Cour Pénale Internationale

International Criminal Court

Original: **English**

No.: **ICC-01/04-01/10**
Date: **13 May 2011**

PRE-TRIAL CHAMBER I

Before: **Judge Cuno Tarfusser, Presiding Judge**
Judge Sylvia Steiner
Judge Sanji Mmasenono Monageng

SITUATION IN THE DEMOCRATIC REPUBLIC OF THE CONGO

IN THE CASE OF
THE PROSECUTOR v. Callixte MBARUSHIMANA

Public Document

Prosecution's response to the Defence submission of a list of potentially privileged documents and request for access to seized electronic material

Source: **Office of the Prosecutor**

Document to be notified in accordance with regulation 31 of the *Regulations of the Court* to:

The Office of the Prosecutor
Luis Moreno-Ocampo
Fatou Bensouda

Counsel for the Defence
Nicholas Kaufman

Legal Representatives of the Victims

Legal Representatives of the Applicants

Unrepresented Victims

Unrepresented Applicants (Participation/Reparation)

The Office of Public Counsel for Victims

The Office of Public Counsel for the Defence

States' Representatives

Amicus Curiae

REGISTRY

Registrar
Ms. Silvana Arbia
Deputy Registrar

Counsel Support Section

Victims and Witnesses Unit

Detention Section

Victims Participation and Reparations Section

Other

I. Introduction

1. On 6 May 2011, the Defence submitted a list of potentially privileged material[1] in accordance with the Chamber's order to "expeditiously carry out and complete its review of the relevant seized material".[2] Accordingly, the Prosecution requests that the Chamber order that the Prosecution be provided immediate access to all data contained on the hard drives presently under review ("the Relevant Hard Drives"), other than those particular documents that the Defence now claims are privileged.

2. Delay in accessing the seized electronic material severely hinders the Prosecution's ability to prepare for the currently scheduled Confirmation Hearing. The Prosecution submits that access to this material is an essential prerequisite of its right to a fair Confirmation Hearing. The Prosecution therefore requests the Chamber to set a deadline for the Prosecution's access to all remaining seized electronic material in order to preserve the fairness of the proceedings.

3. The Defence has filed its list(s) of potentially privileged documents in two "Confidential *ex parte* Defence and Registry Only" Annexes. The Prosecution submits that there is no reason to withhold access to this information, as this will not compromise the privilege allegedly attached to the *content* – that is, the substance of the confidential communications, between the suspect and his counsel, made for the purpose of securing legal advice.

4. The Prosecution submits that it is entitled to contest the Defence's claim of privilege, if it appears that the privilege is wrongly asserted as to any particular documents. Lack of access to the list(s) of potentially privileged material and related information will prejudice its ability to do so.

5. Additionally, the Prosecution cannot determine which hard drive(s) contain the potentially privileged documents. The Prosecution submits that it should be provided with this information in order to make submissions on the reasonableness of the Defence's blanket claim of privilege in respect of all the electronic media seized from the Suspect.

[1] ICC-01/04-01/10-137, 6 May 2011.
[2] ICC-01/04-01/10-105, 18 April 2011, page 8 (emphasis added).

II. Statement of Facts

6. On 11 October 2010 the French authorities conducted a search of the Suspect's residence and work premises and seized a number of documents and a large quantity of electronic media.

7. The French authorities delivered the seized material to Registry officials on 20 October.

8. On 11 February 2011 the Prosecution filed the Prosecution Request for a review of potentially privileged material,[3] alerting the Chamber to the possibility that one or more of the seized documents contained potentially privileged communications.

9. On 18 February the Defence filed its response, in which it asserted that *"privileged materials are likely to be contained in all of the following materials: … b) electronic media seized from the house of Mr. Mbarushimana capable of holding documentary data such as hard drives, cell phones containing SMS messages, compact discs, memory sticks, etc."*.[4]

10. On 4 March the Chamber issued its "Decision on the 'Prosecution's request for a review of potentially privileged material'".[5] In this decision it ordered the parties to provide the Chamber and the Registry, "no later than 9 March 2011, with a properly motivated list of keywords, if any, that can be used in a search for potentially privileged communications in the remaining Seized Material".

