Cour Pénale Internationale

International Criminal Court

Original: **English**

No.: **ICC-01/21-01/25**
Original: **31 August 2026**
Date: **3 September 2026**

TRIAL CHAMBER III

Before: **Judge Joanna Korner, Presiding Judge**
Judge Keebong Paek
Judge Nicolas Guillou

SITUATION IN THE REPUBLIC OF THE PHILIPPINES

IN THE CASE OF THE PROSECUTOR v. RODRIGO ROA DUTERTE

Public

Public Redacted Version of "Defence Request to Amend the E-Court Protocol in Relation to Open Source and User-Generated Material"

Source: **Defence for Mr Rodrigo Roa Duterte**

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**
Duterte Defence Team

☒ **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
Osvaldo Zavala Giler

☐ **Counsel Support Section**

☐ **Victims and Witnesses Unit**

☐ **Detention Section**

☐ **Victims Participation and Reparations Section**

☐ **Other**

I. INTRODUCTION

1. Despite consistent case law finding that the investigation should largely be complete by confirmation,[1] the record of disclosure in the present case has ballooned since the end of the confirmation stage. There has been an over 400% increase in the volume of evidence disclosed by the Prosecution, from just over 5,000 items of evidence received in advance of the confirmation hearing to over 25,000 items at the time of writing, with disclosure still ongoing. This is despite the Chamber urging the Prosecution in the first Status Conference to "review your evidence to make sure that we avoid having repetitive, irrelevant or over-voluminous evidence."[2]

2. Unfortunately, many items that have been disclosed to the Defence are illegible;[3] audio-visual materials have been disclosed without transcripts and/or translations;[4] and individual pages of the same document have been disclosed independently, with distinct and inconsecutive ERNs,[5] amongst many other issues.[6] Most recently, the Prosecution has signalled its intention to disclose a further 200GB of material, which, owing to the

[1] *Yekatom and Ngaïssona*, Transcript of Status Conference, ICC-01/14-01/18-T-012-ENG, 9 July 2020, p. 12, lines 17-21; *Mbarushimana*, Judgment on the appeal of the Prosecutor against the decision of Pre-Trial Chamber I of 16 December 2011 entitled "Decision on the confirmation of charges", ICC-01/04-01/10-514, 30 May 2012, para. 44; *Lubanga*, Judgment on the Prosecutor's appeal against the decision of Pre-Trial Chamber I entitled "Decision Establishing General Principles Governing Applications to Restrict Disclosure pursuant to Rule 81(2) and (4) of the Rules of Procedure and Evidence", ICC-01/04-01/06-568, 13 October 2006, para. 54.
[2] Transcript of Status Conference, ICC-01/21-01/25-T-009-CONF-ENG, 27 May 2026 ("Transcript of the First Status Conference"), p. 47, lines 20-21.
[3] *See e.g.* PHL-OTP-00045125, PHL-OTP-00045124, PHL-OTP-00045123 disclosed as both INCRIM and Rule 77 on 5 August 2026, one-page documents that are illegible, one of which appears to be blank. The Defence provided the Prosecution with lists of illegible items on 17 July 2026 and 14 August 2026. *See* Email, Defence to Prosecution, "D36 Request for Disclosure / Metadata Updates", 17 July 2026, 16:46; Email, Defence to Prosecution, "Re: D36 Request for Disclosure / Metadata Updates", 14 August 2026, 18:54.
[4] A list of 361 such videos, including 90 disclosed as INCRIM, was provided to the Prosecution on 17 July 2026 and 14 August 2026. *See* Email, Defence to Prosecution, "D36 Request for Disclosure / Metadata Updates", 17 July 2026, 16:46; Email, Defence to Prosecution, "Re: D36 Request for Disclosure / Metadata Updates", 14 August 2026, 18:54.
[5] To give an example, PHL-OTP-00239165 is the first page of a document; the third page of the same document is PHL-OTP-00239111, and the fourth page is PHL-OTP-00239089. The Defence has not been able to locate the second page to date. On a bigger scale, the Prosecution disclosed a 400-page document page by page, non-continuously from PHL-OTP-00238126 to PHL-OTP-00239076. The Defence located only 347 pages out of at least 400 pages, as implied by the page number on PHL-OTP-00238634. In addition, at least 60 stand-alone "Table of Contents" documents which have been disclosed separately from their content, such as PHL-OTP-0001-1183, PHL-OTP-0001-1039, PHL-OTP-0001-1021 or PHL-OTP-0001-0991. These issues have been consistently raised with the Prosecution during meetings on 15 and 24 July 2026 and via email: Email, Defence to Prosecution, "D36 Request for Disclosure / Metadata Updates", 17 July 2026, 16:46; Email, Defence to Prosecution, "Re: D36 Request for Disclosure / Metadata Updates", 14 August 2026, 18:54; Email, Defence to Prosecution, "Re: D36 Request for Disclosure / Metadata Updates", 24 August 2026, 12:10.
[6] The OTP has partially resolved some issues, and has endeavoured to fix others that remain unresolved. However, much of this response relies on the Defence identifying the problematic pieces of evidence and bringing them to the OTP's attention, thereby adding additional workload to the Defence team.

