BEFORE THE TRIAL CHAMBER

SPECIAL TRIBUNAL FOR LEBANON

Case No:	**STL-11-01/T/TC**
Before:	**Judge David Re, Presiding** **Judge Janet Nosworthy** **Judge Micheline Braidy** **Judge Walid Akoum, Alternate Judge** **Judge Nicola Lettieri, Alternate Judge**
Registrar:	**Mr Daryl Mundis**
Date:	**16 February 2015**
Filing Party:	**Defence Counsel - Oneissi**
Original language:	**English**
Classification:	**Public**

PROSECUTOR
v.
SALIM JAMIL AYYASH
MUSTAFA AMINE BADREDDINE
HASSAN HABIB MERHI
HUSSEIN HASSAN ONEISSI
ASSAD HASSAN SABRA

Oneissi Consolidated Response to the Prosecution Motions for the Admission of Call Sequence Tables

---

Office of the Prosecutor:
Mr Norman Farrell

Defence Office:
Mr François Roux

Legal Representatives of Participating Victims:
Mr Peter Haynes, Mr Mohammad F. Mattar & Ms Nada Abdelsater-Abusamra

Counsel for Mr Salim Jamil Ayyash:
Mr Eugene O'Sullivan, Mr Emile Aoun & Mr Thomas Hannis

Counsel for Mr Mustafa Amine Badreddine:
Mr Antoine Korkmaz, Mr John Jones & Mr Iain Edwards

Counsel for Mr Hassan Habib Merhi:
Mr Mohamed Aouini, Ms Dorothée Le Fraper du Hellen & Mr Khalil Jad

Counsel for Mr Hussein Hassan Oneissi:
Mr Vincent Courcelle-Labrousse, Mr Yasser Hassan & Mr Philippe Larochelle

Counsel for Mr Assad Hassan Sabra:
Mr David Young, Mr Guénaël Mettraux & Mr Geoffrey Roberts

I. INTRODUCTION

1. The Defence for Hussein Hassan Oneissi ("the Defence") hereby files its Consolidated Response to the Office of the Prosecution's ("the Prosecution") Motions of 28, 29 and 30 January and 2 and 3 February 2015 requesting the admission of Call Sequence Tables ("CSTs") and Short Message Service CSTs ("SMS CSTs" and, together, "Communication Evidence") related to the purple phones and red, green, blue and yellow network phones. Together, these Motions are referred to as the "Prosecution Motions for the Admission of CSTs".

2. The Defence requests the Trial Chamber to reject the relief requested in each of these five Motions on two alternative grounds:

a. The data that were used to produce the CSTs and SMS CSTs were gathered in breach of the international standards governing the collection of such evidence and their admission is therefore "antithetical to, and would seriously damage, the integrity of the proceedings" under Rule 162 of the Rules of Procedure and Evidence ("the Rules"). In light of the importance of these issues, the Defence requests that they be granted the opportunity to make oral submissions.

b. Alternatively, it is not possible to ascertain the reliability of the Communication Evidence under Rule 149(C) prior to hearing the *viva voce* testimony of the relevant witnesses.

3. In these submissions, "CDR" refers to the underlying call and SMS records collected by the UNIIIC and the Prosecutor from Ogero, MTC and Alfa, the Lebanese Communication Service Providers ("CSPs"). "Communication Evidence" refers to the CSTs and SMS CSTs, produced as the result of the analysis of the CDRs, and object of the Prosecution Motions.

II. PROCEDURAL HISTORY

4. The Prosecution filed its Motions for the admission of the CSTs and documents related to the red, green, blue and yellow phones on 28 and 29 January and 2 and 3 February 2015, respectively.[1]

5. The Prosecution filed its Motion for the admission of the CSTs and documents related to the purple phones, one of which allegedly belonged to Mr Oneissi, on 30 January 2015.[2]

[1] STL, *Prosecution v Ayyash et al.*, Case No. STL-11-01/T/TC, Prosecution Motion For the Admission of Red Network-Related Call Sequence Tables and Related Statement, 28 January 2015 ("Red Motion"); Prosecution Motion for the Admission of Green Network Related Call Sequence Tables and Related Statement, 29 January 2015 ("Green Motion"); Prosecution Motion for the Admission of Blue Network-Related Call Sequence Tables and Related Statements, 2 February 2015 ("Blue Motion"); and Prosecution Motion for the Admission of Yellow Phone Related Call Sequence Tables and Related Statement, 3 February 2015 ("Yellow Motion"). All further references to filings and decisions relate to this case number, unless otherwise stated.