11. On 9 March both the Prosecution[6] and the Defence[7] submitted their proposed keyword lists.

12. On 14 March the Prosecution filed the "Prosecution Response to the 'Defence Submission of 'Keywords' for the Review of Potentially Privileged Material'",[8] in which it objected to the Defence's keyword list and specifically pointed out that "these terms extend far beyond what is appropriate to identify potentially privileged communication between the Suspect and his legal counsel and further that "the use of 'names, organisations, places' or other 'notions, concepts and topics' alone cannot distinguish between privileged and non-privileged documents".

[3] ICC-01/04-01/10-54, 14 February 2011.
[4] ICC-01/04-01/10-58, 18 February 2011, at para 9.
[5] ICC-01/04-01/10-67, 4 March 2011.
[6] ICC-01/04-01/10-71, 9 March 2011.
[7] ICC-01/04-01/10-72, 9 March 2011.
[8] ICC-01/04-01/10-77, 14 March 2011.

13. On 16 March 2011 the Single Judge issued her "Decision on the Registry's request for extension of time and on other matters regarding the review of potentially privileged material",[9] in which she:

    a. Approved the Prosecution's keyword list;

    b. Rejected the Defence's keyword list and ordered it "to 'properly motivate' and, when appropriate, reformulate keywords it has submitted".

    c. Ordered the Registry to provide to the Chamber, by 1 April, a list of documents obtained through its search until that date and a report on its progress, including an estimate of how much more time would be required to complete the task.[10]

14. On 17 March the Defence filed its "Defence submission of properly motivated keywords."[11]

15. On 30 March the Single Judge issued her "Decision on the keywords provided by the Defence for the purpose of selection of potentially privileged material",[12] in which she accepted the Defence's keyword list subject to certain reservations.

16. On 8 April the Registry filed the "Registry Report"[13] ("Report") and on 12 April it filed an Addendum to the Registry Report ("Addendum").[14]

17. On 15 April the Chamber issued its "Second Decision on matters regarding the review of potentially privileged material",[15] in which it ordered the Defence to conduct the review of the seized material and submit to the Chamber a list of the documents on which it claims privilege under Rule 73 by no later than 6 May.

18. On 18 April the Registry filed its "Further Submissions on the Processing of Part of the Seized Material",[16] indicating that of the 42 media devices seized, it was unable to access 10, as seven were faulty and three were encrypted. The Registry proposed to ask the Netherlands Forensic Institute ("NFI") to process these devices.

---

[9] ICC-01/04-01/10-80.
[10] The original deadline for this report was 1 April, but this was subsequently extended to 8 April: ICC-01/04-01/10-88, 30 April 2011.
[11] ICC-01/04-01/10-81.
[12] ICC-04/01-01/10-88.
[13] ICC-01/04-01/10-95-Conf, 11 April 2011.
[14] ICC-01/04-01/10-98-Conf, 13 April 2011.
[15] ICC-01/04-01/10-105, 15 April 2011.
[16] ICC-01/04-01/10-109, 18 April 2011.

19. On 19 April, the Defence filed the "Defence Request for OPCD Support", in which it requested the assistance of five staff members from the Office of the Public Counsel for the Defence to assist him with the privilege review.[17] This request was granted by the Single Judge on 21 April.[18]

20. On 21 April the Registry filed the "Registry Report on the Keyword Searches Performed on a Part of Seized Material".[19]

21. On 2 May the Defence filed the "Defence implementation of the second decision on matters regarding the review of potentially privileged material"[20] in which it complained of the Suspect's lack of access to the hardware and software necessary to complete the privilege review by the set date and requested permission to address the Chamber on these issues.

22. On the same day the Single Judge granted the request[21] for the Suspect to be granted access to the requested hardware and software, but refused the request to address the Chamber orally "without prejudice to the defence's right to submit observations in writing".