size and volume of this dataset, eludes all traditional evidence uploading processes.[7] Based on a small sample of documents from the same dataset which has already been received by the Defence, it is clear that there are major issues with this collection of documents; it includes many duplicates and documents of very poor quality which, notwithstanding its volume, makes meaningful review immensely challenging.[8]

3. This is the context in which this motion is filed. On the basis of the evidence disclosed to it to date, and with three months until the start of trial, the Defence is deeply concerned that the quality and quantity of the evidence in this case risks flooding the record with unreliable and/or irrelevant material. This would be detrimental for the parties and the Chamber's search for the truth, and reputationally damaging for the Court. This concern is particularly heightened in this case where, unlike in other cases previously before the Court, the parties and Chamber are operating in an environment where a huge volume of misinformation is being routinely created and shared online about these proceedings and the events on which they focus. The Defence therefore requests an amendment to the E-Court Protocol in relation to open source and user-generated material, as a first step to ensuring that evidence is properly verified by the parties prior to its submission.

II. CONFIDENTIALITY

4. This Request is filed confidentially pursuant to Regulation 23*bis*(1) of the Regulations of the Court as [REDACTED].

III. PROCEDURAL HISTORY

5. In the first Status Conference of 27 May 2026, the Chamber asked the Prosecution how it proposed to introduce evidence from open sources, that is, "material that is not directly attributable to a witness or anybody who can speak about it", and specifically whether it would be calling expert evidence in relation to such material.[9] The Prosecution agreed to consider this question.[10]

---

[7] Email, Prosecution to Defence, "[REDACTED]", 25 August 2026, 18:32.
[8] For example, PHL-OTP-00068875, PHL-OTP-00068876, PHL-OTP-00068877 appear to be the same document, disclosed in three versions of progressively poor quality. Similarly, PHL-OTP-00070563, PHL-OTP-00070564, PHL-OTP-00070565 are the same document. PHL-OTP-0004-5050 to PHL-OTP-0004-5070 are 21 copies of the same photograph of a tube light. Other documents have been disclosed twice.
[9] Transcript of the First Status Conference, p. 20, lines 16-21.
[10] *Id.*, p. 20, line 22 ("MR NICHOLLS: [10:18:57] Okay, that's understood. We'll look at that.").

