

**Cour
Pénale
Internationale**



**International
Criminal
Court**

Original: **English**

No.: **ICC-01/14-01/18**

Date: **29 June 2020**

TRIAL CHAMBER V

Before: Judge Bertram Schmitt, Presiding Judge
Judge Péter Kovács
Judge Chang-ho Chung

**SITUATION IN THE CENTRAL AFRICAN REPUBLIC II
IN THE CASE OF *THE PROSECUTOR v.*
*ALFRED ROMBHOT YEKATOM & PATRICE-EDOUARD NGAÏSSONA***

Public

Motion to Exclude Call Location Evidence

Source: Defence for Mr. Alfred Rombhot Yekatom

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

The Office of the Prosecutor

Ms. Fatou Bensouda

Mr. James Stewart

Mr. Kweku Vanderpuye

Counsel for Mr. Yekatom

Me Mylène Dimitri

Mr. Peter Robinson

Counsel for Mr. Ngaiïsona

Me Geert-Jan Alexander Knoops

Legal Representatives of Victims

Mr. Dmytro Suprun

Mr. Abdou Dangabo Moussa

Ms. Elisabeth Rabesandratana

Mr. Yaré Fall

Ms. Marie-Edith Douzima-Lawson

Ms. Paolina Massidda

Legal Representatives of Applicants

Unrepresented Victims

**Unrepresented Applicants
(Participation / Reparation)**

**The Office of Public Counsel for
Victims**

**The Office of Public Counsel for the
Defence**

Me Xavier-Jean Keïta

States' Representatives

Amicus Curiae

REGISTRY

Registrar

Mr. Peter Lewis

Counsel Support Section

Victims and Witnesses Unit

Mr. Nigel Verrill

Detention Section

**Victims Participation and Reparations
Section**

INTRODUCTION

1. Counsel representing Mr. Alfred Rombhot Yekatom (“Defence” and “Mr. Yekatom”, respectively) respectfully move for a ruling, pursuant to Article 69(7) of the Statute, that prior judicial authorisation is required to obtain call location data, and excluding all call location data evidence obtained without such authorisation.
2. Call location data is obtained from the use of cell phones. Cell phones operate by connecting to a set of radio antennas, usually mounted on a tower, called “cell sites”. Cell phones continuously scan their environment looking for the best signal, which may come from the closest cell site.¹ When a phone connects to a cell site to make a call, it generates a time-stamped record known as cell-site location information. This information is included by telecommunication companies on call data records it maintains.
3. Law enforcement access to call data records allows it to trace a person’s location at a given date and time by determining which cell site the person’s phone was connected to at the time the phone was used to make or receive a call. This allows law enforcement, in principle, to track a person’s whereabouts to the geographical area covered by that cell site.
4. The call location data for phones attributed to Alfred Yekatom that was obtained by the Prosecution would allow it to track his whereabouts minute-by-minute for a two-year period.
5. The Defence contends that there is an international human right to privacy to be free from having one’s location continuously tracked by law enforcement. While this right is not absolute, it requires that law enforcement obtain prior judicial authorisation to obtain call location data from one’s cell phone. The

¹ Although there are a number of factors that can determine the connecting cell.

Prosecution obtained records of Mr. Yekatom's location without judicial authorisation. To admit this call location data into evidence would be antithetical to the integrity of the proceedings. Therefore, the call location data should be excluded.

RELEVANT PROCEDURAL HISTORY

6. On 24 September 2014, the Office of the Prosecutor opened an investigation into crimes committed in the Central African Republic since 2012.²
7. On 13 February 2015, the Office of the Prosecutor sent a Request for Assistance ("RFA") to the Central African Republic authorities requesting that it be provided with all existing records of the call data for seven individuals and 18 telephone numbers for the period from 1 August 2012 to date, including the location of the telephone(s) and the SIM card(s) for these numbers (and the corresponding transmission antenna) at the time of the calls. This request included two telephone numbers for Mr. Yekatom.³
8. A second request for three additional telephone numbers for Mr. Yekatom was sent on 5 June 2015.⁴
9. The Central African Republic's Prosecutor transmitted the requests to the telecommunication companies and those companies provided call data records to the Office of the Prosecutor. No judicial authorisation was sought or obtained. The records included call location data.
10. In the following years, the Office of the Prosecutor sent at least 20 additional RFAs and received thousands of call location records in this manner without judicial authorisation. It is believed that this practice continues to this day.

² [Statement of the Prosecutor of the International Criminal Court on opening a second investigation in Central African Republic](#), 24 September 2014.