23. On 6 May the Defence filed the "Defence submission of a list of potentially privileged material" ("the Privilege List Filing").[22]

24. On 11 May the Single Judge ordered the Registry to submit a report concerning the Defence submission of a list of potentially privileged material[23] by no later than Thursday 12 May.

25. On 12 May the Registry filed the Registry Report on technical problems encountered by Mr Mbarushimana on the computer installed in his detention cell ("the Registry Technical Report").

[17] ICC-01/04-01/10-114, 19 April 2011.
[18] ICC-01/04-01/10-115, 21 April 2011.
[19] ICC-01/04-01/10-119, 21 April 2011.
[20] ICC-01/04-01/10-127, 2 May 2011.
[21] Decision on the "Defence implementation of the second decision on matters regarding the review of potentially privileged material", ICC-01/04-01/10-129, 2 May 2011.
[22] ICC-01/04-01/10-143, 11 May 2011.
[23] Order to the Registry to submit a report concerning the Defence submission of a list of potentially privileged material; ICC-01/04-01/10-114, 19 April 2011.

III. Submissions

The Defence failure to fully comply with Decision ICC-01/04-01/10-105

26. The Defence was ordered to "expeditiously carry out and complete its review of the relevant seized material".[24] The Defence did not request a variation of the deadline to conduct this review, despite the Single Judge explicitly reiterating its right to submit written submissions on the implementation of this decision.[25]

27. In its filing of 6 May, the Defence filed "a list of potentially privileged material".[26] However, the Defence specifically preserves its right to make additional claims of privilege "once several problems with […] hardware and software supplied to Mr Mbarushimana are resolved" without requesting an extension of the deadline to perform this future review.

28. The purported inadequacy of the facilities available to the Suspect should have been known, and reported, at the beginning of the process, not as an after-the-fact explanation for failure. Nor, in any event, is it justification for that failure. The Chamber instructed the Defence -- not the Suspect -- to conduct the privilege review, [27] and the Single Judge thereafter granted the Defence's request for the assistance of five members of the OPCD for this purpose. The filing is silent as to whether the Defence team and their OPCD assistants have reviewed all of the material. It also does not complain that the Defence or the OPCD lacked the necessary equipment, if in fact they were unable to complete the review.

29. Finally, it is unclear why the Suspect's lack of access to a printer or USB port should present a meaningful obstacle to his participation in the privilege review.[28] He can communicate to counsel any potentially privileged documents identified by simply listing the file names and paths of the relevant documents and the ERN's of the device on which they are contained.

[24] ICC-01/04-01/10-105, 18 April 2011, page 8 (emphasis added).
[25] ICC-01/04-01/10-129, page 4, 1st para.
[26] Perhaps significantly, the Defence does not refer to it as "***the*** list of potentially privileged material".
[27] ICC-01/04-01/10-105, page 4.
[28] Granting unsupervised access to the Suspect to a printer or USB port may, however, compromise the Registry's ability to monitor the communications of the Suspect and accordingly risk commission of further crimes or interference with the investigation, as confirmed by the Registry Technical Report, page 6, para d.

30. By failing to comply with the Chamber's order, the Defence is continuing to obstruct and delay the Prosecution's access to the remainder of the seized material.[29] The consequence of such delay is obvious. The Prosecution must file the Document Containing the Charges ("DCC") and List of Evidence ("LoE") it intends to rely upon at the Confirmation Hearing in three weeks. Withholding access will severely prejudice the prospects that the Prosecution can rely on the seized material and still meet this deadline.

