I worked as a professional consultant to Vodafone Ltd. In the late 1980's I was responsible for the development of their regional telephone exchanges throughout the United Kingdom.
- 2.2.3 I subsequently joined Vodafone in 1990 with responsibility for the design and construction of new radio base stations and telephone exchanges throughout the U.K.
- 2.2.4 During overseas secondments to Australia and the Netherlands I was responsible for the development of the radio network infrastructure required for the launch of both networks. In 1998 I became Vodafone UK's National Implementation Manager responsible for network development and quality of service in London and the South-east.
- 2.2.5 On leaving Vodafone in 2002 I worked for a network consultancy company that provided services to the U. K's mobile Network Operators before establishing myself as an expert witness in 2004.
- 2.2.6 Since becoming a full-time expert witness, I have prepared technical reports and witness statements related to mobile telephones, cell-site analysis, telephone attribution and call data analysis in over 700 cases for both prosecution and defence clients.

- 2.2.7 I have provided expert services to UK forensics companies, many of the U.K.s police forces, defence solicitors and to the Special Tribunal for Lebanon, International Residual Mechanism for Criminal Tribunals and International Criminal Court in The Hague.
- 2.2.8 I have frequently attended Court to give evidence at the Old Bailey, The Courts of Appeal and Crown Courts throughout the U.K.
- 2.2.9 I have undertaken specialist training in relation to working as an expert witness including the Regulation of Investigatory Powers Act (RIPA) 2000, the Data Protection Act (DPA) 1998 and the gathering, preparation and presentation of evidence as an expert witness.
- 2.2.10 At Annex 1 I have included a Curriculum Vitae and notes of some notable cases with which I have been involved as an expert witness.

2.3 Synopsis

- 2.3.1 The two defendants Mr Patrice Edouard Ngaïssona and Mr Alfred Yekatom have been charged with war crimes and crimes against humanity that relate to events which occurred in the Central African Republic ('CAR'). The Prosecution alleges Mr Ngaïssona is responsible for the crimes through (1) steps he took to structure an armed group (the 'Anti-Balaka'), (2) financing said group and the purchase of weapons for it, (3) the issuing of instructions, and (4) liaising and coordinating with other key figures.
- 2.3.2 The Prosecution evidence includes Call Data Records obtained from various telecommunication providers and which they have suggested show patterns of contact relevant to their case.

2.4 Instructions

- 2.4.1 I have been instructed by the defence team for Mr Ngaïssona to consider samples of the Prosecution evidence and comment on the interpretation of CDRs and the conclusions that can and cannot be safely drawn for such material.



2.4.2 The defence team have also raised questions on related evidence and arising out of proceedings.

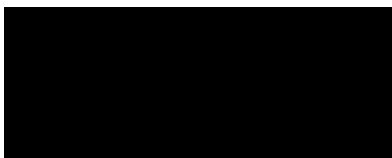
2.4.3 The Terms of Reference provided to me are included as Annex 2.

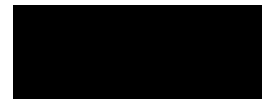
2.5 Disclosure of Interests

2.5.1 I have no connection with the defendants, witnesses or other parties involved in this case.

2.5.2 My analysis and opinions are given as an independent, unbiased expert witness.

2.5.3 My report is based on information received. If any of this information is incorrect, or if any new information is considered relevant, I may have to reappraise my finding.





3 Background

3.1 Information provided:

- 3.1.1 The following files were provided as annexes to the Terms of Reference and as supporting materials:

File
20231025 Specific Questions Annex A
Annex B _ CAR-OTP-2126-2529.pdf
ANNEX B_CAR-OTP-2126-2529_Part 1.pdf
ANNEX B_CAR-OTP-2126-2529_Part 2.pdf
CAR-OTP-2117-0135-R02.pdf
CAR-OTP-2117-0211-R02.pdf
CAR-OTP-2019-1364.xlsb
CAR-OTP-2019-2839.xlsb
CAR-OTP-2046-0766.xls
CAR-OTP-2054-1479.csv

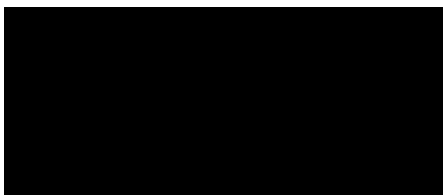
- 3.1.2 The following files were also provided as annexes to the Terms of Reference but were then withdrawn from my considerations. I have read these documents but have not relied upon their content in writing this report.

