

THE SOCIAL MEDIA BATTLEFIELD: USER-GENERATED CONTENT AS EVIDENCE IN INTERNATIONAL ATROCITY CASES

*Mikiko Galpin**

The Russia-Ukraine war has been called “the most documented war in history,” having featured prominently on social media platforms. With the issue of a warrant for Putin’s arrest, the International Criminal Court (ICC) takes on the challenge of sorting through the myriad of information published publicly and recorded by ordinary citizens. The ICC, and other war crimes tribunals, have admitted some types of open source information in past cases but have not yet ruled on the admissibility of user-generated evidence collected from social media platforms. As this evidence continues to grow in prevalence, this Comment emphasizes the necessity for the ICC to develop protocols and clear guidelines to handle and properly utilize user-generated digital evidence and highlights how the inability to collect such evidence may result in a loss of procedural and sociological legitimacy for the Court.

* J.D. Candidate, Law and Public Policy Scholar, and Conwell Scholar, Temple University Beasley School of Law, 2024; B.F.A., Creative Writing, University of British Columbia, 2017. I would like to thank Professor Duncan B. Hollis for his advice and guidance as my faculty advisor and the TICLJ staff for their tireless editing work and contributions. To my parents, thank you for your continued love and support.

TABLE OF CONTENTS

I. INTRODUCTION.....	74
II. INTERNATIONAL TRIBUNALS AND INNOVATION THROUGH EVIDENCE.....	78
<i>A. An Overview of the ICC.....</i>	78
<i>B. The Admissibility of Evidence Before the ICC.....</i>	81
<i>C. Defining Open Source Information and Evidence.....</i>	83
III. EVIDENCE BEFORE INTERNATIONAL CRIMINAL TRIBUNALS: HISTORY AND INNOVATION	85
<i>A. A Historical Perspective of Open Source Evidence Before the ICC.....</i>	86
<i>B. Diversifying Evidence: The Necessary Shift Away from Witness Testimony.....</i>	87
<i>C. User-Generated Content and Future Innovation</i>	89
IV. THE ICC'S LEGITIMACY AND THE NECESSITY OF USER-GENERATED EVIDENCE	92
V. THE COMPLICATIONS OF USER-GENERATED DIGITAL EVIDENCE .97	
<i>A. Difficulties in Collecting and Storing User-Generated Evidence.....</i>	97
<i>B. Securing Digital Evidence During Storage</i>	100
<i>C. Verification of Digital Evidence and Deepfakes</i>	101
VI. RECOMMENDATIONS FOR THE ICC'S PROCESS.....	103
<i>A. Standardizing Protocols for Collection of Digital Evidence</i>	104
<i>B. Education of Judges and Prosecutors</i>	105
<i>C. Security Assessment of the ICC's Databases</i>	106
VII. THE FUTURE OF ATROCITY PROSECUTIONS: UKRAINE AS A CASE STUDY.....	107
VIII. CONCLUSION.....	111

I. INTRODUCTION

On March 17, 2023, the International Criminal Court (ICC or the “Court”) issued a warrant for the arrest of Russian President, Vladimir Putin.¹ The warrant charged Putin with the war crimes of unlawful deportation of a population—in this case, Ukrainian children—and the unlawful transfer of this population from occupied areas of Ukraine to Russia with the alleged intention of erasing their Ukrainian identities.² The ICC’s actions bolster hope that Putin and his accomplices

1. Situation in Ukraine: ICC Judges Issue Arrest Warrants Against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova, INT’L CRIM. CT. (Mar. 17, 2023), <https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and> [hereinafter ICC Judges Issue Arrest Warrants].

2. *Id.*; see also Stephen Pomper, *How Will the ICC’s Arrest Warrant for Putin Play Out in Practice?*, JUST SEC. (Mar. 20, 2023), <https://www.justsecurity.org/85597/how-will-icc-arrest-warrant-for-putin-play-out> (discussing alleged intent of deportation of Ukrainian children).

will be held accountable for the atrocities committed in Ukraine, which have been widely documented online and by the media.³ The actions of the ICC prosecutor also highlight the central role digital evidence, particularly user-generated digital evidence, will play in prosecuting war crimes and other atrocities.⁴

While the ICC has not openly discussed the evidence against Putin on which the warrant is based, ICC prosecutor Karim Khan stated that the Court has “draw[n] on advanced technological tools” to build their case, which likely refers to some form of digital evidence.⁵ Indeed, the Associated Press has compiled a myriad of photos and videos depicting the abduction of Ukrainian children.⁶ This digital evidence details how, despite presenting documentation at Russian checkpoints, children have been separated from their families and deported to Russia.⁷ Advocacy organizations have also used media posted on Russian social media platforms Yandex.Dzen and VKontakte to map the locations inside Russia where the Russian government forcibly deported Ukrainian children.⁸ The deportations of Ukrainian children are not the only atrocities being captured by civilians and viewed on online platforms.⁹ The prevalence of social media and advances in camera phone technology have led to a rise in open source evidence of atrocities, which will play a significant role in the investigation of the Russia-Ukraine war and future conflicts.¹⁰

3. See Pomper, *supra* note 2 (discussing how warrants against Putin and Lvova-Belova create international sense of hope that Russian leadership will be held accountable for crimes committed in Ukraine).

4. Ronald Niezen, *International Criminal Court Is Using Digital Evidence to Investigate Putin – But How Can It Tell if a Video or Photo Is Real or Fake?*, THE CONVERSATION (May 16, 2023, 8:40 AM), <https://theconversation.com/international-criminal-court-is-using-digital-evidence-to-investigate-putin-but-how-can-it-tell-if-a-video-or-photo-is-real-or-fake-204338> (highlighting rising significance of digital evidence for war crimes tribunals).

5. *Id.*; Karim A. A. Khan, *Statement by Prosecutor Karim A. A. Khan KC on the Issuance of Arrest Warrants Against President Vladimir Putin and Ms Maria Lvova-Belova*, INT’L CRIM. CT. (Mar. 17, 2023) <https://www.icc-cpi.int/news/statement-prosecutor-karim-khan-kc-issuance-arrest-warrants-against-president-vladimir-putin> (discussing sources of “relevant information and evidence” gathered by ICC Office of the Prosecutor).

6. Sarah El Deeb et al., *How Moscow Grabs Ukrainian Kids and Makes Them Russians*, ASSOC. PRESS (Mar. 17, 2023, 4:45 PM), <https://apnews.com/article/ukrainian-children-russia-7493cb22c9086c6293e1ac7986d85ef6> (documenting experiences of Ukrainian children deported to Russia).

7. *Id.*

8. *Activists Map Deported Ukrainian Children in Russia*, THE MOSCOW TIMES (May 23, 2023), <https://www.themoscowtimes.com/2023/05/23/activists-map-deported-ukrainian-children-in-russia-a81244>.

9. See Britt McCandless Farmer, *How Bellingcat Is Using TikTok to Investigate the War in Ukraine*, CBS NEWS (Aug. 21, 2022, 5:57 PM), <https://www.cbsnews.com/news/bellingcat-tiktok-ukraine-60-minutes-2022-08-21/> (discussing atrocities captured by civilians posted to TikTok and other social media platforms).

10. See Lindsay Freeman, *Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court*, in DIGITAL WITNESS: USING OPEN SOURCE INFORMATION FOR HUMAN RIGHTS INVESTIGATION, DOCUMENTATION, AND ACCOUNTABILITY 48, 50–52 (Sam Dubberley et al. eds., 2020) (noting social media’s frequent use in documenting atrocities in Ukraine and its growing importance to ICC).

The Russia-Ukraine war has been called—and most likely is—“the most documented war in history.”¹¹ Social media platforms such as Facebook,¹² TikTok,¹³ and Telegram¹⁴ have featured prominently in headlines due to the prevalence of their role in the conflict, both to spread disinformation and to document the atrocities being committed in Ukraine.¹⁵ This flood of information began before the invasion; civilians uploaded videos of Russian tanks to TikTok in the weeks leading up to the Russian invasion.¹⁶ Then, on February 24, 2022, Russia began a three-pronged troop invasion of Ukraine using airstrikes and missiles to bolster the Russian advancement from the north, south, and east.¹⁷ Within twenty-four hours, a wealth of information

11. Daniel Johnson, *Ukraine Could Be the Most Documented War in Human History*, SLATE (Feb. 24, 2022), <https://slate.com/technology/2022/02/ukraine-russia-livestream-google-maps.html>; see also Washington Post Staff, *Database of 305 Videos Exposes the Horrors of War in Ukraine*, THE WASHINGTON POST, <https://www.washingtonpost.com/world/interactive/2022/ukraine-russia-war-videos-verified/> (last updated Feb. 24, 2023, 8:40 PM) (discussing vast amount of documentation of war in Ukraine); see also Farmer, *supra* note 9 (explaining ways this war has been documented and how this documentation has been gathered).

12. See, e.g., Ben Collins, *Four House Committee Chairs Ask Big Tech to Archive Evidence of War Crimes in Ukraine*, NBC NEWS (May 13, 2022, 2:11 AM), <https://www.nbcnews.com/tech/internet/democrats-ask-facebook-youtube-archive-evidence-war-crimes-rcna28563> (discussing how content posted to Facebook could be used to hold Russia accountable for its atrocities).

13. See, e.g., Johnson, *supra* note 11 (noting that TikTok has been used to provide information about ongoing events in Ukraine).

14. See e.g., Bobby Allyn, *Telegram Is the App of Choice in the War in Ukraine Despite Experts' Privacy Concerns*, NPR (Mar. 14, 2022, 7:19 PM), <https://www.npr.org/2022/03/14/1086483703/telegram-ukraine-war-russia> (discussing how Telegram has become a primary news source for Ukrainian refugees who cannot access traditional Ukrainian news sources).

15. See, e.g., Naomi Nix, *In Ukraine, Facebook Fact-Checkers Fight a War on Two Fronts*, THE WASHINGTON POST, (Apr. 12, 2022, 3:00 AM), <https://www.washingtonpost.com/technology/2022/04/12/facebook-fact-checkers-misinformation-ukraine-war/> (highlighting one example of Facebook being used as a source of disinformation); see e.g., Farmer, *supra* note 9 (noting nearly 70% of evidence from Ukraine war gathered by Bellingcat is from TikTok); see Theo Wayt, *TikTok Accused of Hampering Ukraine War Crimes Investigations: Report*, NEW YORK POST (July 15, 2022, 11:54 AM), <https://nypost.com/2022/07/15/tiktok-accused-of-hampering-ukraine-war-crimes-investigations-report/> (reporting that TikTok has been failing to preserve videos of human rights abuses because the company deems them inappropriate); see generally *Disinformation and Russia's War of Aggression Against Ukraine*, OECD POLICY RESPONSES: UKRAINE 2 (Nov. 3, 2022), <https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/#contact-d4e6699> (discussing how Russia-Ukraine war has been waged online due to rise in internet coverage and social media usage).