31. Accordingly, in light of the Defence's failure to fully comply with the Chamber's order or to seek a variation of the time limit, the Prosecution respectfully requests the Chamber to order the Registry to grant it immediate access all material contained on the relevant hard drives *other than* those files identified in the Annexes to the Privilege List Filing. This will allow the Prosecution to commence its review of evidence as to which no claim of privilege is made and avoid even more unnecessary delay. [30]

Request for timely access to all non-privileged electronic data, which is essential to the Prosecution's fair trial rights

32. The Prosecution requested the search of the Suspect's premises and the seizures of his computer hard drives and other digital media because it considered that the evidence would be highly relevant to its investigation. The Chamber and the French authorities agreed. The Suspect's persistent objections to allowing the Prosecution access to the seized materials presumptively confirms the reasonableness of the initial belief that the evidence would be relevant to the case against him.

33. The Prosecution submits that the continuing and unreasonable delay in granting it access to the seized electronic data has severely prejudiced its ability to prepare for the imminent Confirmation Hearing and therefore to fulfil its duty to establish the truth and ensure the effective investigation and prosecution of crimes.[31] Delay also impedes the Prosecution's right to proceedings that are expeditious and fair vis-à-vis the Prosecution as well as the Defence.[32]

[29] That is, everything other than the potentially privileged items identified by the Defence.
[30] Should the Prosecution come across any documents which appear to be potentially privileged, it will immediately quarantine these and refer them to the Chamber for review.
[31] In terms of Article 54(1)
[32] As required by Article 64(2), *mutatis mutandis*.

34. As previously observed by this Chamber, "fairness" within the terms of Article 82(1)(d) incorporates fairness towards the accused, the victims and the Prosecution. It requires that the procedural and substantive rights and obligations of all participants be respected. In particular, that "means that the Prosecutor must be able to exercise the powers and fulfil the duties listed in Article 54".[33] Fairness has also been linked to the ability of a party to present its case.[34]

35. The Prosecution stresses that complete access to the non-privileged portions of all electronic media seized from the Suspect is essential to the preparation of its case and a condition *sine qua non* for the conduct of a Confirmation Hearing that is fair to both parties. The Prosecution anticipates that evidence contained in this electronic media is relevant and important to several aspects of its case. Information contained on his computers and in communications with other senior FDLR leaders, for example, may reveal the true extent of his knowledge of and contribution to the violence, which would be relevant to the issue of the Suspect's *mens rea*.[35] Furthermore, the pattern of communication with his alleged co-conspirators could be an important factor in establishing their common purpose, which is relevant to the mode of liability.[36]

36. The analysis of this evidence is also vital to the selection of the evidence upon which the Prosecution will rely at confirmation. For example, evidence obtained directly from the Suspect may be weightier than evidence obtained from other sources, and it would also be preferable to use evidence that poses less risk to witnesses.

37. It may also be that the contents of the electronic data will be potentially exculpatory, in which case immediate access would be essential to investigate exonerating evidence and, if necessary, terminate the proceedings. The Prosecution has a statutory duty, pursuant to Article 54(1)(a), to consider any such evidence in the course of its investigation, and it particularly should do so before it files the document containing the charges.

---

[33] ICC-01/04-135-tEN, 31 March 2006, paras. 38-39; See also ICC01/04-141, para. 48; ICC□02/04-01/05-212, paras. 10-11 . This principle has also been widely recognized, for instance in the ICTR (*Prosecutor v.Zlatko Aleksovski*, 16 February 1999 [reference?], paras 24 - 25) and the ECtHR (See for instance *Ekbatani v. Sweden* (1988) 10 EHRR 510 at para. 30;. *Barberà v. Spain*. (1988) 11 EHRR 360 at para. 18.; *Brandsetter v. Austria* (1991) 15 EHRR 213 at para. 67; and *Dombo Beheer BV v. The Netherlands* (1993) 18 EHRR 213 at para. 33. This was a civil case but the court was considering whether the requirement of equality of arms recognised in criminal cases should apply to civil cases also).

[34] ICC - 02/04 - 01/05 - 90 - US - Exp (reclassified pursuant to ICC - 02/04 - 01/05 - 135), para. 24.

[35] This could additionally contradict the Suspect's statements, as for example at his initial appearance, disassociating himself from the violence in the Kivus. .ICC-01/04-01/10-T-1-ENG ET WT 28-01-2011, page 12, line 9 – 16.