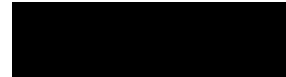
File
Annex C _ Statement CAR-OTP-2122-9874-R01.riv.pdf
Annex C _ Transcripts of Hearing.pdf
CAR-OTP-2134-0124-R01.pdf

- 3.1.3 I have noted that the .xlsb files provided are Excel Binary Workbooks used to reduce the file sizes of .xls and .xlsx files.

3.2 The Issues to be Addressed.

- (a) Respond to Terms of Reference provided (Annex 2)



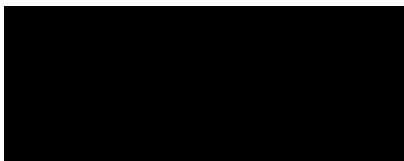


3.3 Background Information

- 3.3.1 For reference purposes, Annex 3 provides a glossary of terms commonly used in telecommunications Analysis and Annex 4 provides a list of abbreviations related to mobile phone networks.

3.4 Exhibits

- 3.4.1 The results of the work undertaken are included in this report identified as 
 and should be read in conjunction with the supporting exhibit identified as
 Annexes.



4 Call Data Records

4.1 Introduction to Call Data Records

- 4.1.1 Call Data Records or Call Detail Records will hereafter be referred to as CDRs or just as call records. These terms will be used for all records whether they are for voice calls, text messages or data connections.
- 4.1.2 All mobile Network Operators record information in respect of the mobile phone connections on their networks. A CDR will be created every time a mobile phone is used and separate CDRs will be created for each party to the connection.
- 4.1.3 An 'Outgoing' CDR will be created for the mobile number initiating the connection, often referred to as the 'A-Number'. A separate 'Incoming' CDR will be created for the receiving number, often referred to as the 'B-Number'. Should the incoming call be diverted to another number this may be referred to as the 'C-Number' and a third CDR may also be created to record this diversion.
- 4.1.4 Every connection through a mobile phone network involves many parts of the network and multiple records may be created. It is often the case that a CDR contains multiple lines of information relating to different parts of the same connection.
- 4.1.5 Law enforcement agencies often request copies of an operators CDRs, and the resulting data files are best thought of as 'CDR Extracts'.

4.2 Content of Call Data Records

- 4.2.1 Although the information recorded by each operator varies it is collected for the same general purposes:
 - a) To correctly charge the cost of the connection (Billing).
 - b) To debit the cost of a call from a prepaid voucher.
 - c) To enable the calculation of taxes payable.
 - d) To provide information for network management and maintenance.

- 4.2.2 For billing purposes, the following information is logged for each originating and, in most cases, terminating, voice calls, text messages and data connections:
- a) The start date and time of each call.
 - b) The call duration usually measured to 1/10th of a second.
 - c) The type of connection for example voice, text or data.
 - d) The quantity of data uploaded and/or downloaded.
 - e) The number called or calling. The connected party.
 - f) In the case of text messages this may be the network's text message deposit number.
- 4.2.3 For network management purposes, many other pieces of information are logged. These can be customised to suit the operator but will usually include:
- a) The identity of the cell used at the start and, in some cases, the end of a call.
 - b) The reason the call terminated.
 - c) Some networks identify if the outgoing or incoming call was diverted to another number (generally a message service).
 - d) The IMEI of and IMSI using the handset.
- 4.2.4 The start time of an incoming voice call is the point at which the call is answered. The start time of an outgoing voice call is the point at which the mobile hears the call has been answered which may be recorded as a second or two later than the incoming call start time.
- 4.2.5 The start time of a diverted call is the point at which the caller hears the start of the message to say the call is being diverted to a voice mailbox. Although it varies, it typically takes around 10 seconds or so before you can start to leave a message so only durations longer than 10 seconds suggest a message has been left.
- 4.2.6 Some operators record the 'ring time' – the time for which the receiving phone was ringing before being answered. A random discrepancy in the duration of the incoming and outgoing calls may be because of the operator including the ring time in the call duration.
- 4.2.7 As an aside, the operators' CDRs will usually contain information as to which cell or cell-site was used at the start and/or end of a connection but, does not contain the details of the antenna configuration or the cell-site details such as the location or address.

