Cour
Pénale
Internationale

International
Criminal
Court

Original: English

No.: ICC-01/14-01/18
Date: 17 July 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 *PROSECUTOR v.*
ALFRED ROMBHOT YEKATOM & PATRICE-EDOUARD NGAÏSSONA

Public

Request for Leave to File *Amicus Curiae* Submission on Behalf of the Electronic Privacy Information Center (EPIC)

Source: **Electronic Privacy Information Center (EPIC)**

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

The Office of the Prosecutor
Ms. Fatou Bensouda, Prosecutor
Mr. James Stewart
Mr. Kweku Vanderpuye

Counsel for Mr. Yekatom
Me Mylène Dimitri
Mr. Peter Robinson

Counsel for Mr. Ngaïssona
Me Geert-Jan Alexander Knoops

Legal Representatives of the Victims
Mr. Dmytro Suprun
Mr. Abdou Dangabo Moussa
Ms. Elsabeth Rabesandratana
Mr. Yaré Fall
Ms. Marie-Edith Douzima-Lawson
Ms. Paolina Massidda

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
Me Xavier-Jean Keïta

States' Representatives

Amicus Curiae

REGISTRY

Registrar
Mr. Peter Lewis

Counsel Support Section

Victims and Witnesses Unit
Mr. Nigel Verill

Detention Section

Victims Participation and Reparations Section

I. INTRODUCTION

1. Pursuant to Rule 103 of the ICC Rules of Procedure and Evidence, the Electronic Privacy Information Center (EPIC) requests leave to file an *amicus curiae* submission regarding Trial Chamber V's ("the Chamber") consideration of the "*Motion to Exclude Call Location Evidence*" of 29 June 2020 ("the Motion") (ICC-01/14-01/18).[1]

2. Should it be granted leave, EPIC intends to make the following submissions to assist the Chamber's decision: (1) There is an emerging international trend recognizing privacy in call data records (CDR) containing cell-site location information (CSLI) as part of the right to privacy, which the ICC recognizes as an international human right; and (2) An individual's historical CSLI is protected under this right.

3. EPIC is uniquely qualified to make these submissions as *amicus curiae*. EPIC is a public interest, non-profit research and educational organization based in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files amicus briefs before United States courts, including the U.S. Supreme Court. In *Carpenter v. United States*, EPIC filed an amicus brief arguing that prior judicial authorization is required to obtain historical CSLI from telephone service providers in criminal investigations.[2] The U.S. Supreme Court agreed, adopting a warrant requirement in that case. In *Riley v. California*, the U.S. Supreme Court cited EPIC's amicus brief and held that a warrant was required for officers to search a cell phone obtained from a lawfully-arrested individual.[3] EPIC also participates as *amicus curiae* in cases involving the right to privacy under international law. EPIC intervened in the case of *10 Human rights organizations and others v. the UK* (App No. 24960/15) before the European Court of

[1] This application is made in accordance with Rule 103(1) of the Rules of Procedure and Evidence.
[2] Brief of *Amici Curiae* Electronic Privacy Information Center (EPIC) and Thirty-Six Technical Experts and Legal Scholars in Support of Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), https://epic.org/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf.
[3] Brief of *Amici Curiae* Electronic Privacy Information Center (EPIC) and Twenty-Four Technical Experts and Legal Scholars in Support of Petitioner, *Riley v. California*, 573 U.S. 373 (2014) (No. 13-132), https://epic.org/amicus/cell-phone/riley/EPIC-Amicus-Brief.pdf.

Human Rights ("ECHR"), which concerned whether alleged surveillance activities by government agencies violated Article 8 of the European Convention on Human Rights ("the Convention"). EPIC has further participated in successful challenges to surveillance regimes under the E.U. Charter of Fundamental Rights ("the Charter") before the Irish High Court and in the Court of Justice of the European Union ("CJEU"). *See Data Protection Commissioner v. Facebook Ireland Limited and Max Schrems*, Case C-311/18.

4. Taken together, EPIC's proposed submissions will ensure that the Chamber understands the privacy implications of obtaining historical CSLI evidence without judicial authorization or otherwise sufficient procedural safeguards. There is increased recognition in the international community that cell phone metadata, and CSLI in particular, can reveal sensitive personal information by allowing investigators to track an individual's movements over time and infer their habits, social associations, and even political and religious beliefs. EPIC hopes it can lend its expertise in privacy and human rights in this instance.

II. SUBMISSIONS

A. There is an emerging international trend recognizing the right to privacy in phone metadata, including CSLI.

5. The ICC treats "[t]he right to privacy" as "an internationally recognized human right," based on numerous international treaties providing that right.[4] EPIC will demonstrate that the right to privacy encompasses a right to privacy in historical CSLI, and judicial authorization should be required to access such data. EPIC does not take a position on whether the court should exclude the evidence at issue in this case.[5]

6. Metadata is data that describes other data, providing information about an electronic or telephone communication without displaying its contents. Phone

[4] *Prosecutor v. Bemba*, ICC-01/05-01/13, Decision on Requests to Exclude Western Union Documents and other Evidence Pursuant to Article 69(7) (Apr. 29, 2016), para. 46; *Prosecutor v. Lubanga*, ICC-01/04-01/06, Decision on the admission of material from the "bar table" (June 24, 2009), para. 21.