[36] The examples are by no means exhaustive.

38. The situation that the Prosecution now faces is that, nearly seven months after the seized material was delivered to the Registry and less than three weeks prior to the deadline set for it to file the Document Containing the Charges and List of Evidence, the Prosecution has yet to have access to its largest and potentially most relevant pool of evidence. The Prosecution submits that it would be manifestly unfair if it is forced to proceed to confirmation without access to these documents. Moreover, the fact that the Defence starts with a general knowledge regarding the contents of the evidence – since it was seized from the Suspect – and has had access to the bulk of this material since April[37] will place the Prosecution at a significant disadvantage.

39. The Defence attribution of blame to the Prosecution is incorrect. The seizure of the electronic media was necessary, reasonable and in keeping with internationally recognised best practices for the seizure of electronic evidence.[38] Indeed, the Prosecution submits that the chief causes of this delay have been: the Defence lateness in raising potential privilege claims; its overly-broad claims of privilege; its resistance to procedures that would focus a search through the seized electronic media for confidential communications between the Suspect and his lawyers for purposes of providing legal advice, and of course its most recent apparent failure to meet the Chamber's May 6 deadline for reviewing the materials for privilege. [39]

    a. The Suspect did not make a timely claim regarding privilege; in that regard, the Defence has been less than accurate in its assertion that it raised the claim at the time of, or shortly after, the initial search. That assertion has already been

[37] The exact date is unknown to the Prosecution.
[38] See in this regard the Association of Chief Police Officers (ACPO) "Good Practice Guide for Computer-based Electronic Evidence", pages 4, 8 – 10, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf - last accessed on 13 May 2011; Scientific Working Group on Digital Evidence (SWGDE) "Best Practices for Computer Forensics", 2006, pages 3 - 6 - http://www.oas.org/juridico/spanish/cyb_best_pract.pdf - last accessed on 13 May 2011; International Organisation on Computer Evidence (IOCE) "Guidelines for Best Practice in the Forensic Examination of Digital Technology", 2002, pages 11–14, http://www.ioce.org/fileadmin/user_upload/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf - last accessed on 13 May 2011; United States Secret Service "Best Practices for Seizing Electronic Evidence" (See "Golden Rules" and "Evidence Preservation") - http://www.forwardedge2.com/pdf/bestpractices.pdf - last accessed on 13 May 2011; Working Group Forensic IT (ENSFI) "Guidelines for Best Practice in the Forensic Examination of Digital Technology" , 2006, para 9.5, http://www.enfsi.eu/uploads/files/ENFSI_Forensic_IT_Best_Practice_GUIDE_5%5B1%5D.0.pdf - last accessed on 13 May 2011; and Council of Europe "Convention on Cybercrime", 2001, Article 19, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm - last accessed on 13 May 2011.
[39] Another contributor to the delay has been the inability of the Registry to expediently and efficiently complete the forensic copying of the seized media and attend to the subsequent keyword privilege search. In this regard, the Prosecution requested in November 2010 that the Registry outsource the copying of the seized electronic material. The Registry ultimately decided against this due to cost concerns. See ICC-01/04-01/10-53-Conf, paras. 5–7 and Conf-Anx.

comprehensively disproved.[40] There is no record that the Defence raised this issue before the French Courts. Nor did the Defence do so during the course of extensive pre-surrender correspondence with the Prosecution. The Defence also did not raise privilege at his initial appearance. It did not raise privilege in any affirmative filing before this Court.[41] In fact, it was only on 18 February, four months after his arrest and the seizures of this material, and only after the Prosecution alerted the Chamber and the Defence to its discovery of a single potentially privileged communication amongst the seized documents, that the Defence came forward to claim that privilege permeated the electronic media.

b. The failure to make a timely claim is even more remarkable given the breadth of the privilege assertion. The Defence conception of what documents ought to be considered as privileged extends well beyond communications with legal counsel in the context of a professional relationship and including legal issues unconnected with the present case. Their submission of a wide-ranging and vague keyword list, rejected by the Chamber, nonetheless successfully delayed the start of the keyword search; even the resubmitted list was clearly too expansive, since it led to a proliferation of spurious hits that rendered the process unworkable.