³ CAR-OTP-2117-0109-R02.

⁴ CAR-OTP-2117-0129-R02.

11. The Office of the Prosecutor compiled the call location data and used it during the confirmation of charges proceedings to show Mr. Yekatom's location at pertinent times.⁵ The Prosecution is expected to seek to submit this evidence during the trial as well.

RELEVANT PROVISIONS

Article 69 of the Statute

7. Evidence obtained by means of a violation of this Statute or internationally recognized human rights shall not be admissible if:

(a) The violation casts substantial doubt on the reliability of the evidence;
or

(b) The admission of the evidence would be antithetical to and would seriously damage the integrity of the proceedings.

8. When deciding on the relevance or admissibility of evidence collected by a State, the Court shall not rule on the application of the State's national law.

ARGUMENT

A. The Framework for Deciding Motions to Exclude Evidence Under Article 69(7)

12. In the *Bemba et al* case, the Appeals Chamber held that Article 69 (7) envisages two consecutive inquiries: First, it must be determined whether the evidence at issue was "obtained in violation of the Statute or internationally recognised human rights". If the answer is in the affirmative, the second step is to consider whether "the violation casts substantial doubt as to the reliability of the evidence" (Article 69(7)(a)) or "the admission of the evidence would be

⁵ [ICC-01/14-01/18-282-Conf-AnxJ1](#), p. 221-22.

antithetical to and would seriously damage the integrity of the proceedings” (Article 69(7)(b)).⁶

13. The first step of the inquiry involves only whether the evidence was obtained in violation of the international human right of privacy, as the Defence does not contend that the evidence was collected in violation of any provision of the ICC Statute.
14. The Chamber must first determine if there is a right to privacy in call location data and, if so, whether the method the Prosecution used to obtain that data violated that right. Investigative activities are measured not against domestic law, but by whether they conform to internationally recognised human rights. A violation of national law is neither a necessary nor sufficient condition of exclusion under Article 69 (7).⁷
15. When considering the second step of the Article 69(7) inquiry, the only question arising, should it be found that the call location data was obtained in violation of the international right of privacy, is whether admitting the evidence would be antithetical to and would seriously damage the integrity of the proceedings. The reliability of the call location data is not at issue in this motion.⁸
16. Therefore, this motion will first address the question of whether there is an internationally recognised right to privacy in call location data.

⁶ *Prosecutor v. Bemba et al*, [Judgement on the appeals of Mr Jean-Pierre Bemba Gombo, Mr Aimé Kilolo Musamba, Mr Jean-Jacques Mangenda Kabongo, Mr Fidèle Babala Wandu and Mr Narcisse Arido against the decision of Trial Chamber VII entitled “Judgment pursuant to Article 74 of the Statute”](#), 8 March 2018, ICC-01/05-01/13-2275-Red, para. 280 (“*Bemba et al Appeal Judgment*”).

⁷ *Id.*, para. 330.

⁸ The Defence may challenge the reliability of call location data during the trial.

B. There is an Internationally Recognised Right to Privacy in Call Location Data

17. The human right to privacy is enshrined in a number of international instruments including Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.
18. In *Carpenter v United States*, the United States Supreme Court held that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through call location data. The collection of this call location data by law enforcement from the telecommunications companies was an intrusion into a person's right of privacy by revealing his physical movements such that a judicial order, based upon probable cause, was required.⁹
19. In *Big Brother Watch and Others v United Kingdom*, a Chamber of the European Court of Human Rights held that a United Kingdom law that did not provide for judicial review before obtaining call data records was invalid.¹⁰ The Court of Justice of the European Union has also invalidated, on privacy grounds, legislation that allowed for the collection and dissemination to law enforcement of telephone data without judicial supervision.¹¹ The Court said:

Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the

⁹ [Carpenter v. United States](#), 585 US ___, No.16-402, 22 June 2018 (« *Carpenter Decision* »).

¹⁰ ECHR, [Big Brother Watch and Others v. United Kingdom](#), 13 September 2018, No. 58170/13, para. 467. The case is currently pending before the [Grand Chamber](#).