III. SUBMISSIONS

A. LEGALITY

6. The CDRs are central to the Prosecution case and the identification of the phone networks is "the cornerstone of the Prosecution's theory".[3] It is therefore essential to establish whether the CDRs were legally collected. To this end, a review of the applicable law and of the steps followed to collect the CDRs is required.

7. Two additional circumstances must be underlined at the outset. First, three years after the commencement of the proceedings, it is still impossible to have a precise and comprehensive idea of the CDRs collected since 2005 that will be relied upon at trial.[4] Second, the issue is already pending before the Trial Chamber and as such, can no longer be ignored or circumvented.[5]

1. Applicable law

8. The collection and admissibility of the CDRs and Communication Evidence must comply with the legal requirements applicable to any category of evidence; as well as those specifically applicable to communication evidence.

a. General requirements

i. Evidence Collection

9. When collecting evidence, both the UNIIIC and the Prosecution are required to comply with the provisions set out below.

10. Resolution 1595 (2005) established the UNIIIC on 7 April 2005.[6] Under that Resolution, the UNIIIC was to enjoy the full cooperation of the Lebanese authorities[7] to collect any additional information and evidence that it deemed relevant to the inquiry.[8] To

---

[2] Prosecution Motion For the Admission of Purple Phone Related Call Sequence Tables, 30 January 2015 (Purple Motion).
[3] STL, *Prosecution v Ayyash et al.*, Case No. STL-11-01/PT/TC, The Pre-Trial Judge's Report Prepared Pursuant to Rule 95(A) of the Rules of Procedure and Evidence, 25 October 2013, paras 55-65. Extract quoted from para 66.
[4] Prosecution Response to Oneissi Defence Request for Disclosure of Requests for Assistance, 10 October 2014, para. 4; Prosecution Request to Amend its Exhibit List, 15 December 2014.
[5] See STL, Official English Transcript, 11 December 2014, p. 56, lines 1-8; p. 58, lines 10-15; p. 59, lines 3-22; p. 79, line 21 – p. 89, line 15; p. 97, line 13 – p. 99. See also, Requête en réexamen de la Décision du 7 novembre 2014 et en communication de toutes demandes d'assistance se rapportant à des données téléphoniques, 23 January 2015; Prosecution Response to "Requête en réexamen de la Décision du 7 novembre 2014 et en communication de toutes demandes d'assistance se rapportant à des données téléphoniques'', 9 February 2015.
[6] S/Res/1595 (Apr. 7, 2005) ("Resolution 1595").
[7] *Ibid*, points 3 and 7.
[8] *Ibid*, points 3.2.

this end, the UNIIIC was directed to determine its own set of internal procedures based on relevant international standards, Lebanese law and judicial procedures.[9]

11. Under Rule 61 of the Rules, the Prosecution may seek the assistance of any State authority in the course of conducting his investigations into the "Hariri Attack". With respect to the Lebanese authorities, Rule 16(B) provides that where the Prosecution considers it necessary in the course of its investigations to "seize documents and other potential evidence, or undertake any other investigative measure in Lebanon", it "may request the Lebanese authorities to conduct such measures or request permission to have his staff conduct such measures themselves, or a combination thereof." The Lebanese authorities are required to comply with such requests under Rule 20(A) of the Rules, which provides that when such a request is received, the authorities "shall provide such assistance without delay".

12. Since 5 June 2009, such requests have been subject to the "Memorandum of Understanding between the Government of the Republic of Lebanon and the Office of the Prosecutor of the Special Tribunal for Lebanon Regarding the Modalities of Cooperation Between Them" ("Memorandum"). Under its Article 4, "[t]he Prosecutor General of the Special Tribunal shall make requests for assistance of any kind or requests for judicial or legal proceedings by the competent authorities and in accordance with the Lebanese Code of Criminal Procedure."

13. Neither Resolution 1595 nor the Rules confer to the UNIIIC or the Prosecution, respectively, unfettered access to any and all CDRs with no procedural safeguards.

ii. Evidence Admissibility

14. Article 19 of the Statute provides how the evidence received by the UNIIIC shall be received by the Tribunal.

15. The general rule of admissibility is set out in Rule 149(C) and (D). Besides, any evidence *shall* be excluded under Rule 162 "if its admission is antithetical to, and would seriously damage, the integrity of the proceedings", particularly if it was "obtained in violation of international standards on human rights".