40. The Defence's blanket assertion of privilege over the entire collection of seized electronic media has also effectively prevented the Prosecution from accessing any of it. The Prosecution notes the Defence's assertions regarding the fact of the Suspect's familiarity with the content of the computer hard drives. That familiarity, which is singularly within the competence of the Suspect, should have made an initial focused identification of confidential communications between the Suspect and his attorney more, not less, feasible. While he may have no legal obligation, his failure to identify the confidential communications from the outset disqualifies the Defence from complaining of the ensuing delay or attributing it to prosecutorial malfeasance.

41. Accordingly, the Prosecution respectfully requests the Chamber to fix a deadline for it to be granted access to the remaining electronic media, including all documents in respect

[40] See ICC-01/04-01/10-66, 1 March 2011, at paras 29–30 and Annexes thereto.
[41] This is in contrast to the privilege which the Defence asserted in relation to the French communication intercepts. See ICC-01/04-01/10-29 14 December 2010, paras 4 and 25.

of which the Chamber rejects the Defence's claim of privilege and the contents of the 10 hard drives which the Registry has not yet been able to access.[42]

42. Having not yet seen the material, the Prosecution cannot estimate how long it will need to review this material. Once it has access, it can inform the Chamber if it is possible to perform an adequate review in advance of the presently scheduled Confirmation Hearing.

Request for access to the recently-filed Defence Annexes

43. The Prosecution does not dispute that the Chamber can withhold privileged documents from the Prosecution. However, the Prosecution submits that, as a party to these proceedings, it is entitled to know the nature of the documents that are alleged by the Defence to be privileged, so long as that information does not itself disclose the substance of a confidential privileged communication, and to make submissions as to whether documents that by their titles or metadata do not appear to be confidential communications that should be protected against disclosure

44. The Prosecution requires access to the Defence list of potentially privileged documents firstly, because it will clearly not be in a position to dispute the existence of privilege in respect of a document in circumstances where it is not even privy to its existence. Secondly, information such as the type of document, the date of creation on the hard drive, the author[43] thereof, the file name and path and the ERN of the device on which the file was contained, is itself not privileged. Again, the privilege protects against the disclosure of confidential attorney-client communications, it does not protect against disclosure of the existence, date, and nature of the document in which the communication is contained. Thirdly, the Prosecution cannot make informed submissions as to the existence of privilege as envisaged by Rule 73 unless it has this predicate non-privileged information about the nature of the document.

    a. With respect to documents allegedly subject to legal professional privilege, Rule 73(1) protects only "communications, made in the context of a professional relationship

[42] The Prosecution regards the contents of the three encrypted hard drives as particularly important, since the application of access control suggests that the data contained thereon may be incriminating.
[43] In the sense of the user who created it on the hard drive, according to the system metadata.

between a person and his or her legal counsel". [44] A document other than a communication[45] between the Suspect and one of his various counsels is not protected by a legal professional privilege.[46] Thus, for instance, documents allegedly collected by the Suspect in order to send them to counsel would not fall within the ambit of Rule 73(1), unless they were specifically contained in or attached to a communication, such as an email. Even in this case, however, the privilege would not attach to separate copies of such documents which might be found in the Suspect's possession. Such documents exist independently of any communication with counsel and the Prosecution submits that a proclaimed act (or intention) to transmit them to counsel cannot in itself clothe them with privilege.[47] Therefore, the type of file and location thereof on the hard drive will be relevant to the determination of privilege. File types such as MS Excel, MS PowerPoint and multimedia files are inherently unlikely to contain communications and therefore privileged documents. Similarly, the date of creation is relevant, since documents created prior to the Suspect becoming aware of the existence of the current investigation are unlikely to be privileged. The file name may also contain important clues as to whether or not the document is a privileged communication.

b. With respect to alleged priest-penitent privilege, the Prosecution reiterates that this privilege is limited by Article 73(3) to "communications made in the context of a sacred confession". Therefore, the type, location, date and title of the potentially privileged files would similarly not be protected from disclosure as a privileged communication, and additionally would be information for which the Prosecution has both entitlement and need.