- 4.2.8 The Operators typically maintain a separate 'Cell-site Information' database that will be used for cell-site planning and should be updated with any changes to the cells or cell-sites.

4.3 Collection of Call Data Records

- 4.3.1 CDRs are created at the time of the connection at the MSC (Mobile Switching Centre) that controlled the connection. This data is then transferred to central servers that provide data storage. In modern networks this is carried out automatically.
- 4.3.2 The data can be processed for billing purposes as required.
- 4.3.3 The data may also be used for maintenance or marketing purposes.
- 4.3.4 Each operator chooses what data to retain and how long to retain that data.

4.4 Preparation of CDR Extracts for Law Enforcement

- 4.4.1 Law enforcement agencies routinely request information about individual subscribers, telephone numbers or handsets. The required information needs to be extracted from the operators' databases and produced in a secure file format.
- 4.4.2 Best practice requires the data files to be provided in a .pdf format that cannot be edited and this becomes the evidential document. Because that data cannot be edited a second copy should be provided in a .csv or other Microsoft Excel format that can be processed for any required analysis.
- 4.4.3 The CDR Extract files produced by the operator are sometimes referred to as the 'Golden Copies' or 'Raw' CDR files and should be securely stored without any further processing including not changing the files names. Working copies can be provided to investigators or defence analysts who can be confident the data is unchanged by reference to the .pdf copies.
- 4.4.4 The subject number of the enquiry may be referred to as the target number. Ideally separate queries are made for each target number.

- 4.4.5 Every Network Operator produces CDR Extracts with varying content and formats. The information included in a CDR extract may also vary depending on what exactly was requested. In the absence of strict protocols to standardise their CDR Extracts the content and formats will vary depending on the database query used by the individual tasked to produce the extract.
- 4.4.6 Some operators use separate queries for incoming and outgoing connections and data connections so that several CDR Extract files are produced for a single target number. Others use an 'all connections involving number 1234' query which may mean that if both parties were on the same network, then both the incoming and outgoing records are provided in the same file and must be processed to exclude the record that does not relate to the target mobile.
- 4.4.7 Relevant cell-site information may be combined with the CDR data by the Operator, or the cell-site information may be provided in separate files.

4.5 Analyst Processing of Call Data Records

- 4.5.1 For consistency and ease of use in court, the CDR Extracts from different networks are usually processed by analysts and presented in tables with a standard format. Generally referred to as Call tables, it should be recognised they are an analysis product and should be produced with a suitable witness statement defining the source materials and processing techniques used.
- 4.5.2 Small data sets can be processed manually but larger data sets will need standardised processing software. There are commercial organisations that specialise in such software.
- 4.5.3 The same software packages are also capable of statistical analysis of the data and if cell-site information has been provided can also be used for producing cell-site mapping to assist geo-location analysis.
- 4.5.4 Should any queries arise as to the integrity of the processed call data records the original .pdf copies should be referenced.

4.6 Interpretation of Call Data Records

- 4.6.1 Once the credibility of a set of CDR files has been established, the Call data records can be used in a multitude of ways.
- 4.6.2 A single mobile can be analysed to identify contacts or patterns of use to create a profile of use and to support the attribution to a named 'Primary User'. The 'Primary User' being an individual who has effective control of the mobile and is likely to make most of the use of the mobile. Multiple phones can be analysed in the same way to see if the user profiles are the same and therefore, they are likely to be used by a single user. Similar analysis may identify networks of users that may have a common purpose.
- 4.6.3 It is possible that few connections may not be recorded by an operator due to technical errors, but the systems cannot invent connections that did not occur and those recorded should be considered reliable.
- 4.6.4 When combined with cell-site information geo-location analysis may also be possible to identify the location and movements of the mobile.

4.7 Limitations of Call Data Records

- 4.7.1 In an ideal situation both the incoming and outgoing CDRs are available for comparison to resolve difficulties that sometimes arise identifying whether the call was connected or diverted.
- 4.7.2 A voice call record only shows the cell or cells used at the start and end of the call event; it does not record any other cells that may have been used within the duration of the call.
- 4.7.3 A text message record only shows the single cell used to send or receive the message. As text messages are effectively sent instantaneously, they are normally recorded on CDRs with a duration of zero (0) or one (1) second duration.
- 4.7.4 So, for voice and text connections the start time noted is accurate for the time at which the recorded cell ID was first used (or last used in the case of end cell records from voice connections).