16. Rule 149(A) and (B) sets out the interpretative methodology for the rules relating to evidence in the case of a lacuna, which .

17. is consistent with Article 28 of the Statute which provides that the drafters of the Rules be guided by "the Lebanese Code of Criminal Procedure, as well as by other reference materials reflecting the highest standards of international criminal procedure".[10]

[9] *Ibid*, point 6; S/2006/375, Fourth report of the UNIIIC prepared pursuant to Security Council resolutions 1595 (2005), 1636 (2005) and 1644 (2005), dated 10 June 2006, para. 111.

b. Specific requirements

18. The collection, use and retention of communication records involve specific risks of arbitrary and unlawful interference with the right to privacy. In order to ensure the respect and protection of this right, international and domestic jurisdictions have defined specific requirements to the admissibility of communication records.

19. There is universal recognition of the fundamental importance and enduring relevance of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice.[11] This right is included in Article 12 of the UDHR,[12] the ICCPR, to which 168 States including Lebanon are parties,[13] the European Convention on Human Rights ("ECtHR")[14] and the European Charter of Fundamental Rights ("Charter").[15]

20. The United Nations High Commissioner for Human Rights ("OHCHR") recently described the collection of CDRs as a very serious interference with the right to privacy.[16]

21. The Court of Justice of the European Union ("CJEU") has similarly concluded that information generated or processed by communications networks "may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained"[17] and that the retention of these data for the purpose of access by the national authorities, "directly and specifically affects private life".[18] The European Court of Human Rights ("ECHR") also found that a number of comparable measures interfere with the right to privacy.[19]

22. International institutions,[20] as well as regional and domestic Courts, have identified a number of basic safeguards against the use of arbitrary or abusive surveillance measures. They all aim to guarantee that where a measure interferes with the right to privacy, it is

---

[10] Following the principle of *generalia specialibus non derogant*, the order of precedence set out in Rule 149 must prevail over that provided for in Rule 3(A). Rule 3(A) lists the same sources, but places the LCCP as the final instrument to be considered "as appropriate".
[11] See for a recent illustration A/HRC/27/37, Report of the Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age", 30 June 2014 ("A/HRC/27/37").
[12] Article 12.
[13] Article 17.
[14] Article 8.
[15] Articles 7 and 8.
[16] A/HRC/27/37, paras 19 and 20.
[17] CJEU, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* para 27.
[18] *Ibid*, para 29.
[19] ECHR, Malone v UK, 2 August 1984; ECHR, Rotaru v. Romania, 4 May 2000; ECHR, Amann v. Switzerland, 16 February 2000; ECHR, Niemietz v. Germany, 16 December 1992; ECHR, Wieser and Bicos Beteiligungen GmbH v. Austria, 16 October 2007; ECHR, Iliya Stefanov v. Bulgaria, 22 May 2008; ECHR, Robathin v. Austria, 3 July 2012; ECHR, S. and Marper v the UK, 4 December 2008; ECHR, Bykov v Russia, 10 March 2009; ECHR, Peck v. the UK, 28 January 2003; ECHR, Uzun v Germany, 2 September 2010; ECHR, Brunet v. France, 18 September 2014.
[20] A/HCR/27/37, paras. 37-38.

defined and implemented in accordance with the applicable procedural requirements; and is necessary and proportionate to the achievement of a legitimate and narrowly-defined aim.

23. The control and oversight of an independent and impartial authority has been considered as the only adequate and effective protection against arbitrary interferences by executive authorities. This applies "[e]ven where national security is at stake, [as] the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence."[21]

24. The ECHR has held that interference by the executive authorities with the right to privacy should be subject to an "effective control" of the legality and the necessity of the investigative measure.[22] To be effective, such control should be assured by the judiciary as no other control affords better guarantees of independence, impartiality and a proper procedure.[23] In that respect, it stated that a Prosecutor whose position depends on the Minister of Justice, who receives his instructions when prosecuting and investigating from that same Minister and reports to him or her on their execution, is not structurally independent from the executive. Thus, a Prosecutor does not offer the guarantees of independence and impartiality required to conduct an impartial judicial review.[24]

25. The need for such safeguards is greater where the protection of personal data undergoing automatic processing is concerned, particularly when such data are used for police purposes. Domestic laws must ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which these data are stored.[25]

26. The right to privacy is protected by the Constitution of the United States of America ("USA")[26] and by the Canadian Charter of Rights and Freedoms.[27] Both the American[28] and