[44] The phrase "in the context of a professional relationship" has been interpreted by one expert commentator as meaning "for the purposes of obtaining legal advice". Donald K. Piragoff in Lee (2002), page 360. "A reference to "the context of the professional relationship" would subtly enable the Court not to recognize a privilege if the communication was outside of the bounds of a professional relationship; eg, it was not made for the purpose of giving or receiving legal advice…"

[45] Since this term is not defined, its ordinary meaning should be applied. In this sense it would include letters, faxes, emails and records of oral conversations, whether telephonic or in person.

[46] In this regard, the Prosecution notes the reference in the last paragraph of the Privilege List Filing to "items defined as potentially privileged **and communications related thereto**" (emphasis added). This implies that the Defence is claiming privilege in respect of documents **other** than communications.

[47] To rule otherwise would open the door for any suspect to allege that any incriminating documentary evidence found in his possession was collected for the purposes of communicating to counsel and is therefore privileged.

c. Finally, the same information is also required to allow the Prosecution to make submissions in the event that the Defence intends to claim any other class of privilege under Rule 73(2)(a)-(c).

45. For these reasons, the Prosecution submits that it is entitled to have access to the Defence list contained in the Annexes to the Privilege List Filing. In the event that the list provided by the Defence does not provide the information listed above, the Chamber is respectfully requested to order the Defence, alternatively the Registry, to provide such information in respect of all documents listed in the Annexes in respect of which the Defence claims privilege.

Request for details regarding number and location of potentially privileged documents

46. The Prosecution notes the Defence submissions that the Suspect is intimately familiar with the contents of the various hard drives and other items of electronic media seized from him.[48] The Prosecution also notes the Defence's assertion that *"privileged materials are likely to be contained in **all** of the following materials: … b) electronic media seized from the house of Mr. Mbarushimana capable of holding documentary data such as hard drives, cell phones containing SMS messages, compact discs, memory sticks, etc."*.[49] The Prosecution observes that it is on the strength of this assertion that the Prosecution has to date been denied access to all of the seized electronic data.

47. In the light of the above, the Prosecution respectfully requests that the Chamber order the Defence, alternatively the Registry, to provide it with details of the number of potentially privileged items identified by the Defence on each of the hard drives to which they have been provided access to date. It is unfair to allow the Defence to make such sweeping assertions without allowing the Prosecution to verify or dispute them. Moreover, if the Defence has overstated the presence of privileged communications on all the seized electronic media, that fact will bear on potential future allegations that prosecutorial misconduct caused a delay in the proceedings.

[48] ICC-01/04-01/10-127, para. 16 ; ICC-01/04-01/10-137 paras. 2 and 3.
[49] ICC-01/04-01/10-58, 18 February 2011, at para 9 (emphasis added).

IV. Conclusion

48. The Prosecution requests an order:

a. That the Prosecution be granted immediate access to all data on the Relevant Hard drives other than the specific items identified by the Defence as potentially privileged;

b. That the Chamber fix a deadline for the Prosecution to be granted access to all remaining seized electronic data;

c. That the Prosecution be allowed access to the Annexes to the Privilege List Filing which are presently filed *ex parte*;

d. That, in the event that the list provided by the Defence does not provide the information listed in paragraph 44 above, the Defence, alternatively the Registry, provide such information to the Prosecution in respect of all documents in respect of which the Defence claims privilege; and

e. That the Defence, alternatively the Registry, provide the Prosecution with details of the number of potentially privileged items identified by the Defence on each of the Relevant Hard Drives.

Luis Moreno-Ocampo
Prosecutor

Dated this 13th day of May 2011
At The Hague, The Netherlands