- 4.7.5 An incoming text message is delivered by the network without any user intervention provided the mobile is switched on. As a result, it cannot be said the user was necessarily with the mobile at that time.

4.8 Limitations of Call Records for Data Sessions (GPRS)

- 4.8.1 A "Smartphone" that uses network data (GPRS) can be connected to the internet and data call events or sessions may occur without user intervention.
- 4.8.2 The records of data sessions need a more careful interpretation as to the time at which the associated cell IDs were used. Whereas for voice and text connections the start time noted is accurate for the time at which the recorded cell ID was first used (or last used in the case of end cell records from voice connections) that is not the case for records of data sessions.
- 4.8.3 In the data session records supplied by the network there is not always a direct association between the call event time shown and the cell identity shown. This is due to the way data connections are handled by the network and each network records the time of the record in different ways. As a result, it is usually only possible to describe that a cell was used within a defined period.
- 4.8.4 Because of this, the voice and text CDRs should be considered as the primary location information for the handset and take precedence over GPRS records in situations where there is a disparity between the two types of records.
- 4.8.5 A mobile telephone using data sessions makes use of a 'Routing Area', a group of many cells. The Routing Area can be thought of as similar to a postcode, with individual addresses (cell-sites) on one or more streets in one unique postcode zone (routing area).
- 4.8.6 At the time of a data call session, the mobile network captures the time of the event and the details of the last cell, as provided by the handset, which will be the first cell used detected in the new and now current Routing Area.
- 4.8.7 This means that if the handset is used within a single Routing Area, the handset may use any of the cells within the Routing Area, without updating the network or creating a new call record.

- 4.8.8 Hence the cell ID recorded may NOT be the cell where the handset actually was at the time shown. As a result, the recorded cell can only be defined as being connected in a particular period depending on which network is used.

4.9 General Limitations of Cell-Site Evidence

- 4.9.1 Whilst each call record shows that the mobile telephone used a specific cell or cells to carry that call no expert can pinpoint where the mobile telephone was specifically located within the extent of coverage of the cell used.
- 4.9.2 Cell-sites vary greatly in the extent of coverage they provide depending on the requirements of the network. In simple terms the greater the capacity required in an area then the greater the number of cell-sites used with each cell providing smaller areas of coverage.
- 4.9.3 It is not possible for the call records or Cell-Site Analysis to identify who was using the telephone at any time. Whilst analysis of CDRs may identify the likely 'Primary User' of a mobile it cannot identify who made any individual connection.
- 4.9.4 A mobile telephone may use one cell for a period. This does not necessarily indicate that the telephone was stationary in one place. The telephone could also have moved within the cell, possibly some distance depending on the coverage of the cell.
- 4.9.5 Hence an expert can only say the phone was somewhere within the cell's coverage area at the time it was used. If there are no CDRs close in time to a particular event it is not possible to identify whether the mobile was in that area at that time.
- 4.9.6 Non-experts may be inclined to think the mobile and user was at or close to the cell-site location and it is important to emphasise the user could have been many kilometres away.
- 4.9.7 Similarly single connections should not be considered in isolation as the location can be misconstrued. Rather a sequence of connections should be considered to identify if the user was static in an area or was merely in transit through that area.

4.10 Limitations of Attribution

- 4.10.1 In general, most attributions of mobile telephones depend on a collection of evidence types that together create a consistent picture of ownership of the subject mobile and thereby identify the 'Primary User' of the mobile. The attribution is obviously strengthened if all threads of evidence point in the same direction and vice versa.
- 4.10.2 In the table below are attribution elements relevant to potential phone ownership or usage that may be considered as part of an attribution process.

Nr	Attribution element
1	Possession of handset
2	Possession of SIM card
3	Subscriber checks
4	Handset/SIM card contact (address) book analysis
5	Handset/SIM card text message analysis
6	Contact lists of associated phones
7	Handset IMEI usage
8	Top up/payment analysis
9	Call records contact analysis
10	Contact with family/friends
11	Contact with other nominated numbers
12	Cell site analysis
13	Geographically separated
14	Potentially co-located
15	Overnight at address
16	Most Used cells at home address
17	First call/cell
18	Last call/cell
19	Concurrent calls
20	Police systems
21	Witnessed associations
22	ANPR

- 4.10.3 It is also of equal importance to consider elements of 'dis-attribution' that might affect the overall strength of the attribution. These elements demonstrate the telephones cannot be attributed to a single user, but to two or more potential users.
- 4.10.4 However strong that overall attribution may be, it must be remembered that attribution can only establish who is likely to be the 'usual holder' or 'Primary User' of the handset and can never determine who actually had the telephone 'in hand' at a particular time or for any specific call.