---

[21] ECHR, Al Nashif v. Bulgaria, 20 June 2002, paras. 123-124.
[22] ECHR, *Brunet v. France*, 18 September 2014, para. 35; ECHR, *Gustanovi v Bulgaria,* para. 224; ECHR, *Ilyia Stefanov v Bulgaria*, para 41; ECHR, *Robathin v Austria*, para. 47.
[23] ECHR, *Uzun v Germany*, 2 December 2010, paras. 71-72; ECHR, *Lupsa v. Romania*, 8 September 2006, para. 34; ECHR, *Huvig v. France*, 24 April 1990, paras. 33-34; ECHR, *Klass and others v. Germany*, 6 September 1978, para. 55.
[24] ECHR, *Moulin v. France*, 23 November 2010, para. 55-59; See also *a contrario* ECHR, *Al Nashif v. Bulgaria*, 20 June 2002, para. 125.
[25] ECHR, *Brunet v. France*, 18 September 2014, para. 35; ECHR, *S and Marper v. the United Kingdom,* 4 December 2008, para 103.
[26] Constitution of the USA, Fourth Amendment.
[27] Canadian Charter of Rights and Freedoms, section 8.
[28] *Riley v. California*, 573 US (2014); *USA v. Davis*, Appeal from the United States District Court for the Southern District of Florida, 11 June 2014, see pp. 13 and 23.

Canadian[29] Courts have considered that substantial privacy interests were at stake in the context of the collection, use and retention of CDRs.

27. In the USA, the Stored Communications Act permits the Government to obtain an order requiring "a provider of electronic communication service … to disclose a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications)" when the Government offers "specific and articulable facts showing that there are reasonable grounds to believe that the… records… sought are relevant and material to an ongoing investigation."[30] Such statutory authorisations must comply with the Fourth Amendment which prohibits searches and seizures. To obtain any information implicating an individual's privacy interests, such as cell phone metadata, the government must obtain a written permission from a court of law or search warrant. Such warrants must be supported by probable cause, limited in scope and executed accordingly. [31]

28. Similar limits are placed on searches in Canada. First, a peace officer must obtain a search warrant from a judge before conducting any search. Second, the search must not be more intrusive than necessary to achieve its objective.[32] Evidence collected in breach of these provisions and of the rights guaranteed by the Canadian Charter of Rights and Freedoms can be excluded.[33]

29. The right to privacy is indirectly guaranteed by the Lebanese Constitution pursuant to Articles 8 and 13 and the express references in the Preamble to two human rights instruments: the UDHR and the ICCPR.[34] Adopting the reasoning of the Appeals Chamber,[35] the right to privacy, as provided for in the UDHR and the ICCPR, has constitutional value under Lebanese law.

30. Further, in the context of an open judicial investigation, the competent authority to seize and collect CDRs is the investigating judge. When CDRs are seized and collected by security services gathering intelligence, Lebanese law provides for specific provisions. Thus, in judicial cases like that of *Ayyash et al.*, a judge must authorise or order the seizure of CDRs.[36]

---

[29] Supreme Court of Canada, *R. v. Plant* (1993) 3 S.C.R. 281 at 293, 5 November 1993; Supreme Court of Canada, *R. v. Telus Communications Co* (2013) 2 S.C.R. 3 at p. 6, 27 March 2013.
[30] 18 U.S.C. §§2703(c)(1), (d).
[31] See for example *United States v. Jones*, 132 S. Ct. 945 (2012) and *Riley v. California*, 573 U.S. (2014).
[32] See, Criminal Code of Canada, s. 487.1 and seq.; Supreme Court of Canada, *R. v. Vu*, (2013) 3 S.C.R. 657.
[33] See, Criminal Code of Canada, s. 487 and Supreme Court of Canada, *The Canadian Broadcasting Corporation v. The Attorney General for New Brunswick*, (1991) 3 R.C.S. 469, p. 482.
[34] See CH/AC/2011/01, Decision on partial appeal by Mr El Sayyed of Pre-Trial Judge's decision of 12 May 2011, 19 July 2011, para. 60 and footnote 102; Lebanese Constitutional Council, decision no. 2/2001, 10 May 2001, published in Al-majless al-doustouri (2001-2005) [Constitutional Council review (2001-2005)], at 150.
[35] *Ibid*, para. 61.
[36] The regime applicable to search and seizures in general is defined under article 98 of the LCCP.