6. On 14 August 2026, the Prosecution wrote to the Defence, responding to some of the disclosure issues that had been raised in person and via email. The Prosecution added:

> [REDACTED].[11]

7. [REDACTED].[12]

8. On 27 August, the Prosecution proposed the following language for joint submission by the OTP, Defence, and Registry:

> [REDACTED].[13]

9. On 28 August, the Defence responded that adding a new metadata field in NUIX "would be pointless unless the Trial Chamber amends the E-Court Protocol to make the completion of this field obligatory."[14] As it had noted in earlier correspondence, the Defence highlighted the insufficiency of the URL as an element in assessing the authenticity of an item of evidence. It further noted the Chamber's earlier request for confirmation as to whether open source material, including any material that is not directly attributable to a witness (such as material from OTPLink), would be verified by an expert. On this basis, the Defence proposed two additions to the table in section D, paragraph 32 of the E-Court Protocol for the present case: one on "URL", based on the Prosecution's request, and the other on "Expert Verification".

10. On 31 August, parties and participants jointly agreed to the first proposed amendment to the E-Court Protocol, adding a "URL" field in NUIX:[15]

Field Name	**Data Type**	**Explanation**	**Example**	**One to**
URL	Memo	Uniform resource locator: The original web address from which the item was collected.	https://www.icc-cpi.int/	ONE

[11] Email, Prosecution to Defence, "Re: D36 Request for Disclosure / Metadata Updates", 14 August 2026, 11:52.
[12] [REDACTED].
[13] Email, Prosecution to parties and participants, "[REDACTED]", 27 August 2026, 11:08.
[14] Email, Defence to parties and participants, "[REDACTED]", 28 August 2026, 09:47.
[15] Email, Prosecution to parties and participants, "[REDACTED]", 28 August 2026, 19:37; Email, Defence to parties and participants, "[REDACTED]", 31 August 2026, 10:29; Email, CLRV to parties, "[REDACTED]", 31 August 2026, 10:36; Email, Prosecution to parties and participants, "[REDACTED]", 31 August 2026, 10:43.

11. However, the parties were unable to agree on the addition of an "Expert Verification" field. The Defence hereby requests that the Chamber order the addition of an "Expert Verification" field to NUIX as an amendment to the E-Court Protocol, as the first step to ensuring that only properly verified open source material is submitted to the Chamber in the present case.

12. On 31 August 2026, the Prosecution filed its submission on an amendment of the E-Court Protocol.[16]

IV. SUBMISSIONS

1. PROVIDING THE URL OF A PIECE OF OPEN SOURCE EVIDENCE IS AN INSUFFICIENT MEANS TO AUTHENTICATE IT

13. The Prosecution, in seeking approval for the creation of the new "URL" field on NUIX, submitted that this:

> [REDACTED].[17]

14. Despite supporting the addition of a new "URL" field as an amendment to the E-Court Protocol, the Defence once again emphasizes that this is insufficient information upon which to assess an item's authenticity or reliability. The URL merely records the web location from which a piece of online content was collected; it cannot indicate its source. As the Trial Chamber in *Yekatom and Ngaïssona* noted, without a statement or testimony from an individual who authored a post or participated in an exchange online, it cannot be conclusively determined who participated in such exchanges or created the posts, even if they were linked to a profile or an IP address.[18]

15. Aside from the limitations as to what can be inferred about the source from a URL, it further says nothing of: the discovery process, which is vital to confirm its chain of custody; whether an item has been edited in any way; whether the content featured at that URL has been independently verified; whether AI tools were used to filter the evidence, and whether there are any other indicia of authenticity and reliability.[19] This

[16] Prosecution's submission on an amendment of the E-Court Protocol, ICC-01/21-01/25-485-Conf, 31 August 2026.
[17] Email, Prosecution to Trial Chamber III and parties and participants, "[REDACTED]", 25 August 2026, 15:00.
[18] *Yekatom and Ngaïssona*, Judgment, ICC-01/14-01/18-2784-Red, 24 July 2025, para. 151. The Chamber additionally found that IP addresses or logs could not confirm an individual's location, in the absence of expert testimony.
[19] *See also Al Hassan*, Trial Judgment, ICC-01/12-01/18-2594-Red, 26 June 2024, para. 726, fn. 2175.

key information on the item's technical, material, and contextual elements, combined with an analysis of the source, are vital in establishing its relevance and probative value.