- 4.10.5 In instances involving the attribution of multiple telephones to the same individual, aspects of usage of one attributed mobile are then compared to other mobiles and use the consistency of those issues to support attribution.
- 4.10.6 This technique should only be considered valid when both mobiles have sufficient CDRs for a reliable analysis and those CDRs overlap in time or follow one another close in time. One mobile telephone must also have a strong attribution. The attributions cannot be relied upon if they have been built only by being dependent upon each other.

5 Questions Arising

5.1 Introduction

- 5.1.1 The following are questions raised by the defence in the annex to the Terms of Reference provided.
- 5.1.2 The CDR Extract files provided were all named with Prosecution references, and it was unclear if these were original copies of files provided by the operators or if they were prosecution products.

5.2 Questions emerging from proceedings and disclosed material.

- 5.2.1 The questions posed to me are reproduced below for ease of reference.

a) Masked numbers.

Have you worked with clients or tribunals where masked numbers was an issue?

- If yes, did the masked numbers appear in the CDRs?
- If you have worked with masked numbers more than once, is it common that the number appears in the CDR?
- Did the CDR indicate that the number was masked, and if so, how was this done?
- Is it correct understanding that according to our experience, if an authority requests a CDR from a telecommunication company that targets a specific number for a time period, all calls including the masked numbers to and from that number should be reflected in the CDR correct?
- Is it correct in your opinion that, presupposing a witness was correct in saying to have received a masked call, the absence of the masked call in their CDRs would indicate that either (a) the CDR was not prepared competently or (b) there is unidentified error in the system used to retrieve or store the records upon which a CDR is built?

- 5.2.2 Calling Line Identification (CLI) is a service available on many networks to allow the receiver to see the calling number and is very common on mobile phones. However, it is usually possible for the caller to choose to hide their number before calling and thereby 'masking' their number.

- 5.2.3 However, these numbers will always be visible to the operator and therefore visible within the call data records produced. I have never seen any information within the CDR extracts normally provided to identify if the caller withheld their number but logically that information would be available in the CDR database.

- 5.2.4 It is sometimes the case that the caller's number does not appear in the CDR for the receiver. The receiver's operator relies on the caller's operator to provide that number and not all operators are reliably able to do that on every occasion. This I have most seen for incoming calls from international callers.
- 5.2.5 It is my opinion that, barring exceptional failings by the operator to record a CDR, all calls whether masked or otherwise will be included in a CDR. I cannot foresee how a CDR could be prepared so that it accidentally did not include masked calls but, I could not definitively eliminate that possibility. The absence of a caller's number in the CDR is most likely to be a result of the caller's network failing to supply the information.

b) Changing IMSI and IMEI numbers despite a consistent phone number.

The Defence has identified the anomaly in CAR-OTP-2054-1479, row 49 to row 419 but cannot exclude that the issue is more widespread. The IMSI/IMSI numbers don't seem to change even though the calling or called number does. How can this be explained? Could this be indicative that the extraction of the CDR was not undertaken with the requisite skill or that there is incorrect information stored in the database from which the CDR was derived? Have you come across this issue in other work and if so, what could be the source of this issue?

- 5.2.6 The simple answer is that CAR-OTP-2054-1479 is not a CDR for a single subject mobile. The table combines the CDRs of multiple mobile phones possibly as a result of the query made by the operator of their database or more likely by somebody later combining the individual CDRs of the mobiles.
- 5.2.7 As an aside it can be seen in the exhibit that column A is headed as the connection **end** time. In my experience it is highly unusual for the CDR to contain the end time rather than the start time. There would be an obvious problem if CDRs with start times were unthinkingly combined with other CDRs with only end times.

c) The order of records in a call-data record.

Please review CAR-OTP-2054-1479, row 2 to row 48 although the pattern appears throughout the CDR. These all concern calls to the number "[REDACTED]". These rows appear to reflect calls from the period of "01/07/2013 09:31:28" to "28/09/2013 19:41"; however, at row 50 the chronology starts again at "02/07/2013 11:00" and this pattern

repeats. If records for several target numbers were drawn from an automatic ledger, it would appear to the Defence that these records would be interwoven chronologically. Here it seems as though the record was assembled by hand. Is the pattern we see characteristic of a competently extracted call data record?