31. In short, international and domestic laws consider that limits must be set to the retention and use of such data in order to achieve a proper balance between the competing interests of State security and preserving respect for private life, including a proper judicial oversight, is necessary to verify the proportionality of the interference found to exist.

2. Steps followed to collect the CDRs

32. According to the information available to the Defence at this stage, the CDRs which underlie the CSTs sought to be introduced were collected by either the UNIIIC or the Prosecution as follows:

a. CDRs were collected in Lebanon by the UNIIIC and the Prosecution from the CSPs between approximately 1 August 2005[37] to 26 February 2014;[38]

b. On 5 August 2005, further to a meeting with UNIIIC Commissioner Deltev MEHLIS, Marwan HAMADE, in his capacity of Minister and in agreement with his government, instructed the services of the Ministry of Telecommunications to fully cooperate with the UNIIIC, thus lifting an existing ban;[39]

c. Based on that authorisation, the UNIIIC (between 2005 and 2009) and the Prosecution (from 2009) collected CDRs in Lebanon from the CSPs, using "warrants" and RFAs;[40]

d. The warrants and RFAs were either addressed directly to the telephone companies or actioned through Prosecutor General Said MIRZA;[41]

e. The temporal scope of the CDRs collected, retained and used covers a period between January 2003 and December 2010.[42] It includes CDRs and SMSs. From at least 4 May 2006, the material scope of the CDRs requested include originating and receiving phone numbers, date, time and duration of

[37] See 4D00092.
[38] 60294745 in 60294735-60294748, (Pending R91).
[39] STL, Official English Transcript, 11 December 2014, p. 9, lines 11 – 16; p. 10 line 18 – p. 11 line 3; p.15, lines 12-25; p.21, line 17 – p. 22, line 4; p. 23, lines 13-17; p. 27 line 25 – p. 28 line 4.
[40] STL, Official English Transcript, 11 December 2014, p. 13 lines 1-9, exhibit 4D00092 ; p. 15, lines 6-25 ; p. 14, lines 16-21 ; p. 26, lines 3-5, exhibit 4D00093 ; p. 27 line 22 – p. 28 line 4; p. 28, lines 13-17; p. 41, lines 21-23, exhibit 4D00094; p. 42, lines 21-24, exhibit 4D00095 ; p. 45, line 17 – p. 48 line 2, exhibits 4D00096 and 4D00097; p. 50, lines 17-21, exhibit 4D00098.
[41] Exhibit 4D00091; STL, Official English Transcript, 11 December 2014, p. 9 line 17 – p. 10 line 13; p. 31, lines 5 to 10; p. 43 line 19 – p. 44 line 21.
[42] See 60283862-60283876 (Annex A).

a call, IMEI and IMSI of the phone numbers and the activated cell-sections.[43]

f. The corresponding subscriber-related information, when requested,[44] includes the IMSI identity, first name, father's name, last name, date of birth, address, category of subscriber, activation date, de-activation date and subscriber's customer identity as referenced in the system.[45]

g. The CDRs collected and retained as described above were subsequently used to produce the CSTs, object of the Prosecution's Motions for Admission dated 28, 29, 30 January and 2, 3 February 2015.[46]

h. In particular and in relation to the purple phones, the CDRs used to produce these CSTs were requested:

   i. by the OTP through an RFA directed to ALFA, via the Lebanese Prosecutor General and the Ministry of Telecommunications;[47]

   ii. by the OTP through an RFA directed to ALFA, via the Lebanese Prosecutor General;[48]

   iii. by the OTP, without an RFA, from ALFA;[49] and by UNIIIC through an RFA directly from ALFA.[50]

i. They were subsequently used by PRH230 who produced the CSTs.[51]

j. The CDRs used to produce SMS CSTs were requested by the OTP from MTC, through the Prosecutor General and the Ministry of Telecommunications.[52]

---

[43] 4D00093.
[44] 4D00093.
[45] 4D00093.
[46] Red Motion, Annex D, 60303181-60303207; Green Motion, Annex D; 60303130-60303166; Purple Motion, Annex D, 60303431-60303440 and 60303441-60303451; Blue Motion, Annex D, 60303208-60303242 and 60303243-60303265; Yellow Motion, Annex D, 60303461-60303474.
[47] R91-805028, R91-804315, item with ERN 60294735-60294748.
[48] R91-800183, R91-804196, R91-800935.
[49] R91-100029.
[50] R91-100032, item with ERN 10003257-10003257B, R91-800192.
[51] For the CST of 3419018 (CST-0303), the following Communication Data were used: R91-805121, R91-800192, R91-804196, R91-800935, 60294735-60294748 (Pending R91); for the CST of 3575231 (CST-0305), the following Communication Data were used: R91-805121, R91-800192, 60294735-60294748 (Pending R91); for the CST of 3598095 (CST-0388), the following Communication Data were used: R91-805121, 60294735-60294748 (Pending R91).
[52] R91-800199.