16. See Kiko Llaneras, *The War in Ukraine via TikTok: How Ordinary Citizens Are Recording Russian Troops*, EL PAIS (Feb. 24, 2022, 06:26 AM), <https://english.elpais.com/science-tech/2022-02-24/the-war-in-ukraine-via-tiktok-how-ordinary-citizens-are-recording-russian-troops.html> (describing how civilians were uploading videos of Russian tanks on social media in lead up to and during war).

17. Jacklyn Goloborodsky, *Russia Launches a Full Scale Attack on Ukraine on Feb. 24*, THE JUST. (Mar. 8, 2022, 11:00 AM), <https://www.thejustice.org/article/2022/03/russia-launches-a-full-scale-attack-on-ukraine-on-feb-24-brandeis>.

exploded online, ranging from actual combat footage on Reddit to footage of airstrikes on Twitter.¹⁸ Sorting through the myriad of information is not an easy task, but it is one that must be undertaken by the ICC to preserve and use this digital evidence in war crimes prosecutions.¹⁹

The ICC, and other war crimes tribunals, have admitted some types of open source information in past cases but have not yet ruled on the admissibility of user-generated evidence collected from social media platforms.²⁰ Victims, non-governmental organizations, and those who wish to see the perpetrators of war crimes brought to justice face a variety of hurdles in admitting this vital evidence in international tribunals.²¹ Numerous scholars have predominantly focused on the benefits or drawbacks of using digital evidence in the context of atrocity prosecution, as well as the technological and legal obstacles to obtaining user-generated evidence.²² This Comment emphasizes the necessity for the ICC to develop protocols and clear guidelines to handle and properly utilize user-generated digital evidence because this evidence is rapidly becoming one of the largest bodies of evidence available to the tribunal²³ and the inability to collect such evidence may result in a loss of procedural and sociological legitimacy.

As the significance of user-generated evidence grows, the ICC must improve its ability to collect, preserve, verify, and present accurate digital evidence in court to contribute to the legitimacy of the Court.²⁴ Admitting user-generated digital evidence is a natural evolution for the Court and is necessary for the Court to hold perpetrators of atrocities accountable.²⁵ The Court is not without guidance on this matter as guidelines governing the collection of digital evidence have recently been released.²⁶ The Court must take steps now to standardize its protocols for handling

18. Johnson, *supra* note 11.

19. See Niezen, *supra* note 4 (discussing ICC procedures for authenticating digital evidence and how this evidence is necessary to prosecute Russian war crimes).

20. See *infra* Part III for an overview of open source evidence before the ICC and other international tribunals.

21. See Rome Statute of the International Criminal Court art. 73, *opened for signature* July 17, 1998, 2187 U.N.T.C. 38544 (noting that the ICC must obtain consent to admit evidence created by third parties).

22. See, e.g., Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, 41 FORDHAM INT'L L. J. 283, 297–98 (2018) (discussing legal hurdles to admitting digital evidence in an ICC case); see also Jeff Deutch & Hadi Habal, *The Syrian Archive: A Methodological Case Study of Open-Source Investigation of State Crime Using Video Evidence from Social Media Platforms*, 7.1 STATE CRIME J. 46, 48 (2018) (explaining physical problems of maintaining digital evidence for use in an ICC case).

23. E.g., Deutch & Habal, *supra* note 22, at 50 (noting that there are now more hours of user-generated content about Syrian conflict on YouTube than hours of the conflict itself).

24. See *id.* at 47–48 (defining problems of using open-source information in human rights enforcement).

25. See generally Freeman, *supra* note 10, at 53–57 (explaining history of open source information in ICC cases).

26. See generally UNITED NATIONS & HUM. RTS. CTR. UC BERKELEY SCH. OF L., BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS (Sareta Ashraph et al. eds., 2022) [hereinafter BERKELEY PROTOCOL].

digital evidence, educate judges and other judicial actors on the importance of this evidence, and ensure that the Court has the technological capacity to safely store large volumes of digital evidence. In doing so, the Court can promote best practices for civil society organizations, journalists, and other actors who seek to preserve digital evidence in a form that will be admissible before international tribunals.

Part II of this Comment discusses the ICC's jurisdiction, summarizes the admissibility of evidence before the ICC, and defines open source content and digital evidence. Part III traces the history of open source evidence before the Court, illustrating the ways in which innovation has shaped prosecution techniques. This Comment then emphasizes the benefits of user-generated content and how this evidence can be used effectively to prosecute atrocities, an area that has often suffered from a lack of viable evidence. Part IV discusses the normative and sociological legitimacy of the ICC as a judicial body and how these concepts can be impacted by the Court's ability, or inability, to utilize digital evidence.

Next, Part V addresses complications that may arise when using digital evidence and how these concerns can be mitigated with proper protocols and processes on the part of judicial actors. Part VI follows with recommendations that can be implemented by the ICC to prepare for the use of digital evidence in future atrocity cases. Finally, Part VII concludes with a case study of how the successful implementations of the recommendations in Part VI may affect the investigations and prosecution of atrocities committed during the Russia-Ukraine war.

II. INTERNATIONAL TRIBUNALS AND INNOVATION THROUGH EVIDENCE

A. *An Overview of the ICC*

The ICC is the first treaty-based, permanent international criminal court.²⁷ The ICC was established in 1998 by the Rome Statute, a treaty adopted by a conference of 160 states and which entered into force in 2002 to adjudicate “the most serious crimes of international concern.”²⁸ The Rome Statute provides the crimes over which the ICC has jurisdiction,²⁹ as well as the rules, procedures, and mechanisms that govern the ICC's operation and cooperation with states.³⁰ Currently, 123 countries are parties to the Rome Statute,³¹ but this is far from the Court's goal of universal ratification.³²

27. INT'L CRIM. CT., UNDERSTANDING THE INTERNATIONAL CRIMINAL COURT 10 (2020) [hereinafter UNDERSTANDING THE ICC].

28. *Id.* at 9-11; Rome Statute of the International Criminal Court, *supra* note 21, art. 1.

29. The most serious crimes are enumerated in the Rome Statute as genocide (Article 6), crimes against humanity (Article 7), and war crimes (Article 8). Rome Statute of the International Criminal Court, *supra* note 21, art. 6-8.

30. See UNDERSTANDING THE ICC, *supra* note 27, at 10-15 for a discussion on the governing rules of the ICC.

31. *The States Parties to the Rome Statute*, INT'L CRIM. CT., <https://asp.icc-cpi.int/states-parties> (last visited Nov. 17, 2023).

32. *Id.*; Meeting Coverage, U.N.G.A., Universal Ratification of Rome Statute Crucial to Reduce Impunity for Atrocity Crimes, International Criminal Court President Tells General Assembly, U.N. Meetings Coverage GA/12210 (Nov. 4, 2019) (discussing needs for ICC to have

The Rome Statute dictates the specific circumstances in which the ICC is granted jurisdiction over a case.³³ State Parties to the Rome Statute agree to submit themselves to the ICC's jurisdiction for the crimes enumerated in the Statute.³⁴ The Rome Statute also provides additional avenues for jurisdictional grants.³⁵ One such avenue is that a state not party to the Rome Statute can voluntarily accept the jurisdiction of the ICC.³⁶ Situations within the Court's jurisdiction involving non-state parties can be referred to the Office of the Prosecutor by State Parties.³⁷ Situations with non-states parties may also be referred by the U.N. Security Council when it acts under its Chapter VII powers.³⁸

The ICC currently has territorial jurisdiction over war crimes committed in Ukraine because Ukraine has submitted two declarations accepting the ICC's jurisdiction under Article 12(3) of the Rome Statute.³⁹ The first declaration accepted the Court's jurisdiction for any alleged crimes occurring in Ukraine between November 2013 and February 2014 during the Maidan protests.⁴⁰ The acceptance of jurisdiction was subsequently extended in the second declaration; the ICC's jurisdiction expanded to cover alleged crimes against humanity committed by Russia in Ukraine from February 2014 onwards.⁴¹ In addition to Ukraine's declarations, a total of forty-three State Parties have referred the situation in Ukraine to the Office of the Prosecutor.⁴² The Office of the Prosecutor has opened an investigation on

universal ratification), <https://press.un.org/en/2019/ga12210.doc.htm>; see Steven W. Becker, *The Objections of Larger Nations to the International Criminal Court*, 81 REVUE INTERNATIONALE DE DROIT PÉNAL 47, 48, 53 (2010) (discussing why several of the world's largest nations, including the United States, voice strong objections to ICC).

33. Rome Statute of the International Criminal Court, *supra* note 21, art. 5–8, 11–14.

34. The ICC can exercise jurisdiction where the perpetrator is a national of a State Party or when the crime is committed in the territory of a State Party. UNDERSTANDING THE ICC, *supra* note 27, at 11; Rome Statute of the International Criminal Court, *supra* note 21, art. 12(1) (referencing the list of enumerated crimes found in article 5).

35. See Rome Statute of the International Criminal Court, *supra* note 21, art. 12–14 (listing alternative routes of jurisdiction).

36. UNDERSTANDING THE ICC, *supra* note 27, at 11; Rome Statute of the International Criminal Court, *supra* note 21, art. 12(3).

37. Rome Statute of the International Criminal Court, *supra* note 21, art. 14.

38. See *id.* art. 13 (listing ways that ICC may exercise jurisdiction over non-state parties); see also UNDERSTANDING THE ICC, *supra* note 27, at 11 (describing situations under which ICC jurisdiction is appropriate).

39. *Ukraine*, INT'L CRIM. CT., <https://www.icc-cpi.int/ukraine> (last visited Nov. 17, 2023); see Rome Statute of the International Criminal Court, *supra* note 21, art. 12(3) (explaining process for submitting declaration to accept ICC jurisdiction); see generally, *Statement of the Prosecutor of the International Criminal Court, Fatou Bensouda, on the alleged crimes committed by ISIS*, INT'L CRIM. CT. (Apr. 8, 2015), <https://www.icc-cpi.int/news/statement-prosecutor-international-criminal-court-fatou-bensouda-alleged-crimes-committed-isis> (differentiating between personal and territorial jurisdiction of ICC).