16. Both the Berkeley Protocol on Digital Open Source Investigations and the Office of the Prosecutor's own guidelines (co-authored with Eurojust and the EU Genocide Network) emphasize that the original URL is but one element that should be recorded when material is collected from an online location. The Berkeley Protocol lists eight separate elements that should be recorded when collecting online information, only one of which is the item's URL. The other seven items are: HTML source code, full screen capture, embedded media files, embedded metadata, contextual data, collection data, and hash value.[20] Similarly, the Office of the Prosecutor/Eurojust guidelines state that, at a minimum, online investigations should download information such as screen capture; embedded media files, and embedded metadata as well as the web address.[21] They also recommend that a unique cryptographic hash value should be calculated and recorded for each digital item at the time that it is obtained.[22]

17. Furthermore, both the Berkeley Protocol and the Office of the Prosecutor/Eurojust guidelines make clear that these are merely elements that should be recorded at the time of collection; verification is a separate matter and involves an expert analysis of source, content, and technical aspects.

18. Lastly, the addition of a URL field disregards the fact that much of this information may not have been posted online. The definition of "open source" material adopted by the Chamber in the first status conference (material "not directly attributable to a witness or anybody who can speak about it") is clearly, and correctly, broader than just information on the internet. This definition would also extend to "user-generated evidence", defined as open or closed source information generated through users' personal digital devices which may be of evidentiary value and used in legal

[20] *Berkeley Protocol on Digital Open Source Investigations, A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, Office of the United Nations High Commissioner for Human Rights, University of California Human Rights Center, 2022 ("Berkeley Protocol"), para. 155.
[21] *Documenting international crimes and human rights violations for accountability purposes: Guidelines for civil society organisations*, Eurojust, Network for investigation and prosecution of genocide, crimes against humanity and war crimes, Office of the Prosecutor of the International Criminal Court, 2022, p. 32.
[22] *Id.*

proceedings.[23] Much user-generated evidence may be transmitted privately, via messaging software, email, or transmitted through compact disc or USB storage device, and therefore a URL would not always be available.

19. For these reasons, the Defence proposes the addition of a "expert verification" metadata field in NUIX, as a further amendment to the E-Court Protocol, discussed in more detail below.

2. A FURTHER SPECIFIC AMENDMENT TO THE E-COURT PROTOCOL IN RELATION TO OPEN SOURCE AND USER-GENERATED EVIDENCE IS REQUIRED

20. The current case operates in a uniquely challenging information ecosystem, in which a large volume of misinformation, or "fake news"[24] has circulated, and will continue to circulate, online. Extra caution is therefore required to ensure that evidence is properly verified before it is submitted to the Court. As the Nuremberg Principles Academy has noted, "given the sophistication of technology and the high susceptibility to manipulation of digital evidence today, it is difficult to see how digital evidence can ever be 'self-authenticating' or how the parties can agree to an item's authenticity without the Prosecution having verified its evidence and thus fulfilled the burden of proving that the evidence is authentic."[25] It further added that the "E-Court Protocol should be updated regularly for solutions on how to adapt to newer challenges".[26]

21. A new challenge is posed by the advent of the Office of the Prosecutor's "OTPLink" system, which allows anyone to submit evidence directly to the Prosecution. The Defence has been informed that some material received via OTPLink has already been disclosed to it as "open source" (although it is not open source in the sense of it being publicly available). However, without an identifying tag, the Defence cannot identify