k. They were subsequently used by PRH377, who produced the SMS CST of 3598095.[53]

3. The CDRs were collected, are used and retained illegally

33. As stated above, the right to privacy that covers CDRs can only be infringed to the extent necessary to fulfil the narrowly-defined, reasonable and legitimate purposes of the investigation; after having gained approval from the relevant authorities and adhered to the applicable procedure.

34. A Lebanese independent commission[54] has confirmed that, in the context of intelligence gathering as opposed to judicial investigation "providing the full communication database on all Lebanese territories in a periodic manner violates the provisions of effective laws because it amounts to a clear violation of basic freedoms".[55] The same independent commission also considered illegal a similar authorization to transfer the "full contents of SMSs sent through the two operating mobile telephone companies all over the Lebanese territories".[56] Though the opinion of this commission is only consultative, it states the obvious: the wholesale transfer of CDRs and accompanying personal information of almost all of Lebanon to foreign entities, for a period stretching between 2003 and 2010, is not legal in the context of intelligence gathering, which makes it even worse when collected in the context of a judicial investigation.

35. In any case, any request involving the collection of CDRs would have required a specific authorisation from an investigating judge prior to its execution[57] or at least some form of independent judicial review focusing on the justification provided for such a wide scope. This was not the case.

36. Indeed, from the information provided by M. HAMADE and from the documents disclosed to the Defence, it is obvious that no-judge was involved at any of the procedural stages followed by either the UNIIIC or the STL Prosecutor. Besides, M. HAMADE confirmed that all these requests were sought and obtained either directly from the two operating mobile telecom companies or through the Lebanese Public Prosecutor who report

---

[53] ECT-SMS-0113 SMS CONTENT.
[54] 4D00100.
[55] In an opinion dated 8 November 2012 on a Council of Ministers Decision taken in application of article 9 of Law 140/99 to authorise the transfer of the entire communication data of Lebanon from 19 September 2012 to 31 December 2012 data to security and military agencies, 4D00104. Note however that according to the interpretation of former Minister of Telecommunications Marwan HAMADE, the material scope of Law 140/99 is limited to interceptions and does not include Communication Data. See STL, Official English Transcript, 11 December 2014, p.55, lines 20-21.
[56] In an opinion dated 21 November 2012 on a Council of Ministers Decision taken in application of article 9 of Law 140/99 to authorise the transfer of the full contents of SMSs sent through MIC1 and MIC2 all over the Lebanese territories, 4D00105.
[57] See Law 140/99, article 2.

to the Minister of Justice.[58] The Prosecutor General of Lebanon, the UNIIIC or the Prosecution cannot be considered as neutral and independent judicial authorities, which could have legally received without any prior authorisation or control the whole of the CDRs as described above. In particular, UNIIIC and then the STL Prosecutor have been transferred the entire CDRs for the telephone number allegedly attributed to M. Oneissi with no prior authorisation and without any judicial control of the reasons and investigative leads justifying such a measure. Finally, none of the warrants or RFAs issued in relation to CDRs and disclosed to the Defence include any explanation or justification as to why such a wide scope was justified and proportionate to a legitimate aim pursued.

4. Admission of the CSTs would seriously damage the integrity of the proceedings

37. As set out by the CJEU, and as is made clear by the substantively uniform content of the right to privacy at both international and domestic law, the transfer of eight years' worth of private data belonging to the citizens of Lebanon and to the telephone number allegedly attributed to M. Oneissi, to an international investigative body in the total absence of any control – prior or post its collection - is both unprecedented and wholly illegal.

38. Before most civil law domestic jurisdictions, the mere fact that a piece of evidence was obtained illegally would suffice to guarantee its exclusion.[59] In Lebanon, Article 179 of the Lebanese Criminal Code requires that each offences charged be proved on the basis of any sufficient proof, provided that such proof is **legal**. In other words, evidence must be collected in compliance with the applicable law and procedures to be admissible. This was obviously not the case for the CDRs. Therefore, it could not have been used as evidence before a Lebanese judge and court and under these circumstances; it cannot be used before this Tribunal, and particularly with respect to the CDRs of the telephone number attributed to M. Oneissi over several years.