[5] Art. 69(7)(a)–(b); *Lubanga*, ICC-01/04-01/06 ("However, the right to privacy under each [treaty] . . . is not absolute, and can lawfully be restricted.").

metadata can include information identifying the time and duration of calls, phone numbers of callers and receivers, whether a message was delivered, the status of routine data connections, and other information.[6] CSLI is a type of metadata that is automatically produced by cell phone networks when phones connect to nearby cell towers; whenever an individual's cell phone is turned on and connected to the network, they cannot avoid generating CSLI records. The ability to monitor location data in CSLI represents a type of "near perfect surveillance, as if [one] had attached an ankle monitor to the phone's user."[7]

7. Many courts have considered metadata collection in a variety of contexts. Taken together, these decisions demonstrate a burgeoning global recognition of the human right to privacy in metadata, and CSLI in particular. The Special Tribunal for Lebanon put it succinctly: "It is evident that international human rights standards are evolving to include legal protection of metadata such as call data records from unwarranted disclosure."[8] EPIC will argue that protection of this type of data is widely recognized and accepted as part of the right to privacy and that the ICC should also require protections for this type of evidence.[9] Courts such as the Special Tribunal for Lebanon, the CJEU, the ECHR, the U.S. Supreme Court, and others have recognized that (1) law enforcement access to CSLI and other metadata interferes with the right to privacy; and (2) the right is violated absent sufficient safeguards, such as prior judicial authorization, to limit law enforcement access to the data.

B. Historical CSLI is protected under the individual right to privacy.

8. International courts that recognize the right to privacy in phone metadata and CSLI have largely done so in cases challenging programmatic mass surveillance or

---

[6] *See, e.g.*, CJEU, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger v. Minister for Communications*, Marine and Natural Resources, 8 April 2014, para. 27 ("*Digital Rights*"); *Carpenter v. United States*, 138 S. Ct. at 2206, 2212 (noting modern cell phones "generate increasingly vast amounts of increasingly precise CSLI").

[7] *Carpenter*, 138 S. Ct. at 2218.

[8] *Ayyash et al.*, para. 86 (quoting Resolution of the UN Human Rights Council, 24 March 2015, A/HRC/28/L.27, p. 3).

[9] *See The Prosecutor v. Omar Al*, ICC-02/05-01/09-139, Decision on the Failure by the Republic of Malawi to Comply with the Cooperation Requests Issued by the Court with Respect to the Arrest and Surrender of Omar Hassan Ahmad Al Bashir (Pre-Trial I) (Dec. 12, 2011), para. 39.

real-time CSLI collection. EPIC will argue that the reasoning in these cases also extends to an individual's right to privacy in historical CSLI. Indeed, as the U.S. Supreme Court recently articulated, historical location records reveal much more about an individual than real-time records.

9. First, EPIC will argue that the internationally recognized right to privacy is infringed whether phone metadata is collected from one individual, or from millions. The right to privacy is an individual right, and mass surveillance programs indicate an arbitrary infringement on that individual right. Several courts have found that accessing an individual's CSLI infringes their right to privacy. Courts in mass surveillance cases have also recognized that the aggregation of an individual's location data over an extended period of time infringes their right to privacy.[10] Through aggregation, investigators can discern patterns in behavior and discover intimate details about any individual whose data is collected.[11] The threat that such aggregation poses to privacy is not context-dependent. It persists whether their CSLI is swept up in a nation- or continent-wide metadata surveillance program or in an individualized investigation.

10. Second, EPIC will demonstrate that the internationally recognized right to privacy in an individual's CSLI protects historical data. First, several courts have explicitly recognized that law enforcement access to historical CSLI interferes with or violates the right to privacy. Second, the CJEU invalidated mass surveillance directives because law enforcement access to the collected data—*historical* data—was not sufficiently safeguarded. Third, the reasoning in real-time location data cases applies with even greater force to the aggregation of historical location data. Analysis of historical CSLI allows investigators to retrace an individual's movements in a

[10] *See, e.g.*, *Digital Rights*; CJEU, Judgment in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige, AB v. Post-och Telestyrelsen and Secretary of State v. Tom Watson* (Dec. 21, 2016); ECHR, *Case of Big Brother Watch and Others v. The United Kingdom*, Judgment (Sept. 13, 2018); ECHR, *Breyer v. Germany*, Judgment (Fifth Section) (Dissent), 30 January 2020.

[11] *Digital Rights*, para. 27. *See also Ayyash et al.*, paras 85 ("[Metadata] may give an insight into an individual's behavior ... that goes beyond even that conveyed by accessing the content of a private communication.") (quoting 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, para. 19).

systematic manner. Such comprehensive data is much more likely than real-time location data to reveal an individual's patterns, social relations, and other private activities.[12] Thus, the aggregation of an individual's historical CSLI over an extended period of time violates the right to privacy even more than real-time CSLI collection. The individual right to privacy in CSLI must thus also include privacy in one's historical CSLI.

11. EPIC hopes to submit further information to aid the Chamber in its decision on the Motion before it. EPIC's *amicus curiae* submission will demonstrate an emerging international trend recognizing that an essential aspect of an individuals' right to privacy—a right previously recognized by the ICC—includes a right to privacy in their phone metadata, including their historical CSLI. EPIC intends to provide information that the Chamber would not otherwise receive from either party, with hopes that its submission will enable the Chamber to rule in an informed and just manner.

Respectfully submitted,

Megan Iorio
Appellate Advocacy Counsel
Electronic Privacy Information Center

Dated this 17 of July 2020
At the District of Columbia, the United States of America.

[12] *Carpenter*, 138 S. Ct. at 2218.