¹¹ Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, [Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Seitinger and Others](#), 8 April 2014, paras. 35, 69. This principle was recently affirmed by the Court of Justice's Advocate General, who recommended earlier this year that a UK data retention law be struck down because, *inter alia*, it failed to provide for judicial or independent administrative review before law enforcement could access those records. *Privacy International v. Secretary of State*, [Opinion of Advocate General delivered on 15 January 2020](#), Case C-623/17, para. 139.

purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.¹²

20. At the Special Tribunal for Lebanon, the Trial Chamber, while denying a motion to exclude call data records, nevertheless held that “it is evident that international human rights standards are evolving to include legal protection of metadata such as call data records from unwarranted disclosure to governments and law enforcement agencies.”¹³
21. In *R v Rogers Communications*, the Ontario Superior Court of Justice held that “Canadians have a reasonable expectation of privacy in their cell phone records”.¹⁴
22. Therefore, the Chamber should find that there is an internationally recognised human right of privacy in call location data. If it so finds, it must go on to consider the question of whether that right was violated.

C. The Prosecution’s Means for Obtaining Call Location Data Violated the International Human Right to Privacy

23. The internationally recognised right to privacy is not absolute, but may be subject to legitimate interference when necessary for the protection of important public interests, including law enforcement.¹⁵ A court must consider the proportionality of the interference with the right to privacy by balancing the nature of the information concerned against the investigative need warranting such access.¹⁶ A judicial officer, upon being presented with a

¹² *Id.*, para. 62.

¹³ *Prosecutor v. Ayyash et al*, [Decision on Five Prosecution Motions on Call Sequence Tables and Eight Witness Statements and on the Legality of the Transfer of Call Data Records to UNIIC and STL’s Prosecution](#), 6 May 2015, No. STL-11-01/T/TC, para. 86 (“*Ayyash Decision*”).

¹⁴ *R v. Rogers Communications*, 14 January 2016, 2016 ONSC 70, para. 31.

¹⁵ *Bemba et al Appeal Judgment*, para. 285.

¹⁶ *Bemba et al Appeal Judgment*, para. 333.

reasoned request, may authorise the collection of information that is otherwise private.

24. However, the Prosecution's collection of call location data in this case, both in the two RFAs directed at five telephones attributed to Mr. Yekatom, and the 20 subsequent RFAs that have been disclosed to the Defence, never involved a judicial determination. The Prosecution never sought authorisation from a Chamber of this Court to collect the call location data. Nor did it seek, or obtain, authorisation from any court in the Central African Republic.
25. Instead, the Prosecution simply sent a request of the records to its focal point for cooperation with the ICC within the government of the Central African Republic.
26. The Defence contends that obtaining the call location data without judicial authorisation violated Mr. Yekatom's right to privacy. It requests that the Trial Chamber rule, as a matter of law, when weighing the right to privacy in one's location against the need for such information by law enforcement, that the proportionality test requires that judicial authorisation be sought whenever the Office of the Prosecutor wishes to obtain call location data.
27. The fact that Central African Republic law does not require such judicial authorisation is not dispositive. Compliance with domestic law in the collection of evidence is not *per se* proof that the evidence was not obtained by means of a violation of the Statute or internationally recognised human rights. Investigative activities are measured not against domestic law, but by whether they conform to internationally recognised human rights.¹⁷
28. In the *Bemba et al* case, the Prosecution obtained judicial authorisation from a Pre-Trial Chamber before seeking intercepted telephone communications

¹⁷ [Bemba et al Appeal Judgment](#), para. 330.

through the Dutch authorities and obtained authorisation to review Western Union financial records from courts in Austria.¹⁸ There is no reason why the Prosecution cannot get judicial authorisation before collecting call location data, whether from an ICC Chamber or a court in the State in which the records are located.

29. The decision of the Trial Chamber of the Special Tribunal for Lebanon that a judicial order was not required to obtain call data records¹⁹ is distinguishable from the present case because the violation of privacy in one's location, as opposed to in the call records themselves, was never raised or decided, and because the decision turned on compliance with Lebanese law and judicial review of evidence collection, neither of which are applicable at this Court.
30. Because the Prosecution did not obtain judicial authorisation before obtaining the call location data in this case, the Trial Chamber should find that Mr. Yekatom's international right to privacy in his call location records was violated. If it so finds, the Chamber should go on to consider the second step in the Article 69(7) regime.

D. Admission of the Call Location Data would be Antithetical to and Seriously Damage the Integrity of the Proceedings

31. The fact that evidence was obtained in violation of an individual's rights does not automatically result in the exclusion of that evidence. The accused must also establish that the admission of the evidence would be antithetical to and seriously damage the proceedings.²⁰
32. In the *Bemba et al* case, the Trial Chamber considered that whether the violation resulted from actions of the Prosecution itself and not from a third

¹⁸ *Id.*, paras.

¹⁹ [Ayyash Decision](#), paras. 108-10.