40. *Ukraine*, INT'L. CRIM. CT. PROJECT, <https://www.aba-icc.org/country/ukraine/> (last visited Nov. 17, 2023).

41. *Declaration of the Verkhovna Rada of Ukraine*, V.R. No. 145-VIII (Ukr.), <https://www.icc-cpi.int/sites/default/files/itemsDocuments/997/declarationVerkhovnaRadaEng.pdf>.

42. See *Ukraine*, *supra* note 40 (listing states that have referred situation in Ukraine to ICC).

Ukraine, which will encompass any enumerated crimes committed in the territory of Ukraine from November 21, 2013 onwards.⁴³

The warrant for Putin's arrest has raised further questions about whether the ICC can successfully obtain jurisdiction over Putin, which would be the first step towards accountability.⁴⁴ Putin is a national of Russia, a state that is not party to the Rome Statute and thus has not submitted to the jurisdiction of the Court.⁴⁵ In the past, some states have objected to the ICC exerting jurisdiction over nationals of non-party states.⁴⁶ The United States is a strong supporter of this persistent minority view.⁴⁷ Member states to the Rome Statute, such as South Africa and Brazil, may signal further support for a lack of ICC jurisdiction over Putin by allowing Putin to freely travel in and out of their countries.⁴⁸

However, even if jurisdiction is proper, additional issues of jurisdiction must be considered under the Rome Statute.⁴⁹ "The ICC is a court of last resort, and . . . requires national courts to have primary jurisdiction."⁵⁰ As detailed by Article 17 of the Rome Statute, the ICC only has jurisdiction when states are unwilling or unable to prosecute cases.⁵¹ For a case to be admissible, it must also be of "sufficient gravity to justify further action by the Court."⁵² Assessing the gravity of a case includes considerations such as the "scale and nature, the manner in which they were carried out, their impact on the victims, and any aggravating circumstances."⁵³ However, the Office of the Prosecutor can apply a stricter test than what is statutorily required when assessing gravity for the purposes of case selection.⁵⁴ Although the Office of

43. *Id.*

44. See Miles Jackson, *The ICC Arrest Warrants Against Vladimir Putin and Maria Lvova-Belova – An Outline of the Issues*, EJIL: TALK! (Mar. 21, 2023), <https://www.ejiltalk.org/the-icc-arrest-warrants-against-vladimir-putin-and-maria-lvova-belova-an-outline-of-issues/> (discussing legal and practical problems of obtaining jurisdiction over Putin).

45. *Id.*

46. *Id.*

47. *Id.*

48. See Pomper, *supra* note 2 (noting potential damage to ICC credibility where states fail to arrest Putin within their territories).

49. See Rome Statute of the International Criminal Court, *supra* note 21, art. 17 (enumerating factors which would lead to case being inadmissible).

50. Freeman, *supra* note 10, at 57.

51. Article 17(1)(b), (2), and (3) elaborate on the unwilling and unable criteria, noting situations where cases are inadmissible based on domestic prosecutions (or lack thereof) and detailing considerations for determining unwillingness or inability. Rome Statute of the International Criminal Court, *supra* note 21, art. 17; Cf. Darryl Robinson, *The Mysterious Mysteriousness of Complementarity*, 21 CRIM. L.F. 67, 70-71 (highlighting that complementarity is a two part test which finds that cases remain admissible before the Court where (i) there are no national proceedings concerning the case and (ii) there are national proceedings but the State is unwilling or unable to genuinely carry out the proceedings).

52. *Id.* art. 17(1)(d).

53. Situation in the Republic of Côte d'Ivoire, Case No. ICC-02/11, Corrigendum to 'Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Republic of Côte d'Ivoire', ¶ 204 (Nov. 15, 2011), https://www.icc-pi.int/sites/default/files/CourtRecords/CR2011_18794.PDF.

54. See Policy Paper on Case Selection and Prioritisation, INT'L CRIM. CT. OFF. OF THE

the Prosecutor has discretion in applying the gravity standard, conflicts or human rights violations that attract global attention will more easily meet the standard.⁵⁵ The Russia-Ukraine war has likely met this standard based solely on the record-breaking number of State Parties that referred the situation to the Office of the Prosecutor,⁵⁶ demonstrating significant international concern.⁵⁷

B. The Admissibility of Evidence Before the ICC

The Rome Statute and the Rules of Procedure and Evidence (RPE) for the ICC lay out fairly permissible standards for assessing evidence.⁵⁸ The Rome Statute adopted a combination of civil and common law legal concepts.⁵⁹ When considering the admissibility of evidence, the ICC skews predominantly towards the flexibility of the civil law system, foregoing much of the more rigid technical process of the common law.⁶⁰ Under this flexibility, judges have wide discretion to determine the weight and scope of evidence before them.⁶¹ Surprisingly, this discretion has limited the use of open source material.⁶² Judicial discretion is applied through an analysis of three factors laid out in Article 69 of the Rome Statute considered in light of the type of evidence.⁶³ The judge may consider (i) the relevance of the evidence, (ii) its probative value, and (iii) its potential for any prejudicial effect.⁶⁴ While the ICC applies the three-part test to all categories of evidence, the type of evidence becomes relevant when assessing the probative value because the evidentiary weight assigned

PROSECUTOR, 13 (2016), https://www.icc-cpi.int/sites/default/files/itemsDocuments/20160915_OTP-Policy_Case-Selection_Eng.pdf; see also Freeman, *supra* note 10, at 59 (noting that Office of the Prosecutor utilizes qualitative and quantitative assessments of gravity when selecting and charging cases).

55. See Freeman, *supra* note 10, at 59-60 (explaining that prosecutions typically target high-profile suspects).

56. See Yvonne Dutton & Melina Sterio, *The War in Ukraine and the Legitimacy of the International Criminal Court*, JUST SEC. (Aug. 30, 2022), <https://www.justsecurity.org/82889/the-war-in-ukraine-and-the-legitimacy-of-the-international-criminal-court> (noting unprecedented number of referrals led to rapid initiation of ICC investigation).

57. Further analysis of the Office of the Prosecutor's determination on the fulfillment of these three factors is outside the scope of this paper. This paper proceeds under the assumption that the Russia-Ukraine war has met the standard of gravity. See *id.* (noting twenty states contributed financially to the ICC, twenty-one committed to sending national experts to the Office of the Prosecutor's team).

58. See Rules of Procedure and Evidence, Doc. No. ICC-PIOS-LT-03-004/19_Eng (2019), <https://www.icc-cpi.int/sites/default/files/Publications/Rules-of-Procedure-and-Evidence.pdf> (explaining supplementary rules of procedure and evidence subordinate to Rome Statute of the ICC).

59. See Bartłomiej Krzan, *Admissibility of Evidence and International Criminal Justice*, 7 REV. BRAS. DE DIREITO PROCESSUAL PENAL 161, 168-69 (discussing how Rome Statute adopted flexibility of civil law system for determining relevance and admissibility of evidence).

60. *Id.* at 169.

61. See *id.* at 171 (describing judicial system of "utmost flexibility").

62. Freeman, *supra* note 10, at 51.

63. Rome Statute of the International Criminal Court, *supra* note 21, art. 69(4). While Part 6 of the Rome Statute where Article 69 is found concerns trial proceedings, the Article 69 standard applies to proceedings before all Chambers through Rule 63(1) of the RPE. Krzan, *supra* note 59, at 170.

64. Rome Statute of the International Criminal Court, *supra* note 21, art. 69(4).

can vary by category.⁶⁵

Evidence law textbooks often identify four categories of evidence: testimonial, documentary, physical, and forensic.⁶⁶ Online open source evidence is mostly considered to be categorized as documentary or forensic evidence.⁶⁷ Digital and electronic forms of evidence are assessed under the same criteria as paper forms of these documents.⁶⁸ Some online open source evidence could also be considered forensic evidence even if forensic processes, like photograph augmentation, have been applied.⁶⁹ Finally, online open source evidence can be introduced as part of an expert report which would require additional considerations before being admitted.⁷⁰

Assuming it constitutes documentary evidence, the Court will look at a variety of factors in examining user-generated evidence including its provenance and source, the source's role in the relevant events, the chain of custody from creation to submission to the Court, and any other information deemed relevant by the Court.⁷¹ These factors are particularly important because judges may give little weight to online user-generated open source evidence that cannot be authenticated or lacks an identifiable source.⁷²

The assessment of these factors contributes to the effectiveness and legitimacy of the ICC. In terms of effectiveness, if judges are unable to accurately assess user-generated content due to lack of expertise, they assign less value than these sources merit. Additionally, judges may be unable to assign adequate value to user-generated digital evidence if the ICC is not equipped to assess, store, and verify this evidence. As a matter of legitimacy, a failure to utilize readily available evidence which has been viewed globally across social media will undermine confidence in the Court,

65. See Freeman, *supra* note 22, at 295 (discussing Chamber's assessment of weight to be attributed to any item of evidence depending on type of evidence).

66. *Id.*

67. See *id.* at 297 (explaining that most digital evidence is considered documentary or forensic evidence, depending on whether any analysis or scientific procedure has been applied in order to validate or verify the digital item); THE INTERNATIONAL CRIMINAL COURT, DOCUMENTING INTERNATIONAL CRIMES AND HUMAN RIGHTS VIOLATIONS FOR ACCOUNTABILITY PURPOSES: GUIDELINES FOR CIVIL SOCIETY ORGANIZATIONS, 33 (2022) [hereinafter GUIDELINES FOR CIVIL SOCIETY ORGANIZATIONS] (explaining how digital information like documentary evidence needs to be handled with care and by experts when handling electronic devices).

68. See, e.g., Freeman *supra* note 22, at 297 (listing forms of digital evidence that are evaluated as if they were paper documents).

69. See *id.* (specifying that if forensic processes have been applied to digital information (i.e., audio enhancement or photograph augmentation) or an analytic product or expert report has been compiled using raw digital data (i.e., a geolocated photograph or call sequence table) that evidence may have to be introduced through an expert witness, which would require additional conditions to be met).

70. *Id.*

71. Prosecutor v. Bemba, Case No. ICC-01/05-01/08, Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute, ¶¶ 10–13 (Nov. 29, 2013) https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2013_10117.PDF. The burden of proving admissibility lies with the party seeking admission. Freeman, *supra* note 22, at 296.