39. Before this Tribunal, Rule 162 provides that evidence that "is antithetical to, and would seriously damage, the integrity of the proceedings" must be excluded; which includes the mandatory[60] exclusion of evidence that was "obtained in violation of international standards on human rights". This evidence reaches this threshold. When seen in light of the principles described above, the astonishing scope of the CDRs collected becomes clear. Whether viewed per request (many of which spanned two or more years) or cumulatively, the Prosecution has obtained the CDRs of almost every citizen who made phone calls in Lebanon

[58] STL, Official English Transcript, 11 December 2014, p. 44, lines 11-25.
[59] See article 179 of the LCCP.
[60] Rule 162(B) "shall".

– from a mobile, landline or public phone –from 2003 to 2010.[61] Within the bulk of this data would be the CDRs of the telephone number attributed to M. Oneissi and which were used to generate the CSTS which the Prosecution seeks to have admitted. Such a wide personal, temporal and geographical scope cannot be considered proportionate to a legitimate aim in a democratic society.

40. The conduct of the UNIIIC and the Prosecution is related to its primary mandate, which is to promote the rule of law at the national and international levels. The Trial Chamber has not only the power, but also the duty to vindicate the rule of law and redress the wrongdoings resulting from the UNIIIC and Prosecution's practices by following as the Lebanese independent commission. And considering the illegally obtained CDRs, within which the Oneissi CDRs would be included, as admissible evidence would amount to condone the practices described above, equivalent to those implemented by the NSA, and recently condemned in the United Kingdom by the Investigatory Powers Tribunal.[62]

41. For these reasons, the Defence requests that the Trial Chamber dismisses the Prosecution's Motions for the Admission of the CSTs and refrain to rule on the admissibility of any other Communication Evidence until the legality of the collection of the CDRs has been the subject of a public hearing.

B. RELIABILITY

42. Should the Trial Chamber conclude that the CDRs were legally obtained, the Defence submits that it cannot admit the CSTs at this stage as it is not possible to ascertain their reliability under Rule 149(C) prior to hearing the *viva voce* testimony of the relevant witnesses.

43. The CSTs were generated exclusively with a view to supporting the theory of the Prosecution. The CSTs are supposed to be the graphic representation as understandable tables of years of collection and processing of CDRs by various entities.[63] Once obtained and transferred to the Prosecution, the CDRs were processed by its experts and investigators. It was first uploaded in the Structured Query Language (SQL) Database which was then used by the Prosecutor to filter the data and produce the CSTs.[64] Within that process, calls that the Prosecution deemed irrelevant were removed; then from the remaining data, duplicates were

[61] See Annex A; Annex B (CDR Graphic Table produced by the OTP); R91-803948; R91-800196.
[62] A judicial body, independent of the British government, established by the Regulation of Investigatory Powers Act 2000 (RIPA), which hears complaints about surveillance by public bodies. It found on 6 February 2015 that the regime that governs the sharing between Britain and the US of electronic communications intercepted in bulk was unlawful. Investigatory Powers tribunal, Cases Nos IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173-H, IPT/13/194/CH, IPT/13/204/CH, *Liberty and others* v. *Secretary of States for Foreign and commonwealth Affairs and others*, 6 February 2015.
[63] As noted in the Purple Motion, para 5.
[64] See R91-805079, in particular Annex A.

removed, and errors were removed or corrected by reference to other, unidentified, materials.[65] The resulting CST, though derived from the business records of the CSPs, is far removed from the original CDRs and can only be seen as the Prosecution's work product.

44. The reliability of the CSTs depends *inter alia* on three broad factors: (i) the processes followed by the CSPs in recording, maintaining, and producing the CDRs; (ii) the chain of custody of the CDRs from the CSPs to the UNIIIC then to the Prosecution, and from the CSPs directly to the Prosecution; and (iii) the process of transforming the various CDRs into CSTs.