[23] K. Stavrou, "User-Generated Evidence in International Criminal Proceedings before Domestic Courts: Is Seeing Always Believing?" in M.L. Fremuth et al. (eds.), *International Criminal Law before Domestic Courts: The Role of National Criminal Justice in the Prosecution of International Core Crimes* (Verlag, 2024) 344; K. Stavrou and Y. McDermott, "Digital Evidence" in W. Schabas et al. (eds.), *The Routledge Handbook of International Criminal Law* (2nd edn., Routledge 2027); R. Hamilton, "User Generated Evidence" 57 *Columbia Journal of Transnational Law* (2018) 1.
[24] Transcript of Status Conference, ICC-01/21-01/25-T-010-ENG, 23 June 2026, p. 7, lines 8-11.
[25] *E-Procedure, The Impact of the Increased Usage of Digital Evidence and Sophistication of Technology on the Rules and Practices of the International Criminal Court, Final Report*, International Nuremberg Principles Academy, 27 October 2023, p. 43.
[26] *Id.*, Annex 1, p. 13. The Nuremberg Academy has also noted that the "E-Court Protocol is largely limited to harmonising the format, means of storage and presentation of evidence. Does not address authentication other than specifying that metadata should be attached and that the cryptographic hashing standard to be adopted is MD5. This is insufficient to address digital evidence." at p. 18.

which of the disclosed "open source" items have come from OTPLink. Even if items that had come through OTPLink were capable of identification, or if an additional metadata field were introduced to confirm this in NUIX, the source of this material would always be unknown. This is because individuals can submit to OTPLink anonymously if they wish,[27] and even where a name is provided by the submitting person or organisation, no apparent identity checks are in place.

22. According to the Office of the Prosecutor's annual reports, over 400,000 electronic files were received via this platform in 2024, rising to more than 570,000 files in 2025 alone.[28] Whether or how the Office of the Prosecutor has triaged this huge volume of material to identify exculpatory material to meet its Article 54(1)(a) duty in the present case is not clear. There is also the obvious danger that nefarious actors will use the system to transmit falsified, manipulated, or forged evidence, which might also be circulated online; a risk identified by the Office of the Prosecutor itself.[29]

23. In light of these difficulties, the Defence proposes a further amendment to the E-Court Protocol, to add a new "expert verification" metadata field. This field would confirm whether or not the item will be accompanied by an expert report if it is to be submitted to the Chamber as evidence. This field would operate similarly to the witness fields in the E-Court Protocol, which list forms of metadata "to be provided on an ongoing basis during the trial phase".[30]

---

[27] *See* "OTPLink", International Criminal Court (noting that "the form below can be used to submit such information, also known as 'communications,' to the OTP either anonymously or named.") and with a tick box for "I want to make this submission anonymously". Although intended as a platform for Article 15 communications, OTPLink also allows for the submission of information relating to ongoing investigations, *see* "FAQs", International Criminal Court (Q: "What happens if the information sent relates to a situation already under preliminary examination or investigation?" A: "The OTP will ensure that the information related to an existing situation will be sent to the relevant team for further consideration.").

[28] *Resilient Justice In every step. Office of the Prosecutor Annual Report 2025*, Office of the Prosecutor of the International Criminal Court, 1 December 2025, p. 39 (83,119 submissions, more than 570,000 files: "Approximately half of the submissions received (47,636) were related to an open investigation or preliminary examination, and half (35,483) related to other matters."); *The law in action For all. Office of the Prosecutor Annual Report 2024*, Office of the Prosecutor of the International Criminal Court, 4 December 2024, p. 17 (74,803 submissions (average 200 per day), total of 401,488 electronic files).

[29] *See Office of the Prosecutor Policy on Cyber-Enabled Crimes under the Rome Statute*, Office of the Prosecutor of the International Criminal Court, 3 December 2025, para. 106 ("A person can also falsify or forge the relevant evidence by using cyber tools, and thus at least facilitate the commission of this offence and potentially be a co-perpetrator – for example, by manipulating a video with the intent and knowledge that it will be presented to the Court as evidence.").

[30] Annex to the Registry's Report Pursuant to the Chamber's Oral Decision issued on 27 May 2026 on Consultations with Parties and Participants Regarding the 'E-Court Protocol', ICC-01/21-01/25-469-Anx, 17 June 2026, pp. 18-21, Table 3.