72. See Freeman, *supra* note 22, at 297 (discussing how digital evidence may be given little weight if it cannot be sourced or authenticated).

leading to a lack of cooperation by member states both in arresting perpetrators and funding the Court.⁷³

C. Defining Open Source Information and Evidence

Open source information is “publicly available information that anyone can obtain by request, purchase, or observation.”⁷⁴ Traditionally, open source information included physical documents and pictures compiled by civilians, journalists and news outlets, political figures, governments, and others.⁷⁵ The internet and technological innovations, such as camera phones, have led to a rise in online and electronic open source information.⁷⁶ Examples include PDF documents, user data and statistics, and social media posts.⁷⁷ Since the 1990s, digital open source information and access to such information has increased dramatically due to four key developments: satellite imagery, camera-enabled phones, digital social networks, and more publicly accessible data such as weather data, government records, and census data.⁷⁸ Each of these innovations has played a key role in the analysis, documentation, and reporting of conflicts.⁷⁹ Two in particular—camera-enabled phones and digital social networks—are significant for the prosecutions of war crimes.⁸⁰ These two innovations have provided civilians with the means to document potential evidence of war crimes or atrocities as they are happening and upload the footage for the world to see.⁸¹

Open source information, online and otherwise, can be referred to as “open source evidence” in two situations: first, when it is used to prove facts in a judicial hearing,⁸² and second, when it is recorded with the intent of being used to achieve legal accountability for wrongdoing.⁸³ While user-generated social media evidence

73. The ICC itself is not granted the power to enforce warrants. As such, the Court is completely reliant on member states to execute arrest warrants. INTERNATIONAL CRIMINAL COURT, ARRESTING ICC SUSPECTS AT LARGE, 12, 14 (2019), <https://www.icc-cpi.int/sites/default/files/bookletArrestsENG.pdf>.

74. Sam Dubberley et al., *Introduction: The Emergence of Digital Witnesses*, in DIGITAL WITNESS 3, 9 (Dubberley et al. eds., 2020).

75. See, e.g., Rebecca J. Hamilton, *User-Generated Evidence*, 57 COLUM. J. OF TRANSNAT'L L. 1, 3–5 (2018) (describing how advances in technology have changed nature of user-generated evidence and provided certain advantages).

76. See *id.* at 4–5 (describing impact of cell phones, high speed internet, and social media uploads on documenting human rights abuses).

77. Dubberley et al., *supra* note 74, at 9.

78. See generally Christoph Koettl et al., *Open Source Investigation for Human Rights Reporting: A Brief History*, in DIGITAL WITNESS 12, 14–18 (Sam Dubberley et al. eds., 2019) (explaining key examples of pivotal technological developments enabling open source investigations since mid-20th century).

79. See *id.* at 18 (discussing impact of technological developments on human rights research).

80. See Hamilton, *supra* note 75, at 11 (noting significance of ordinary civilian witnesses to record and share evidence of atrocities).

81. *Id.* at 3–4.

82. Dubberley et al., *supra* note 74, at 10.

83. Hamilton, *supra* note 75, at 3.

has not yet been relied on before an international criminal tribunal,⁸⁴ open source evidence more generally has been a staple of international criminal trials since the International Military Tribunal for Nuremberg (the Nuremberg Trial).⁸⁵ During the Nuremberg Trial, prosecutors relied heavily on documents, videos, and photographs created by the Nazis themselves to demonstrate both the atrocities committed and the intent required for charging genocide.⁸⁶ However, the use of open source evidence was a novel approach for prosecutors.⁸⁷ The Office of the Prosecutor continues to adapt to new forms of open source evidence.⁸⁸ User-generated evidence represents a new tool which the Office of the Prosecutor can utilize at trial under the ICC's flexible evidence standards.

User-generated videos and pictures have been produced in abundance and are potential forms of digital evidence in the Russia-Ukraine war.⁸⁹ User-generated evidence is content recorded by ordinary people, generally through the use of a smartphone, with the intent to help achieve legal accountability for wrong-doing.⁹⁰ This digital content can appear on a variety of platforms including blogs, websites, social media posts, and internet archives.⁹¹ While some of this potential user-generated evidence will be removed due to content moderation on social media platforms,⁹² some will remain accessible on public sites, creating the likelihood that

84. See Alexa Koenig, *Open Source Evidence and Human Rights Cases: A Modern Social History*, in DIGITAL WITNESS 32, 41 (Sam Dubberley et al. eds., 2019) (explaining that user-generated evidence has been used to issue arrest warrant but has not yet been considered by judge during trial).

85. See *infra* Part II.C for a discussion on the history of open source evidence before the ICC.

86. *Evidence from the Holocaust at the First Nuremberg Trial*, UNITED STATES HOLOCAUST MEMORIAL MUSEUM, <https://encyclopedia.ushmm.org/content/en/article/evidence-from-the-holocaust?series=26> [hereinafter *The First Nuremberg Trial*] (last visited Oct. 19, 2023); Freeman, *supra* note 22, at 298.

87. See Freeman, *supra* note 22, at 285 (explaining how Office of the Prosecutor moved away from reliance primarily on witnesses to focus more on documentary evidence in Nuremberg Trials).

88. See *infra* Part III for a discussion of relevant international criminal law cases which utilized new technologies in prosecuting atrocities.

89. See, e.g., Washington Post Staff, *supra* note 11 (hosting database of 305 videos of Russian attacks and their aftermath); Johnson, *supra* note 11 (explaining rise of user-generated content in Russia-Ukraine war); Llaneras, *supra* note 16 (describing use of TikTok by Ukrainian civilians to document Russian aggression).

90. Hamilton, *supra* note 75, at 3.

91. Dubberley et al., *supra* note 74, at 9.

92. See, e.g., Rebecca J. Hamilton, *Social Media Platforms in International Criminal Investigations*, 52 CASE W. RESV. J. OF INT'L L. 213, 221–22 (2020) (highlighting how YouTube and Facebook often practice over-removal of content to comply with state regulatory goals). While retrieval of deleted content is an important step in utilizing user-generated content in international tribunals, the retrieval of de-platformed user-generated content is a complex process which requires a separate legal analysis and suggestions for legislative reform. See *generally id.*; see also *Mass Atrocities in the Digital Age: Preserving Social Media Evidence*, UNIV. OF OXFORD: BLAVATNIK SCH. OF GOV'T., <https://www.bsg.ox.ac.uk/research/mass-atrocities-digital-age-preserving-social-media-evidence> (last visited Feb. 27, 2023) (outlining project dedicated to developing policies to address how private social media corporations can effectively preserve digital evidence and share it with relevant authorities). As such, the technological retrieval process is beyond the scope of this Comment. For the purposes of this Comment, it is enough to recognize the distinction between

some of this evidence will be utilized by prosecutors in war crimes cases.⁹³

There is no shortage of publicly available evidence. The Washington Post has verified videos of Russian tanks abandoned on the side of a dirt road in Izyum, fiery explosions of kamikaze drones striking electrical transmission offices in Kyiv, burnt out windows of a destroyed maternity hospital in Mariupol, and evidence of many more atrocities, which were all filmed and uploaded to various social media platforms.⁹⁴ Citizen videos and photographs have supplemented publicly available evidence for the Ukrainian government.⁹⁵ With the abundance of evidence available, “crowdsourced” user-generated evidence is likely to be introduced in future prosecutions of these atrocities.⁹⁶ Admitting “crowdsourced” evidence will provide the ICC with an opportunity to further innovate—an opportunity the Court must take to prevent falling behind.⁹⁷

III. EVIDENCE BEFORE INTERNATIONAL CRIMINAL TRIBUNALS: HISTORY AND INNOVATION

Open source evidence has a long history before the ICC and other ad hoc international criminal tribunals. Initially, these sources were written documents, particularly war documents like those used at the Nuremberg Trial.⁹⁸ As technology advanced, open source evidence grew to encompass radio broadcasts, as well as digital photographs and videos.⁹⁹ While many sources are now exclusively found in digital formats, the ICC applies the evidentiary standards for print material to these digital formats.¹⁰⁰ Additionally, the Nuremberg Trial demonstrated that using open source evidence originally prepared by the perpetrators was a successful strategy for prosecuting atrocities.¹⁰¹ Tracing the history of evidence before the Court

user-generated content which is still currently available and content that has been de-platformed by social media moderation processes but may still be available in private social media databases. *See* Republic of Gambia v. Facebook, Inc., 575 F. Supp. 3d 8, 10 (D.D.C. 2021) (noting that Facebook had removed accounts promoting ethnic violence against Rohingya from public view but had maintained some content privately). This Comment focuses on user-generated content that is still currently available or has already been preserved prior to deletion.

93. *See eyeWitness to Atrocities App Surpasses Collection of 20,000 Verifiable Items of Potential Human Rights Violations in Ukraine, and Group Submits Evidence to UN COI*, INT’L BAR ASS’N (Oct. 4, 2022) [hereinafter *eyeWitness to Atrocities App*], <https://www.ibanet.org/eyeWitness-to-atrocities-app-surpasses-collection-of-20000-verifiable-items-of-potential-human-rights-violations-in-Ukraine-and-group-submits-evidence-to-UN-COI> (reporting that users of eyeWitness app submitted 20,000 verifiable pieces of content documenting war atrocities in Ukraine).

94. Washington Post Staff, *supra* note 11.

95. Vera Bergengruen, *How Ukraine Is Crowdsourcing Digital Evidence of War Crimes*, Time (Apr. 18, 2022, 6:00 AM), <https://time.com/6166781/ukraine-crowdsourcing-war-crimes>.

96. *See generally id.*

97. *Id.*

98. *E.g., The First Nuremberg Trial*, *supra* note 86.

99. *See* Freeman, *supra* note 22, at 301 (discussing how media such as satellite imagery and radio broadcasts were offered as evidence before international tribunals).

100. *Id.* at 297.

101. *See id.* at 298–99 (explaining how meticulous recordkeeping of Third Reich assisted prosecutors at Nuremberg Trial).

demonstrates that the ICC, and its predecessors, have successfully prosecuted crimes of the utmost gravity and seriousness by innovating when needed to bring perpetrators to justice.