- 5.2.8 The answer again is that CAR-OTP-2054-1479 is not a CDR for a single subject mobile. As the table combines the CDRs of multiple mobile phones each is sorted by its own chronology, and they have not been collectively reordered.

d) Inconsistency in time information between two CDRs that purportedly cover the same information.

CAR-OTP-2019-2839 is the result of a broader request whereas CAR-OTP-2046-0766 is targeting the number [REDACTED] which appears within CAR-OTP-2019-2839. Please focus upon CAR-OTP-2019-2839, rows 709916 and 709917 (date and time: 2015-05-15 at "19:02:02") and CAR-OTP-2046-0766, row 9321 (date and time: "2015-05-15, 19:04:30"). Please also consider the call at CAR-OTP-2019-2839, rows 760071 and 760072 (date and time: 2015-07-18 at "13:53:21") and CAR-OTP-2046-0766, row 9915 (date and time: "2015- 07-18, 13:53:14"). It appears plausible to assume that these are the same calls. The duration of the calls has a consistent 1 second difference; however, the beginning time of the calls are different. Moreover, there is not a constant difference in time shift. In one case the time difference is two and half minutes. In other case it is 7 seconds.

- Is concluding that these are the same calls forensically sound in your opinion?
- If the underlying information was derived from a database, shouldn't it normally be the case that information is precisely the same?
- If the offset was consistent (i.e. 7 seconds), this might indicate some sort of miscalibration but it would show a systemic, but consistent error, that could be explained as more of a user error than a malfunction?
- Presuming this is the same call, doesn't this suggest an error in the system? Could you explain why this is possibly more serious than a consistent offset?
- Could this in your opinion be indicative of a technical issue that impacts upon the integrity of the database?

- 5.2.9 The first point to understand is that the outgoing and incoming calls are timed individually. As a result, it is common for the two ends of the call to have durations that differ by a second or two. Simply put, the receiver's call duration starts when the incoming call is accepted but the network still needs to send a signal back to the callers mobile that the call has been answered. Whilst this will usually take only a fraction of a second it will sometimes take longer especially for connections with complex routing such as international calls.

5.2.10 The second point to note is that the two subject mobiles may be connecting through different MSCs (Mobile Switching Centres). In the most up to date networks all the timeclocks of the MSCs are automatically synchronised but this has not always been the case and the MSCs needed to be manually synchronised; a maintenance task that might be neglected. I have seen examples where the lack of synchronisation meant the start times had drifted to several minutes.

5.2.11 For ease of comparison of the two exhibits I have rearranged the column order so the two match and then combined the relevant lines of data for mobiles [REDACTED] 34 and [REDACTED] 48. A sample is provided below. Entries from CAR-OTP-2046-0766 are coloured yellow and the queries highlighted in red.

DATE_JOUR	HEURE	DUREE	TYPE	SENS	A_NUMBER	B_NUMBER	SITE
DATE FIN	HEURE FIN	DUREE(SEC)	TYP		NUMERO	N. DEMANDE	DESTINAT
15/05/2015	19:02:02	186	TEL	Entrant	[REDACTED] 18	[REDACTED] 34	GALABADJA
15/05/2015	19:02:02	186	TEL	Sortant	[REDACTED] 34	[REDACTED] 48	BOY-RABE
15/05/2015	19:04:30	185	PPP		[REDACTED] 34	[REDACTED] 48	1 GSM Orange
09/06/2015	20:07:44	85	TEL	Sortant	[REDACTED] 18	[REDACTED] 34	CARNOT
09/06/2015	20:07:44	85	TEL	Entrant	[REDACTED] 34	[REDACTED] 48	BOY-RABE
16/06/2015	14:44:37	191	TEL	Entrant	[REDACTED] 34	[REDACTED] 48	ASSEMBLEE
16/06/2015	14:44:37	191	TEL	Sortant	[REDACTED] 18	[REDACTED] 34	CARNOT
18/07/2015	13:53:14	97	PPP		[REDACTED] 34	[REDACTED] 48	1 GSM Orange
18/07/2015	13:53:21	98	TEL	Sortant	[REDACTED] 34	[REDACTED] 48	ASSEMBLEE
18/07/2015	13:53:21	98	TEL	Entrant	[REDACTED] 18	[REDACTED] 34	CARNOT
30/07/2015	15:38:02	122	TEL	Entrant	[REDACTED] 34	[REDACTED] 48	BOY-RABE
30/07/2015	15:38:02	122	TEL	Sortant	[REDACTED] 18	[REDACTED] 34	CARNOT
07/08/2015	14:44:43	139	TEL	Entrant	[REDACTED] 34	[REDACTED] 48	ASSEMBLEE
07/08/2015	14:44:43	139	TEL	Sortant	[REDACTED] 18	[REDACTED] 34	CARNOT
07/08/2015	14:49:26	59	TEL	Sortant	[REDACTED] 34	[REDACTED] 48	ASSEMBLEE
07/08/2015	14:49:26	59	TEL	Entrant	[REDACTED] 18	[REDACTED] 34	CARNOT