²⁰ *Prosecutor v Bemba et al*, [Decision on Requests to Exclude Western Union Documents and Other Evidence Pursuant to Article 69\(7\)](#), 29 April 2016, ICC-01/05-01/13-1854, para. 63.

party, and the importance of the right to privacy were factors to be considered under the second step of Article 69(7).²¹

33. In Mr. Yekatom's case, it was the Prosecution, and not a third party, that decided to obtain the call location data without seeking judicial authorisation. In addition, the right to privacy in one's location over an extended period of time is an important one, and one that led to the exclusion of the evidence in the *Carpenter* case in the United States Supreme Court, even in the absence of bad faith or negligence by law enforcement.
34. The Trial Chamber in the *Bemba et al* case noted that judicial orders were issued to obtain the Western Union records, and that this militated in favor of admission of the evidence.²² Here, the call location data was obtained without any judicial orders whatsoever.
35. The widespread nature of the violation of rights by obtaining call location records without judicial review, as opposed to the relatively limited nature of the Western Union records in the *Bemba et al* case, also provides a distinction that warrants exclusion in this case. The call location records for Mr. Yekatom covered a two-year period and tens of thousands of incoming and outgoing calls.²³ Since the records show that the phones attributed to Mr. Yekatom were constantly being used, this allowed the Prosecution to track his movements on a minute-by-minute basis for a two-year period.
36. This surveillance was not limited to Mr. Yekatom. In the course of the CAR II investigation, involving both the Anti-Balaka and Seleka, it is likely that

²¹ *Id.*, para. 65.

²² *Id.*, paras. 68-69.

²³ CAR-OTP-2008-0480; CAR-OTP-2008-0481; CAR-OTP-2019-1364; CAR-OTP-2046-0714 ; CAR-OTP-2046-0730; CAR-OTP-2054-1477; CAR-OTP-2054-1479; CAR-OTP-2054-1480; CAR-OTP-2054-1481; CAR-OTP-2054-1482; CAR-OTP-2054-1483; CAR-OTP-2054-1484; CAR-OTP-2068-0034.

records of millions of calls and texts were obtained by the Prosecution without judicial review, allowing it to track the movements of dozens of individuals.²⁴

37. Since call location data now features prominently in most criminal investigations, the Prosecution's failure to seek judicial review when obtaining call location data likely cuts across most of the situations under active investigation, including those in Mali, Sudan, Libya, Ivory Coast, and Georgia, violating the privacy rights of hundreds of more persons. The Prosecution likely continues to obtain call location data without judicial review to this very day.
38. Admission of the call location data in Mr. Yekatom's case would be antithetical to and seriously damage the proceedings because it would condone the wholesale violation of the right to privacy in one's location over an extended period of time.
39. It is not necessary to prove that the Prosecution acted in bad faith in order to obtain exclusion of evidence pursuant to Article 69(7). Admission of evidence can be antithetical to the integrity of the proceedings where it would be seen as condoning the widespread violation of human rights. That is the case here.
40. The Trial Chamber should therefore exclude the evidence of Mr. Yekatom's location obtained from his call location records.

E. This Motion is Not Premature

41. Mr. Yekatom has brought this motion before the Prosecution has tendered the call location data through a witness or bar table motion. He has done so because the collection of call location data is ongoing and guidance from the Trial Chamber is needed. A decision that the collection of call data location information requires a judicial order, even if the Chamber declines to exclude

²⁴ See, i.e. the 500-page compilation of calls used during the confirmation hearing. [ICC-01/14-01/18-282-Conf-AnxJ1](#).

the evidence in this case, will guide all parties, including the Defence, in their collection of this material going forward, and will promote respect for the human rights of those individuals whose call location data has yet to be sought or produced.

42. Should the Chamber not wish to rule on this issue until the evidence is formally tendered, it is requested that it not reject this motion as premature, but take it under submission until the Chamber is ready to rule on the issue.

CONCLUSION

43. This Trial Chamber should find that (1) there is a right to privacy in one's movements over a period of time as reflected in call location data; (2) this right is violated when call location data is collected without a prior judicial determination; and (3) admission of the call location data of Mr. Yekatom would be antithetical to and seriously damage the proceedings. Therefore, the evidence should be excluded pursuant to Article 69(7) of the Statute.

RESPECTFULLY SUBMITTED ON THIS 29th DAY OF JUNE 2020



Me Mylène Dimitri
Lead Counsel for Mr. Yekatom



Peter Robinson
Associate Counsel for Mr. Yekatom

The Hague, the Netherlands ²⁵

²⁵ The contribution of the Office of Public Counsel for the Defence to the research for this motion is gratefully acknowledged.