A. A Historical Perspective of Open Source Evidence Before the ICC

The Nuremberg Trial was groundbreaking in its reliance on a large amount of documentary evidence in the form of Third Reich propaganda, photographs, and videos taken by journalists, and official records of the Nazi regime itself.¹⁰² In fact, there was such an abundance of evidence that it shaped Justice Robert H. Jackson's prosecution strategy as Chief of Counsel for the United States.¹⁰³ His opening statement proclaimed, "We will show you their own films."¹⁰⁴ Because of the extensive documentation created by the Nazi regime, Justice Jackson's strategy marked a shift away from the traditional reliance on witnesses to a focus on documentary evidence.¹⁰⁵ Hours of video footage and hundreds of photographs from perpetrators, governments, and journalists, were presented at the trial.¹⁰⁶ The Nuremberg Trial established that international criminal cases could successfully present "the cold, hard facts and evidence."¹⁰⁷ This choice marked a shift from the norm of relying on the testimony of victims which were viewed, up until the Nuremberg Trial, as being most effective at trials because these testimonies invoked an empathetic response.¹⁰⁸ Justice Jackson's strategy at the Nuremberg Trial illustrated the necessity of innovation within more modern international criminal tribunals, like the ICC, to adapt to and take advantage of new forms of evidence.

The next landmark case using open source evidence was *Prosecutor v. Nahimana et al.*, which occurred before the International Criminal Tribunal for Rwanda (ICTR).¹⁰⁹ The ICTR was an ad hoc tribunal established through U.N. Security Council Resolution 955 to address crimes arising during the 1994 genocide of the Tutsi people in Rwanda.¹¹⁰ While early cases before the ICC continued to rely predominantly on witness testimony, the *Nahimana* case introduced another type of open source evidence: radio broadcasts.¹¹¹ In this case, three members of the

102. *Id.* at 298.

103. *Id.* at 299.

104. *Opening Statement Before the International Military Tribunal*, ROBERT H. JACKSON CTR., <https://www.roberthjackson.org/speech-and-writing/opening-statement-before-the-international-military-tribunal> (last visited Jan. 23, 2023).

105. Freeman, *supra* note 22, at 285.

106. *Id.* at 286.

107. *Id.*

108. *Id.*

109. *Id.* at 301 (internal quotations omitted).

110. Anne-Marie de Brouwer, *International Criminal Tribunal for Rwanda*, OXFORD BIBLIOGRAPHIES, <https://www-oxfordbibliographies-com.libproxy.temple.edu/view/document/obo-9780199796953/obo-9780199796953-0177.xml?rskkey=BkCRDq&result=1&q=evi> (last updated Mar. 27, 2019); see *Ad Hoc Tribunals*, INT'L COMM. OF THE RED CROSS (Oct. 29, 2010), <https://www.icrc.org/en/document/ad-hoc-tribunals> (labeling ICTR as *ad hoc* tribunal and explaining process of establishing these tribunals).

111. See Freeman, *supra* note 22, at 301 (explaining how use of radio broadcasts as evidence helped to brand case as landmark).

media—two radio station founding members and a newspaper editor-in-chief¹¹²—were charged with genocide, crimes against humanity, and several other offenses.¹¹³ Key pieces of evidence that ultimately led to their conviction were the recordings of radio broadcasts inciting violence against the Tutsi population.¹¹⁴ The Radio Télévision Libre des Milles Collines promoted extremist Hutu ideology and regularly broadcasted messages commanding the execution of Tutsis with directives such as “go work” and “the graves are not yet full.”¹¹⁵ While radio was not a new technology, expanded data storage capacity allowed for the recordings of the incriminating radio broadcasts to be stored for years after the initial broadcasts, enabling the recordings to be used as evidence.¹¹⁶ As the ICC grapples with the ability to store the vast amounts of digital evidence produced by current investigations, the ICC must once again innovate to remain an effective tribunal for trying the gravest crimes.

B. Diversifying Evidence: The Necessary Shift Away from Witness Testimony

The ICC must innovate to maintain its legitimacy and to reap the significant benefits of user-generated evidence. User-generated digital evidence can be an abundant source of corroborating evidence, which has been lacking in past ICC trials,¹¹⁷ and the use of this evidence can maintain the procedural integrity of the ICC. Digital evidence can support witness testimonies and be used to present forensic evidence in novel ways. While prosecutors have predominantly relied on witness testimony, diverse types of evidence should be presented.¹¹⁸

First, user-generated evidence is a potential remedy for the lack of viable evidence that has plagued the ICC in prior cases.¹¹⁹ The ICC has struggled with a lack of physical or forensic evidence in prosecutions, especially in the case of *Prosecutor v. Lubanga*.¹²⁰ The *Lubanga* case concerned events in Ituri, a resource-rich region of the Democratic Republic of the Congo, where an assortment of militias engaged in intense fighting over natural resources escalated to ethnically-targeted

112. *Prosecutor v. Nahimana* Case No. ICTR 99-52-T, Judgment and Sentence, ¶¶ 5-7 (Dec. 3, 2003), <https://ucr.irmct.org/scasedocs/case/ICTR-99-52#eng>.

113. *Id.* ¶¶ 8-10.

114. Freeman, *supra* note 22, at 301.

115. *Prosecutor v. Nahimana* Case No. ICTR-99-52-T, Amended Indictment (Nov. 15, 1993), ¶¶ 6.6-6.7 <https://ucr.irmct.org/LegalRef/CMSDocStore/Public/English/Judgement/NotIndexable/ICTR-99-52/MS26797R0000541998.PDF>.

116. Freeman, *supra* note 22, at 301.

117. See *infra* notes 148–54 and the accompanying text for a discussion on how a scarcity of witnesses and noncooperation by states can lead to a lack of corroborating evidence in ICC trials.

118. See Freeman, *supra* note 22, at 305 (discussing how presiding judge in *Katanga and Ngudjolo* emphasized that prosecution would benefit from diversifying evidence beyond witness testimonies).

119. See Hamilton, *supra* note 75, at 12 (noting how user-generated evidence is being proactively advanced as part of solution to challenges of evidence collection).

120. See Freeman, *supra* note 22, at 303 (enumerating challenges investigators faced collecting direct evidence of international crimes).

attacks and violence against civilians.¹²¹ Thomas Lubanga founded and served as president of the Union des Patriotes Congolais, one of several militias involved in the conflict, and was charged with the conscription, enlistment, and use of children under the age of fifteen.¹²²

In the *Lubanga* case, VHS recordings¹²³ were used to corroborate witness testimony after it was revealed that a portion of witnesses' testimonies had been tainted by the influence of corrupt intermediaries.¹²⁴ While this evidence was not granted a significant amount of weight, the videos corroborated the witness testimony, which is considered to have been of significant value to the judge's ruling.¹²⁵ As international prosecutions shift from witness testimony as the primary source of evidence, digital evidence has become more prevalent.¹²⁶

The Prosecutor in *Lubanga* primarily relied on testimonial evidence through the interviews of sixty-seven witnesses.¹²⁷ During the trial, it was alleged that some of the witnesses had been encouraged by intermediaries to lie about their ages, and nine testimonies were ultimately found to be unreliable.¹²⁸ These intermediaries had been introduced into the investigative process to combat security threats to ICC staff and potential witnesses in areas of ongoing conflict.¹²⁹ However, the corrupt intermediaries nearly compromised the Prosecution's case.¹³⁰ To combat the lack of credibility of the witnesses, the Prosecution submitted a video of children who were visibly under the age of fifteen and were recruited as troops for the Union des Patriotes Congolais.¹³¹ Lubanga was ultimately found guilty of war crimes.¹³²

The investigative conditions for the *Lubanga* case are relevant to the discussion of user-generated evidence and the need for admitting this evidence at trial.

121. Prosecutor v. Lubanga Dyilo, No. ICC-01/04-01/06, Judgment Pursuant to Article 74 of the Statute of Judge Fulford, ¶¶ 71-85 (Mar. 14, 2012), https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2012_03942.PDF.

122. *Id.* ¶¶ 81, 91.

123. See Chelsea Quilling, *The Future of Digital Evidence Authentication at the International Criminal Court*, J. OF PUB. & INT'L AFFS. (May 20, 2022), <https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court> (explaining experts were able to verify information based on the unique nature of a VHS tape which could not be verified in digital format).

124. Freeman, *supra* note 22, at 302–03.

125. *See id.* at 303 (explaining video footage of underage Lubanga troops alongside expert testimony helped to corroborate parts of witness testimony).

126. *See, e.g., id.* at 335 (summarizing recent cases where defendants' own use of technology led to their prosecutions).

127. *Id.* at 302.

128. *Id.* at 302-03.

129. *See* Hamilton, *supra* note 75, at 14 (explaining that, as locals, intermediaries would attract less attention than investigators from the Hague, and therefore reduce security risks).

130. *See id.* at 15 (highlighting compromised witnesses' testimony did not form basis of Court's ultimate guilty ruling).

131. Freeman, *supra* note 22, at 303; Yvonne Ng, *How to Preserve Open Source Information Effectively*, in DIGITAL WITNESS: USING OPEN SOURCE INFO. FOR HUM. RTS INVESTIGATION, DOCUMENTATION, AND ACCOUNTABILITY 143, 143–44 (Sam Dubberley et al. eds., 2019).

132. Int'l Crim. Ct., *Case Information Sheet: The Prosecutor v. Thomas Lubanga Dyilo*, ICC-01/04-01/06 (July 2021), <https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/LubangaEng.pdf>.

Investigators did not speak to family or community members because they wanted to protect the alleged child soldiers.¹³³ The Court found that this lack of investigation undermined the Prosecution's case.¹³⁴ The video evidence, despite being given minimal probative value under the Article 69 test, provided concrete, specific proof of the defendant's crimes, corroborated the testimonies of the witnesses, and ultimately helped secure a conviction.¹³⁵ In this case, the introduction of open source evidence prevented the loss of legitimacy that may have resulted if Lubanga had been released because of the intermediaries' witness tampering.

Prosecutor v. Katanga and Ngudjolo also demonstrates a shift in ICC prosecution tactics. Defendants Katanga and Ngudjolo were charged with jointly committing, through other persons, the Bogoro massacre in the Democratic Republic of Congo.¹³⁶ Similar to the *Lubanga* case, the Prosecution again had to deal with difficulties of witness credibility due to corrupt intermediaries.¹³⁷ When sole reliance on witness testimony proved insufficient to obtain convictions, the Prosecutor sought admission of a digital 360-degree visual representation of crimes committed and more than 200 photographs which were used to create the representation.¹³⁸ Once again, the Court found that this novel presentation of the evidence had little probative value but admitted it for consideration to help the Court visualize the scene of the alleged crimes.¹³⁹ While the *Ngudjolo* case granted relatively little probative value to the digital evidence presented, the evidence was still used to supplement the convictions.¹⁴⁰

C. User-Generated Content and Future Innovation

Two recent cases—*Prosecutor v. Ahmad Al-Faqi Al-Mahdi* and *Prosecutor v. Mahmoud Mustafa Busyf Al-Werfalli*—illustrate the necessity of innovation and the significant benefits of digital evidence. In these cases, user-generated evidence posted on social media played a role in court proceedings; however, neither case provides clear guidelines to predict the admissibility of future user-generated digital evidence. These cases demonstrate that user-generated digital evidence can preserve witnesses' experiences across long periods of time and provide testimony for victims who are unable to testify. While these cases demonstrate some of the ways in which user-generated evidence can be beneficial to international criminal prosecutions, they also highlight significant gaps in the ICC's knowledge of how to properly use and store digital evidence, particularly user-generated evidence.