5.2.12 My examination of CAR-OTP-2019-2839 has identified that it contains CDR type information for both mobiles [REDACTED] 34 and [REDACTED] 48. As shown in the sample above the incoming and outgoing legs of the calls are consistent in time and duration.

5.2.13 I do not believe CAR-OTP-2046-0766 is a normal CDR. Rather it is the records of some other activity possibly money transfers or some other transaction between the parties. It is not possible to be certain of the purpose of these records without an originating witness statement and therefore not possible to resolve the inconsistency in timings.



e) *Missing records in a CDR.*

CAR-OTP-2019-2839 is the result of a broader request whereas CAR-OTP-2046-0766 is targeting the number [REDACTED] which appears within CAR-OTP-2019-2839.

Provided that the time frames overlap, as CAR-OTP-2046-0766 appears to be specifically targeting the number [REDACTED] it would follow that every call in CAR-OTP-2019-2839 originating from the phone number [REDACTED] would appear in CAR-OTP-2046-0766.

Please examine CAR-OTP-2019-2839, rows 776820, 776883, 776917, 777238-777240, 777285, 777289, 777325, 777373, 777377, 777380, 777400, 777424, 777453, 777521, 777564, 777627, 777659, 784291, 784292, 784324-784327, 784342, 784375-784377, 784379- 784396. Now please examine rows 10093 to 10111 of CAR-OTP-2046-0766 which covers the same period.

- Presuming the above is correct, we should see the calls on 2015-08-07 and 2015-08-17 in CAR-OTP-2046-0766?
- Yet there appears to be at a minimum 46 missing records in CAR-OTP-2046-0766?
- If the 46 records in CAR-OTP-2019-2839 exist and are omitted in CAR-OTP-2046-0766, would this suggest that the competence of the person preparing CAR-OTP-2046-0766 either made a major error or there was a major technical error?
- Yet as there is not a basis to conclude to which CDR is more accurate (if either), could this suggest that records in CAR-OTP-2019-2839 might also be erroneous?

5.2.14 As noted in 5.2.12, I do not believe CAR-OTP-2046-0766 is a normal CDR. Rather it is the records of some other activity possibly money transfers or some other transaction between the parties. It is not possible to be certain of the purpose of these records without an originating witness statement. As they are not normal CDR records there is no reason to believe the records should have an equivalent in the other exhibit.

5.3 Questions arising from conclusions of the Swiss police analyst report.

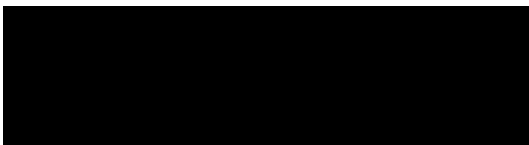
5.3.1 See CAR-OTP-2126-2529.

5.3.2 The questions posed to me are reproduced below for ease of reference.

a) *The futility of conducting an IMEI analysis.*

In the report of the Swiss analyst, he concludes that given the quality of the data that he was provided was not of a sufficient quality to conduct a IMEI to IMEI analysis.¹

- Can you please explain the process he is discussing in greater detail so that the Chamber and parties to the trial can understand the nature of the analysis he finds that he is unable to conduct.



- As the analyst does not provide an extended discussion of his methodology with respect to this and how he drew the conclusion, could you please describe the conditions that would be essential to be able to conduct such an analysis.