45. The Prosecution has acknowledged the second and third factors in its Motion. As to the first, it states that the "CDRs, SMS content records and cell [s]ite information used to produce the Purple Phone CSTs and SMS CSTs are the business records of the CSPs",[66] but does not explain their creation or maintenance. As to the second, it "intends to lead evidence on the creation, storage, and retrieval of the underlying material at a later date."[67] As to the third, it explains the production of the CSTs from the CDRs;[68] states that it has undertaken a number of audits to ensure consistency;[69] and seeks to rely on the witness statements of PRH230, PRH308 and PRH377 explaining the production process.[70]

46. None of the documents listed in the four annexes[71] provide any relevant information – for example, basic information about the software and hardware used to create, maintain, and export the CDRs; or any indication that the CDRs themselves are accurate. The Witness Statement of PRH064[72] sets out technical information in a very general way.[73] The only information that is provided as to the production of the CSTs has not been examined and tested by any impartial authority independent of the Prosecution. The relevant evidence that it *has* provided goes directly to the provenance of the work product and must therefore be made open to challenge prior to the assessment of reliability.

47. The Defence wants to be able to control in Court the nature of the telephone data upon which the Prosecution relies and the conditions in which such data were stored by the CSPs before being sent to the UNIIIC or the Prosecutor. The Defense has the right, before the Trial Chamber rules on the admission of the CSTs, to examine under its control whether the raw data, which is the basis of the CSTs, are data whose integrity has not been altered between

[65] *Ibid*, para 30.
[66] Purple Motion, para 26.
[67] *Ibid*, para. 28.
[68] *Ibid*, paras. 31-35.
[69] *Ibid*, para. 30.
[70] *Ibid*, paras. 5-6.
[71] To the Purple Motion.
[72] Purple Motion, Annex C, R91-804196.
[73] See paras. 13-139.

the date where the telephone communications occurred and the date where the recorded data were communicated by the CSPs to the UNIIIC and / or the Prosecutor.

48. Indeed, as recalled above, the raw CDRs were transferred to the UNIIIC and the Prosecutor in a succession of batches over the course of several years.

49. However, it does not seem, as it is, that the CDRs were the object of any judicial seizure decided under the control of a judge and aiming at preserving their content, or to have the data secured by the CSPs through the production of an authentic digital image (golden copy) before 2010, that is five years after the start of the investigations. In these conditions, and if that were the case, the integrity of the telephone data used for the CSTs which the prosecutor asks admission cannot be guaranteed.

50. The Defence is therefore entitled to question the underlying material for the CSTs and therefore wishes to cross-examine, *inter alia*, the CSPs employees or contractors, who were involved in the data repositories, those who actually produced the data and, of course, those who gave the data to the Prosecution. In addition, the Defence wishes to cross-examine the UNIIIC investigators and the Prosecution experts and investigators involved in the collection of the CDRs and in the maintenance of the SQL as well as in the production of the CSTs.

51. Such a process is the only way through which the reliability of the underlying material, and hence the reliability of the end product (the CSTs), can be assessed. The importance of cross-examination is confirmed by the discrepancies in CST-0388 set out below, which raise serious doubts about the reliability of the CSTs and their underlying CDRs:

a. 63 call and SMS records involving phone number 3598095 (attributed to ONEISSI by the OTP), available in GC-SQL database, but missing from CST-0388;[74]
b. 10 records of calls between 3598095 and MTC phone numbers, included in CST-0388, but not available in GC-SQL database;[75] and
c. 273 phone numbers in contact with 3598095 missing from CST0388.[76]

~~52.~~ A thorough review of each aspect of the CDRs via direct and cross-examination is therefore an essential precondition to the admission of the CSTs.

IV. RELIEF SOUGHT

53. The Defence requests the Trial Chamber to

a. DISMISS the Prosecution Motion for the Admission of CSTs;

[74] Annex C.
[75] Annex D.
[76] Annex E.

b. ORDER that the legality of the CDRs be adjudicated upon prior to any decision on the admissibility of the CSTs;

c. ORDER that in light of the importance of the issue, the Defence be granted the opportunity to make oral submissions;

In any case,

d. EXCLUDE and DECLARE inadmissible the CSTs, in particular those tendered for the telephone number 3598095 allegedly attributed to M. Oneissi by the Prosecution, since they were generated based on CDRs illegally collected.

Alternatively

e. ORDER the Prosecution to tender the Communication Evidence through a series of witnesses who can comprehensively address all of the reliability issues.

16 February 2015

VINCENT COURCELLE-LABROUSSE
Lead Counsel for Hussein Hassan Oneissi

PHILIPPE LAROCHELLE
Co-Counsel for Hussein Hassan Oneissi

YASSER HASSAN
Co-Counsel for Hussein Hassan Oneissi

Word count: 5,813