The *Ahmad Al-Faqi Al-Mahdi* case is a striking example of social media

133. Freeman, *supra* note 22, at 303.

134. *Id.*

135. *Id.*

136. *Prosecutor v. Germain Katanga*, ICC-01/04-01/07, Judgment Pursuant to Article 74 of the Statute, ¶ 7 (Mar. 7, 2014), https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2015_04025.PDF.

137. Freeman, *supra* note 22, at 304.

138. *Id.*

139. *Id.* at 305.

140. *Id.*

evidence at the ICC. The Office of the Prosecutor used satellite imagery, videos, and geolocation data found on the internet to support its case against Al-Mahdi for destroying cultural property, a war crime.¹⁴¹ These online videos were a combination of video interviews with Al-Mahdi recorded by journalists and user-generated evidence filmed by Timbuktu residents and shared on public websites.¹⁴² The probative value of this evidence was not determined by the Court as Al-Mahdi pled guilty to the crimes, but the video evidence was admitted as part of the guilty plea.¹⁴³

Although the Court did not rule on the probative value of the evidence, the significance of user-generated evidence in this case should not be understated. Similar to the *Ngudjolo* case, prosecutors combined a variety of open source evidence to recreate Al-Mahdi's destruction of the mosques to establish the identity of the perpetrator and the severity of the damage.¹⁴⁴ Recreations made with user-generated and open source evidence, like the ones used in the *Al-Mahdi* case and the *Ngudjolo* case, can preserve a witness or victim's experience as documentary evidence. Visual user-generated evidence allows investigators to show a victim's experience at the moment an event occurred rather than relying on what little evidence may remain years later, as is common in international criminal investigations.¹⁴⁵ The greater the length of time between the commission of a crime and the investigation, the greater likelihood that evidence has been compromised or destroyed.¹⁴⁶ Digital evidence can also provide insight into ongoing atrocities in conflict zones that investigators cannot access without compromising their safety.¹⁴⁷

Additionally, user-generated evidence can preserve the experiences of witnesses who do not survive atrocities, like those in *Prosecutor v. Mahmoud Mustafa Busyf Al-Werfalli*, the most recent ICC case involving user-generated social media evidence. Al-Werfalli was accused of executing over 40 people during the armed conflict in Libya.¹⁴⁸ The ICC heavily relied on open source evidence in issuing warrants for Al-Werfalli's arrest in 2017 and 2018; this evidence included graphic videos of the executions that were posted on Facebook.¹⁴⁹

The *Al-Werfalli* case was poised to finally test the weight of social media evidence in court.¹⁵⁰ However, the proceedings were terminated in June 2022 after

141. Freeman, *supra* note 10, at 52.

142. Freeman, *supra* note 22, at 317.

143. *Id.* at 317; Freeman, *supra* note 10, at 56.

144. Freeman, *supra* note 10, at 56.

145. See Nikita Mehandru & Alexa Koenig, *Open Source Evidence and the International Criminal Court*, HARV. HUM. RTS. J., <https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/> (last visited Dec. 30, 2022) (discussing usual time gap of many years between commission of a crime and ICC's investigation).

146. Hamilton, *supra* note 75, at 14.

147. See Hamilton, *supra* note 92, at 213 (2020) (discussing how open source videos have been key to providing evidence of atrocities committed during Syrian conflict which has been particularly difficult for investigators to access).

148. See Int'l Crim. Ct., *Case Information Sheet: The Prosecutor v. Mahmoud Mustafa Busyf Al-Werfalli*, ICC-01/11-01/17 (June 2022), <https://www.icc-cpi.int/sites/default/files/2022-09/al-werfalliEng.pdf> [hereinafter *Case Information: Al-Werfalli*].

149. Koenig, *supra* note 84, at 41.

150. Hamilton, *supra* note 75, at 8 (noting that evidentiary strength of social media video

the Court reviewed witness statements, photographs, and social media material that established Al-Werfalli's death.¹⁵¹ Consequently, the Court did not rule on the admissibility of user-generated evidence. Since then, due to the increasing prevalence of this evidence, the ICC has proceeded with developing and issuing guidelines to civil society organizations to collect, verify, and preserve this kind of evidence.¹⁵² While the admission of this evidence for issuing warrants and supporting guilty pleas is promising, the evidentiary weight any user-generated evidence would carry still remains unclear.

User-generated evidence can bridge the evidentiary gap which has previously plagued the ICC. In the past, the ICC has struggled to collect corroborating evidence due to the long duration of ICC investigations and trials, which has hampered the Court's ability to identify or locate witnesses and noncooperation by states in investigations. The cases of Al-Faqi Al-Mahdi and Al-Werfalli demonstrate that user-generated evidence can preserve not only the experiences of testifying witnesses but also the experiences of victims who may be unable or unwilling to testify before the Court. No survivors are seen in the videos of Al-Werfalli's violent and systematic murders.¹⁵³ Due to the severity of crimes the ICC addresses, this outcome is not uncommon. Where victims do survive, the lengthy duration of ICC investigations and proceedings can make identifying surviving witnesses increasingly difficult.¹⁵⁴

User-generated evidence, once verified as authentic, can preserve the experience of victims who have been killed, displaced, or are otherwise unable to be located. Additionally, with strong protocols developed for verifying and using this digital evidence, prosecutors do not necessarily have to identify the original uploader of the content, allowing the evidence to speak for itself in highlighting a series of events or facts. Use of this content can save the Court time and resources in undertaking the potentially impossible task of tracking down a specific individual who may have been displaced or killed during the atrocity in question.

Finally, user-generated evidence—and digital evidence more broadly—allows investigators to obtain evidence of atrocities in conflicts where States are uncooperative.¹⁵⁵ The ICC expects to investigate sixteen situations in 2023 and continue preliminary examinations in three other countries.¹⁵⁶ Some of these

footage would not be known until Al-Werfalli's trial commenced).

151. *Case Information: Al-Werfalli*, *supra* note 148.

152. *See* Hamilton, *supra* note 75, at 51-59 (discussing guidelines ICC has explored and proposing others).

153. *See* Prosecutor v. Al-Werfalli, Case No. ICC-01/11-01/17, Warrant of Arrest, ¶¶ 7–22 (Aug. 15, 2017), https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2017_05031.PDF (describing multiple videos of murders committed by Al-Werfalli).

154. *See* Benjamin Gumpert & Yulia Nuzban, *Part I: What Can Be Done About the Length of Proceedings at the ICC?*, EJIL: TALK! (Nov. 15, 2019), <https://www.ejiltalk.org/part-i-what-can-be-done-about-the-length-of-proceedings-at-the-icc/> (discussing various lengths of trials and investigations before the Court).

155. *See* Hamilton, *supra* note 92, at 217 (discussing how digital evidence was instrumental in investigating atrocities against Rohingya population when Myanmar government prohibited investigators from entering country).

156. Int'l Crim. Ct., *Proposed Programme Budget for 2023 of the International Criminal*

investigations are taking place in States which are uncooperative with the efforts of the Prosecutor.¹⁵⁷ Digital evidence—specifically user-generated content—that can be publicly accessed on social media sites offers ICC investigators tools to see what is happening in these countries without being on the ground, and thus strengthens the investigatory abilities of the Office of the Prosecutor.

The history of open source evidence before the ICC and other international tribunals demonstrates that innovation has been a consistent and necessary part of international criminal law, even as a lack of expertise on the Court may constrain the weight assigned to new forms of evidence. As more evidence is captured digitally by ordinary people, user-generated evidence will grow, along with the need for successful storage, verification, and preservation of this evidence for international criminal tribunals. In the past, the ICC has successfully incorporated new technological advances to both safeguard the integrity of the Court's process—as seen in the *Lubanga* and *Ngudjolo* cases where open source evidence was used to combat corruption within the proceedings¹⁵⁸—and help to supplement evidence—as in the *Al-Mahdi* case. However, a failure to continue to innovate and successfully utilize user-generated evidence will affect the ICC's competency to effectively prosecute crimes, thereby jeopardizing the Court's legitimacy.

IV. THE ICC'S LEGITIMACY AND THE NECESSITY OF USER-GENERATED EVIDENCE

The ICC may face a worsening legitimacy issue if it cannot innovate and develop key strategies to utilize user-generated digital evidence. The legitimacy of the ICC has been often discussed since the Court's inception.¹⁵⁹ Scholars have examined legitimacy as it pertains to the ICC and to the legal field more broadly with varying meanings attributed to the concept.¹⁶⁰ For present purposes, legitimacy may be defined as the “justification of authority of the law,”¹⁶¹ relying on two established theories of legitimacy: normative (or procedural) legitimacy and sociological (or substantive) legitimacy.¹⁶² Both views are necessary to assess the ICC and demonstrate the potential impact the mishandling of open source evidence

Court, Doc. ICC-ASP/21/10, ¶¶ 130–35 (Aug. 19, 2022), <https://asp.icc-cpi.int/sites/asp/files/2022-08/ICC-ASP-21-10-ENG.pdf>.

157. See, e.g., Saumya Uma, *State Cooperation and the Challenge to International Criminal Justice*, THE WIRE (Sept. 13, 2021), <https://thewire.in/law/state-cooperation-and-the-challenge-to-international-criminal-justice> (highlighting how President Duterte is non-cooperative with ICC investigators).

158. See Freeman, *supra* note 22, at 302–04 (describing how prosecutors introduced and leveraged open source evidence in the *Lubanga* and *Ngudjolo* cases respectively).

159. See Hitomi Takemura, *Reconsidering the Meaning and Actuality of the Legitimacy of the International Criminal Court*, 4 AMSTERDAM L.F. 3, 4 (2012) (discussing several historical factors which have contributed to an increase in legitimacy scholarship).