Field Name	Data Type	Explanation	Example	One to
Expert Verification	Boolean	YES= the item will be accompanied by an expert verification report at the time of its submission as evidence.NO= the item will not be accompanied by an expert verification report at the time of its submission as evidence	Yes or No	N/A

24. It is proposed that such expert verification reports, which can cover multiple items of evidence, should always accompany open source and user-generated evidence submitted to the Chamber in the present case. User-generated evidence would include material sourced from OTPLink and screenshots of text messages that are unaccompanied by a statement or testimony from an individual who authored any of the messages or participated in the exchange.

25. In the Defence's view, any such expert report ought to include, at a minimum, information on: the source of the item (both the sender/uploader and the creator of the piece of evidence, if known); its chain of custody and whether the item is the original or a copy; its metadata and any other technical aspects, such as the hash value generated at the time of capture; the steps taken to verify the material and to check for editing or manipulation.[31] It should also include information on the qualifications and experience of the person who undertook those steps to verify the material on behalf of the tendering party, and the methodology that they followed. Without this information, it would be very difficult for the Chamber to come to a view on the evidence's relevance and admissibility, pursuant to Article 69(4) of the Statute. To this end, the Chamber may wish to approve a template ahead of trial for such expert verification reports. The Defence would be happy to liaise with the other parties and ideally make joint submissions on the fields that the parties believe should be included in such a template.

V. CONCLUSION

[31] The main analytical methods used are geolocation; chronolocation; cross-referencing; checking for internal consistency and obvious signs of manipulation; conducting source analysis; and other non-visual considerations: *see* *Evaluating digital open source imagery: A guide for judges and fact-finders*, TRUE Project, 2024, pp. 12-29; *Berkeley Protocol*, paras. 176-207.

26. Since the first status conference in this case, the Prosecution has been on notice that the Trial Chamber wishes to avoid "unnecessary and irrelevant evidence" being "dumped into the court record".[32] In response to the Chamber's request for information as to whether open source material would be introduced through an expert, the Prosecution agreed to consider that proposition. The Defence submits that the Prosecution's apparent proposed solution to this issue (the addition of a "URL" metadata field in NUIX) is wholly insufficient. All it signifies is that the item once existed on the internet. Nevertheless, the Defence has agreed to support the proposed metadata field being added to NUIX, through an amendment to the E-Court Protocol approved by the Trial Chamber.

27. In view of both the quantity and quality of the evidence disclosed to it to date, the Defence is concerned that the evidentiary record in the present case risks being overwhelmed by material of dubious relevance, authenticity and reliability. This is particularly pertinent in view of the information ecosystem surrounding this case, coming from a situation country with over 70 million smartphone users[33] and the highest average screen time in the world,[34] who are following these proceedings and engaging online in a volume never before experienced in a case before the ICC.

28. As a first step to mitigate against this risk, the E-Court Protocol should be further amended in advance of trial, to add a new "Expert Verification" field for open source and user-generated evidence. This field would confirm that, when the item is submitted to the Court, it will (or will not) be accompanied by an expert report.

VI. RELIEF SOUGHT

29. On the basis of the above submissions, the Defence respectfully requests the Trial Chamber to order an amendment to the E-Court Protocol to add an "Expert Verification" field as outlined above.

---

[32] Transcript of the First Status Conference, p. 19, lines 23-25.
[33] D.A. Cordero Jr, "Mastering Smartphones through Enhancement of Physical Activity in Adolescents" 45(2) *Korean journal of family medicine* (2024) 121. According to the same source, there were over 37 million smartphone users in the Philippines in 2019.
[34] K. Purnell, "The Philippines has highest average screen time on phones – study", *Philstar*, 21 May 2023.

Mr Peter Haynes, KC
Counsel for Mr Rodrigo Roa Duterte

Dated this 3rd day of September 2026
At The Hague, the Netherlands