- 5.3.3 In my opinion the analyst was not referring to an IMEI to IMEI analysis but rather to the analysis of a target IMEI to identify which SIM cards had used that handset. This is an analysis often performed to provide evidence that two or more phone numbers can be attributed to the same user or was shared by several users.
- 5.3.4 The analysis is a simple one that can be completed in an Excel spreadsheet if suitable data files are available. The analysis identifies all phone numbers that have used the IMEI identified as the target of the analysis.
- 5.3.5 CDRs are normally generated for a single target mobile number and in this situation the CDR will identify different IMEI's that have been used by the target number but will NOT identify other mobile numbers that may have used those IMEIs.
- 5.3.6 For that analysis it is possible for the network operator to query their CDR database searching for an identified IMEI number.
- 5.3.7 Alternatively, multiple data sets can be combined by an analyst and then queried. This was perhaps the intent of the Swiss analyst, but they did not feel the IMEI data available was sufficiently reliable.
- 5.3.8 The problem identified by the Swiss analyst was that they could not be certain which IMEI related to which number. It seems they did not feel they could reliably identify whether the IMEI shown in a line of data related to the A-number or the B-number.
- 5.3.9 To reliably complete an IMEI analysis requires the lines of data to clearly identify whether that line of data was recorded for the A-number or the B-number. In other words, was the connection an incoming CDR or an outgoing CDR?
- 5.3.10 CDRs will usually identify whether a connection is incoming or outgoing using the description of the connection type or a separate field that states which it is.
- 5.3.11 The Swiss analyst had been provided with large numbers of files and I cannot comment whether the IMEIs could have been identified in the original files or whether this became impossible because of the processing they undertook to create a master database.

b) Geo-locating cell tower antennas.

The Swiss analyst explained that drawing conclusions about location is more complex than an IMEI analysis. He concluded that he could not provide a conclusive or unambiguous location to the calls. This was because the information he received was not precise or a locality was associated with many different geographical coordinates.

- Can you explain why it is that having a precise location for the antenna is necessary for cell site analysis?
- Is it the case that seemingly even small differences in the azimuth or GPS coordinates of the antenna can impact upon conclusions that an analyst might draw?

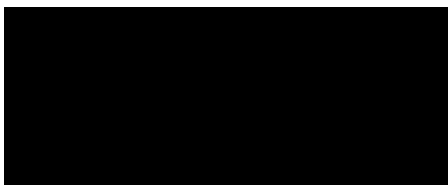
- 5.3.12 Firstly cell-site analysis (geo-location) can only ever provide a description of the area within which a mobile is most likely to have been located. The size of the location area will be determined by the definition of the cell-site location and cell detail provided by the network.
- 5.3.13 If the network provide some identification of the cell-site location then cell-site analysis (geo-location) should be possible. If they only provide the cell-site address as a city, then the analysis can only consider if they were in that city at that time but not where within the city they may have been. Should they provide an identifiable address then a more closely defined area can be given and ultimately if the antenna orientation is provided an even more closely defined area could be described.
- 5.3.14 I consider it normal practice for a network to record the identity (ID) of the cell used for a connection so it can be referenced in the CDR. However, that may not be the same for all networks who may just record a cell-site name. Site names may usefully refer to the building or local area or may be less useful for geo-location.
- 5.3.15 As noted earlier, the operator would normally maintain a database of cell-site locations and cell configurations. Accurate location information is essential to high quality radio propagation predictions and therefore to network planning.
- 5.3.16 The detailed cell/cell-site information required for the most accurate geo-location is not normally included in a simple CDR file and is often provided separately but only if requested.
- 5.3.17 As only a sample of CDR materials was provided for consideration, I am not able to comment whether the Prosecution received sufficient information to conduct a reliable CDR and cell-site analysis.



5.3.18 The best quality cell-site analysis would obviously require accuracy in all details provided but that does not mean cell-site analysis is pointless. A cell-site expert will always consider the quality of the information provided and express his opinions accordingly.

Duncan Brown

End of Report





6 Experts Declaration

STATEMENT OF TRUTH

I confirm that the contents of this report are true to the best of my knowledge and belief, and that I make this report knowing that, if it is tendered in evidence, I would be liable to prosecution if I have wilfully stated anything which I know to be false or that I do not believe to be true.

Signed

A handwritten signature in black ink, appearing to read 'D. Brown', written over a light blue horizontal line.

Date 23rd November 2023