160. See, e.g., Margaret M. deGuzman, *Gravity and the Legitimacy of the International Criminal Court*, 32 FORDHAM INT'L L.J. 1400, 1437 (2009) (discussing differing perceptions of legitimacy).

161. Takemura, *supra* note 159, at 5.

162. These theories are also considered to be “two dimensions” of the concept of legitimacy. *Id.*

may have on the legitimacy of the Court.

The ICC's inability to properly utilize user-generated evidence implicates normative and sociological theories of legitimacy. Normative legitimacy is an objective test concerning how laws are justified by authority.¹⁶³ Normative legitimacy is particularly important in international law because of the variety of sources from which a law derives its authority and the overlap between codified laws, such as treaties and "soft" law, such as customary international law.¹⁶⁴ In contrast, sociological legitimacy is a subjective test dependent on a population's perception of an authority or law.¹⁶⁵ An assessment of sociological legitimacy requires identifying the stakeholders of the institution which exercises the authority or law in question.¹⁶⁶

Despite these distinctions, some scholars conflate normative and sociological legitimacy.¹⁶⁷ This conflation underscores that a population's perception of an authority's legitimacy (sociological legitimacy) may be derived or influenced by the normative factors used to justify that authority (normative legitimacy).¹⁶⁸ The opposite is also true where popular perception influences the development of legal norms.¹⁶⁹ In fact, some scholars place popular acceptance as an element of normative legitimacy.¹⁷⁰ However, it is important to delineate normative and sociological legitimacy because stakeholders may perceive an authority to be unsatisfactory (not sociologically legitimate) where normative legitimacy—the procedural aspect through which the authority is derived—is fulfilled.¹⁷¹

To determine normative legitimacy, Thomas Franck enumerated four factors that affect a norm's ability to influence conduct, thereby establishing a pull of compliance by a rule-making institution.¹⁷² Franck's four indicators are determinacy, symbolic validation, coherence, and adherence, which can be used to explain why rules do or do not exert a compliance pull.¹⁷³ Determinacy is defined as

163. *Id.*

164. *Id.* (highlighting thin distinction between hard and soft laws in international law). *But see* Jan Klabbers, *The Undesirability of Soft Law*, 67 *NORDIC J. OF INT'L L.* 381, 385–387 (1998) (arguing that normative usage of soft law as morally binding is undesirable).

165. Takemura, *supra* note 159, at 6.

166. *See id.* (arguing that because sociological legitimacy is based on perceived legitimacy of norms, it's necessary to identify actors creating and wielding those norms).

167. There is also some debate over whether moral legitimacy is incorporated into normative or sociological legitimacy or stands as a separate theory altogether. *Compare* deGuzman, *supra* note 160, at 1437 (criticizing conflation of moral and sociological legitimacy), *with* Takemura, *supra* note 159, at 5 (including morality and sense of justice in definition of sociological legitimacy).

168. deGuzman, *supra* note 160, at 1437.

169. *Id.*

170. Takemura, *supra* note 159, at 6 (citing Daniel Bodansky, *The Legitimacy of International Governance: A Coming Challenge for International Environmental Law?*, 93 *AM. J. INT'L L.* 596, 601 (1999)).

171. *Id.*

172. *Id.* at 7; THOMAS M. FRANCK, *THE POWER OF LEGITIMACY AMONG NATIONS* 38 (Oxford University Press ed., 1990).

173. Takemura, *supra* note 159, at 7; *see generally* Thomas Franck, *Legitimacy in the*

the “ability of . . . text to convey a clear message,” and symbolic validation is the ability of a rule to convey authority, serve to legitimize rules. The two other terms—coherence and adherence—situate rules within larger systems. Coherence assesses the consistency with which a rule is applied across similar situations and adherence refers to the relationship between a single primary rule and a “pyramid of secondary rules” dictating how “rules are made, interpreted, or applied.”¹⁷⁴ While these factors predominantly relate to procedural or legal legitimacy, Franck also emphasized the importance of sociological legitimacy and described it as stakeholders’ perception that an institution operates according to “generally accepted principles of right process.”¹⁷⁵ This emphasis on sociological legitimacy is particularly important when discussing the ICC because international law differs from domestic law in that state compliance is motivated by conformist behavior.¹⁷⁶

While the legality of norms relating to the ICC’s activities is important in shaping aspects of procedural legitimacy, sociological legitimacy is determined by the perceptions of stakeholders, particularly State Parties to the Rome Statute.¹⁷⁷ Both procedural and sociological legitimacy can be affected by the Court’s ability to innovate and maintain relevance in prosecuting the gravest of crimes; a loss of legitimacy of the Court could lead to a loss of faith and thereby reduced funding and support by State Parties to the Rome Statute.¹⁷⁸ As noted by David Luban, the procedural legitimacy of a tribunal is determined by the “quality of justice” delivered.¹⁷⁹ Because international tribunals must “earn” their legitimacy, rather than inherit it as states do, their legitimacy is particularly dependent on their fairness.¹⁸⁰ International tribunals, in order to remain legitimate, must maintain basic procedural rights, including the right to a fair and speedy trial, the right to counsel, and others.¹⁸¹

Open source evidence can be used to bolster the ICC’s legitimacy through these procedural rights. In the *Lubanga* case, video evidence was relied on to corroborate witness testimony where witnesses had been coerced to lie by corrupt intermediaries

International System, 82 AM. J. INT’L L. 705 (1988).

174. Franck, *supra* note 173, at 750, 752.

175. FRANCK, *supra* note 172, at 19.

176. *Id.* at 38.

177. Takemura, *supra* note 159, at 7. Other stakeholders include victims of atrocities, academics, legal counsel, and NGOs. AMNESTY INT’L & T.M.C. ASSER INSTITUUT, THE ROME STATUTE AT 40, at 13 (2021).

178. See *Statement of ICC Prosecutor, Karim A.A. Khan QC: Contributions and Support from States Parties will Accelerate Action Across Our Investigations*, INT’L CRIM. CT. (Mar. 28, 2022) [hereinafter *Statement on State Parties Support*] <https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-qc-contributions-and-support-states-parties-will> (detailing how financial contributions by State Parties will advance ICC’s use of technology in collection, analysis, and processing of evidence).

179. David Luban, *Fairness to Rightness: Jurisdiction, Legality, and the Legitimacy of the International Criminal Law in THE PHIL. INT’L L.* 569, 579 (Samantha Besson & John Tasioulas eds., 2010).

180. See *id.* at 579–80 (discussing view that legitimacy of international tribunals comes from their manifested fairness).

181. *Id.* at 580.

who had been introduced into the judicial process by the ICC.¹⁸² If the prosecution's case had been dismissed due to the improper acts of the intermediaries who were working on behalf of the ICC,¹⁸³ the Court would have suffered a blow to its normative and sociological legitimacy.¹⁸⁴ If the intermediaries' witness tampering would have acquitted Lubanga, then the perception of the Court's ability to bring perpetrators to justice would be severed.¹⁸⁵

Similarly, the ICC's hesitation to utilize digital evidence negatively impacts the normative legitimacy of the Court. The Office of the Prosecutor lacks the investigatory capacity to provide sufficient evidence to secure successful convictions.¹⁸⁶ Members of the ICC judiciary have criticized this shortcoming.¹⁸⁷ The ICC's normative legitimacy is undermined by prosecutors' lack of sufficient evidence, particularly when the Office of the Prosecutor is unable to meet even the lowest burden required to confirm proceedings.¹⁸⁸ This evidentiary threshold is particularly important for the ICC to address the gravest crimes over which the Court has jurisdiction like genocide, crimes against humanity, and war crimes.

In addition to concerns over investigative techniques' capacity to produce a significant body of evidence,¹⁸⁹ the Court's legitimacy is implicated by the ICC's inadequate means to verify, store, and preserve digital evidence. This lack of technological capacity may lead to evidence being mishandled or rendered ineffective.¹⁹⁰ In its inability to handle digital evidence, the ICC compromises a fair and just proceeding and deprives victims of atrocities of the benefits that digital evidence can provide to a prosecution.¹⁹¹ Importantly, if the Court is unable to develop proper protocols and systems for dealing with digital evidence, the

182. Hamilton, *supra* note 75, at 14.

183. *See id.* (explaining how prosecution should not have delegated *Lubanga* to intermediaries).

184. *See* Sara Anoushirvani, *The Future of the International Criminal Court: The Long Road to Legitimacy Begins with the Trial of Thomas Lubanga Dyilo*, 22 PACE INT'L L. REV. 213, 216 (2010) (stating *Lubanga* will have legitimacy implications for ICC).

185. *Id.*

186. Jeremy Pizzi, *The ICC's Investigation Problem and Safeguarding Justice for the Rohingya*, PKI GLOB. JUST. J. QUEEN'S L. (Oct. 31, 2019), <https://globaljustice.queenslaw.ca/news/the-iccs-investigation-problem-and-safeguarding-justice-for-the-rohingya> (discussing criticisms that both Prosecutor Ocampo and Bensouda brought cases with insufficient evidence).

187. *Id.*

188. *E.g.*, Hamilton, *supra* note 75, at 12 (discussing Office of the Prosecutor's struggle to develop successful approach to investigations); Prosecutor v. Ngudjolo, No. ICC-01/04-02/12-3-tENG, Judgment Pursuant to Article 74 of the Statute of Judge Cotte, ¶¶ 115-123 (Dec. 26, 2012), https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2013_02993.PDF (highlighting areas of investigative failure on part of Office of Prosecutor which contributed to decision to acquit Ngudjolo of war crimes, including the willful killing of civilians); Pizzi, *supra* note 186.

189. *E.g.*, Pizzi, *supra* note 186 (discussing how lack of investigatory personnel has contributed to failures to collect witness testimonies sufficient to secure convictions).

190. *See* Quilling, *supra* note 123 (explaining that ICC is underprepared to meet challenges surrounding authenticating digital evidence).

