Cour Pénale Internationale

International Criminal Court

Original: **English**

No.: **ICC-01/04-01/10**
Date: **27 June 2011**

PRE-TRIAL CHAMBER I

Before: **Judge Sanji Mmasenono Monageng, Presiding Judge**

Judge Sylvia Steiner

Judge Cuno Tarfusser

SITUATION IN THE DEMOCRATIC REPUBLIC OF THE CONGO

IN THE CASE OF
THE PROSECUTOR v. Callixte MBARUSHIMANA

Public Document

Prosecution's request for review of intercepted internet data

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

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
Esteban Peralta Losilla

Victims and Witnesses Unit

Detention Section

Victims Participation and Reparations Section

Other

Submissions

1. On 21 January 2011 the Prosecution received from the French authorities a hard drive containing internet data intercepted from the Suspect over the period July to October 2010 ("the Internet Data").[1] This data was disclosed in its original format to the Defence in terms of Rule 77 on 2 May 2011. Although this data is accessible using the FTK software available to the Defence, this requires considerable technical expertise. To date the Defence has been unable to access the data, even with the assistance of Counsel Support Section ("CSS"). The Prosecution understands that the CSS presently lacks the capability to provide the necessary technical assistance to enable the Defence to access the data.
2. In order to facilitate its own access to this data, the Prosecution consulted the providers of the software used by the French authorities to intercept it. They provided the Prosecution with a computer terminal on which the data may be viewed. The system does not, however, allow the data to be searched or exported. It is therefore unsuited to the effective review of the data, nor does it provide the means to place relevant evidence before the Pre-Trial Chamber ('the Chamber") in eCourt-compliant format.
3. A preliminary review of sample data by the Prosecution's Knowledge Based Unit ("KBU") revealed the presence of potentially privileged communications among this data. For this reason, the data has been quarantined to date by KBU pending the identification of a suitable means to search for and extract potentially privileged material for subsequent review by the Chamber.
4. The Prosecution consulted with CSS to find an efficient and cost effective solution to both the Prosecution and Defence difficulties in respect of this data.
5. The Prosecution has now identified a service provider who is able to convert the data into a format that will be more readily accessible, searchable and compatible with the eCourt protocol. This will allow both the Prosecution and Defence to

[1] This includes internet browsing history, webmail messages and "voice-over-internet-protocol" ("VOIP") call data.

more easily access and review the data and export relevant material into their respective Ringtail systems. It will also permit a privilege review to be conducted.

6. The Prosecution, in consultation with CSS, intends to forward a forensically sound copy of the Internet Data for processing by the service provider as soon as the necessary procurement processes are completed. The service provider has indicated that it will take up to three weeks to complete processing before the data may be reviewed in its system for privilege or relevance to the case.
7. The Prosecution proposes that after processing by the service provider is completed, the service provider will facilitate the identification of potentially privileged material by KBU, using keyword searches. This material would be extracted from the processed Internet Data and provided to the Chamber for review. A copy will also be provided to the Defence. The remainder of the data would be made available to both the Prosecution and Defence for further review for potentially relevant items.
8. KBU will prevent access to any potentially privileged data by anyone in the Prosecution outside their unit until the Chamber has reviewed such data and issued its decision.
9. The Prosecution submits that this procedure (*mutatis mutandis*) worked successfully in respect of the seized documents. Firstly, the keyword searches appear to have successfully identified all privileged communications amongst the seized documents, as neither the Prosecution nor the Defence has since identified any further privileged documents.[2] Secondly, the advanced search techniques employed by the KBU succeeded in limiting the number of non-privileged documents submitted for review.[3]
10. The Prosecution therefore submits that there is no reason to deviate from this process in respect of the Internet Data.

[2] As ordered by the Chamber in its decision ICC-01/04-01/10-67, 4 March 2011.
[3] Of the 179 documents identified as potentially privileged, only half were found not to be privileged. This is in contrast to the vast number of spurious hits produced by the Registry's keyword search of the seized electronic material.

11. Nothing in the proposed procedure would, however, prevent the Defence from identifying any documents alleged to be privileged and forwarding these to the Chamber for review.
12. The Chamber is accordingly requested to designate itself to review any potentially privileged material identified by the Prosecution, alternatively by the Prosecution and the Defence, among the Internet Data.

Luis Moreno-Ocampo,
Prosecutor

Dated this 27th day of June 2011

At The Hague, Netherlands