191. *Id.*

sociological legitimacy of the Court will be undermined.¹⁹² Negative perceptions from stakeholders, such as State Parties to the Rome Statute, can lead to decreased funding for the Court.¹⁹³

As shown by the Nuremberg Trial and the history of cases before international tribunals, open source evidence from defendants themselves is often incredibly effective in prosecutions.¹⁹⁴ As more content is uploaded exclusively online, the ICC will have no choice but to develop procedures for assessing user-generated content to escape the evidentiary problems of the past.¹⁹⁵ In fact, the ICC itself has acknowledged the necessity for technological advancement,¹⁹⁶ seeking to provide more clarity in the guidelines for collecting digital evidence.¹⁹⁷

Digital evidence is widely available to the public—particularly in a situation like the Russia-Ukraine war where the public's awareness of the situation is quite high.¹⁹⁸ The ICC must be able to act with a fair process and with as much evidence as can be collected.¹⁹⁹ While the sociological legitimacy of the ICC has not been discussed in as much detail as the normative legitimacy, these two concepts affect one another.²⁰⁰ For example, the African Union's negative opinion of the ICC and vocal resistance caused several States in the Union to engage in noncooperation with the Court, thus undermining the Court's process.²⁰¹

Additionally, the inability of the ICC to deal with digital evidence undermines the universality of the Court because it severely limits the ability of the Court to operate outside of Africa and Southeast Asia. In the past, the ICC has been criticized for biased investigations, particularly targeting African States.²⁰² This divide will only grow if the ICC is incapable of prosecuting cases that require advanced technological tools and experts, because these kinds of crimes will occur typically in developed nations where internet connectivity and smartphones are abundant.²⁰³

192. *See id.* (outlining policy recommendations which would improve Court's legitimacy and authority with respect to digital evidence authentication and verification).

193. *See* Janet Sankale, *Larger Budget Reflects Increased ICC Workload in 2023*, JOURNALISTS FOR JUST. (Dec. 15, 2022), <https://jfjustice.net/larger-budget-reflects-increased-icc-workload-in-2023>.

194. *See supra* Part III for a discussion on the history of open source evidence before the ICC.

195. *See generally* Hamilton, *supra* note 75 (explaining how increased access to cameras will allow user-generated evidence to become prevalent in court).

196. *See Statement on State Parties Support, supra* note 178 (explaining that funds received from states parties will be used to acquire new technological tools and equipment in processing evidence).

197. *See, e.g.*, GUIDELINES FOR CIVIL SOCIETY ORGANIZATIONS, *supra* note 67 (offering guidance to civil society organizations on how to preserve evidence of crimes with emphasis on collection of digital evidence).

198. *See* Farmer, *supra* note 9 (explaining how Ukrainian war has been captured and observed by the world on social media).

199. *See* UNDERSTANDING THE ICC, *supra* note 27 (explaining evidence collection and preserving rights of people).

200. Takemura, *supra* note 159, at 9–10.

201. *See id.* at 10 (describing African Union's negative perception of ICC).

202. Hamilton, *supra* note 75, at 20–21.

203. Jacob Poushter et al., *Social Media Use Continues to Rise in Developing Countries but*

V. THE COMPLICATIONS OF USER-GENERATED DIGITAL EVIDENCE

An analysis of user-generated digital evidence would be incomplete without discussing several unique complications inherent to the digital nature of this evidence. Some complications are more prevalent with digital sources than physical ones, like the potential for manipulation or fabrication.²⁰⁴ The ICC's lack of effective protocols, resources, and guidance on the handling of digital evidence exacerbates these potential pitfalls.²⁰⁵ Technical and legal limitations arising from the complications of digital evidence can generally be mitigated through technological advances, as seen with "deepfakes."²⁰⁶ Where a technical solution exists and can remedy the drawbacks of digital evidence, the ICC's legitimacy is undermined when it is unable to implement the solution, particularly when average citizens have been viewing this evidence both through media coverage and from their smartphones.²⁰⁷

A. Difficulties in Collecting and Storing User-Generated Evidence

The process of collecting digital evidence, like other forms of evidence, remains a lengthy one. However, unlike more traditional forms of evidence, guidance on collecting, storing, and preserving user-generated content has only recently emerged.²⁰⁸ Complications arise at each stage of obtaining evidence, predominantly because (i) the ICC has failed to adequately advance its technology; (ii) judicial actors remain largely uneducated on the technology; and (iii) domestic legal regimes may deter, or even prohibit, the transfer of this new type of evidence to international courts such as the ICC.

Since the rise of social media, these platforms have recognized the necessity of regulating user-uploaded content to avoid potentially harmful content from being seen and distributed across platforms.²⁰⁹ While platforms initially employed human content moderators, today most predominantly moderate using algorithms, which can be completed by artificial intelligence (AI) without human oversight.²¹⁰ One of the greatest barriers deterring the use of user-generated evidence arises when atrocity evidence uploaded to a social media platform is removed and archived in private

Plateaus Across Developed Ones, PEW RSCH. CTR. (June 19, 2018), <https://www.pewresearch.org/global/2018/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones>.

204. GUIDELINES FOR CIVIL SOCIETY ORGANIZATIONS, *supra* note 67, at 33.

205. Quilling, *supra* note 123.

206. See Alexa Koenig, "Half the Truth Is Often a Great Lie": Deep Fakes, Open Source Information, and International Criminal Law, 113 AM. J. OF INT'L L. UNBOUND 250, 252 (2019) (describing efforts to harness potentially malevolent technologies in order to strengthen accountability).

207. Tim Bjarin, *Russian-Ukraine War . . . The Most Broadcast War in History that Includes Physical and Cyber Warfare*, FORBES (Mar. 2, 2022, 10:00 AM), <https://www.forbes.com/sites/timbjarin/2022/03/02/ukraine-russian-warthe-most-broadcast-war-in-history/?sh=53d1edbe5b3b>.

208. See BERKELEY PROTOCOL, *supra* note 26 (noting Berkeley Protocol was developed and published in 2022).

209. Hillary Hubley, *Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations*, INT'L CRIM. L. REV. 989, 993–94 (2022).

210. *Id.* at 995.

social media servers.²¹¹ When user-generated evidence is no longer publicly available on a social media platform, retrieval of this evidence is nearly impossible when that content is stored in the United States.²¹² As a result of *Republic of Gambia v. Facebook, Inc.*, companies do not have to comply with orders to disclose deleted evidence from their platforms.²¹³

Because of this recent decision and the frequency at which videos and photos are removed from platforms,²¹⁴ innovative solutions have allowed for the collection of user-generated evidence by avoiding content moderation of social media platforms.²¹⁵ Several different applications (apps) have been created to verify and store this media.²¹⁶ One of these early apps, CameraV, was developed to collect evidence in high-risk settings.²¹⁷ Although not specifically designed with international criminal tribunals in mind, CameraV collects a large amount of metadata with the goal of “authenticat[ing] what users document.”²¹⁸ CameraV is the predecessor to an app called eyeWitness to Atrocities which is specifically designed to capture atrocity evidence for use as evidence.²¹⁹

The eyeWitness to Atrocities app has featured prominently in the Russia-Ukraine war.²²⁰ The app was created by an organization of the same name, originally formed by the International Bar Association, and aims to preserve the evidentiary value of open source evidence.²²¹ The app, through a mobile camera, allows users to capture photos and videos of atrocities in real time.²²² When media is captured

211. See Belkis Wille, “Video Unavailable:” *Social Media Platforms Remove Evidence of War Crimes*, HUM. RTS. WATCH (Sept. 10, 2020), <https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes> (discussing how social media sites’ removal of content often hampers investigations of serious crimes).

212. See *Republic of Gambia v. Facebook, Inc.*, 575 F. Supp. 3d 8, 16 (D.D.C. 2021) (holding that Stored Communication Act prohibits sharing of user-generated content stored in social media archives with a foreign government). Further implications of this decision are outside the scope of this Comment, but it is important to highlight this decision as it relates to the development of alternative apps to collect digital evidence of atrocities.

213. *Id.*

214. See Hubley, *supra* note 209, at 997 (noting YouTube removed 6 million videos and Facebook removed 50 million pieces of content between January and March 2020).

215. See, e.g., Barrie Sander, *Innovating Justice: The Mobile Apps Aiming to Transform How We Respond to Situations of Mass Atrocity*, JUST. IN CONFLICT (June 23, 2015), <https://justiceinconflict.org/2015/06/23/innovating-justice-the-mobile-apps-aiming-to-transform-how-we-respond-to-situations-of-mass-atrocity> (highlighting several different humanitarian apps which enhance documentation of atrocities).

216. *Id.*; Stephanie van den Berg, *Mass Atrocities? There’s an App for That*, JUSTICEINFO.NET (Feb. 5, 2019), <https://www.justiceinfo.net/en/40176-mass-atrocities-there-s-an-app-for-that.html>.

217. Hamilton, *supra* note 75, at 18.

218. *Id.* at 19.

219. *Id.* at 17-18.

220. See *eyeWitness to Atrocities App*, *supra* note 93 (noting that users of the app have deposited over 20,000 verifiable videos, photographs, and audio files of alleged war crimes into a secure digital vault since the start of the invasion).

221. *About Us*, EYEWITNESS GLOB., <https://www.eyewitness.global/about-us> (last visited Nov. 19, 2023).

222. *Our Work*, EYEWITNESS GLOB., <https://www.eyewitness.global/our-work> (last visited Nov. 19, 2023).

through the app, the footage is embedded with metadata, verifying the time and location of where it was recorded, as well as whether the footage has been altered.²²³ The app stores all collected footage in an encrypted folder and creates a chain of custody which allows subsequent holders of the footage to verify its past ownership and ensure that it has not been altered.²²⁴ Finally, the app prioritizes the preservation of user-generated footage for legal accountability, ensuring that footage uploaded to the app is reviewed and catalogued by lawyers to meet the requirements of investigators.²²⁵ In the case of Ukraine, the app's users have deposited 20,000 verifiable videos, with some of this evidence having already been submitted to Ukrainian prosecutors and the ICC.²²⁶

The Ukrainian government has also collected digital evidence of atrocities through several different services.²²⁷ One example of these services is a chatbot called e-Enemy which allows Ukrainians to submit footage of war crimes and report the movement of Russian troops.²²⁸ As of April 2022, more than 253,000 people reported and captured footage of Russian movements and 66,000 submitted evidence of damaged homes.²²⁹ All the footage is shared with the Ukrainian military and stored in a centralized database maintained by the Ukrainian Office of the Prosecutor General.²³⁰ The Prosecutor General of Ukraine has also set up a website which has received over 10,000 submissions from citizens documenting atrocities.²³¹ The website allows users to upload evidence or submit links to social media sites under a variety of categories including torture, death, and sexual violence.²³² In addition to the government's efforts, other countries, the U.N. Human Rights Council, other non-governmental entities, human rights analysts, and more are conducting investigations into potential violations.²³³ Most Ukrainian groups are now adhering to recently developed guidelines pertaining to digital content in hopes that the evidence they collect will be admitted by judges in future cases before the ICC.²³⁴

223. *Id.*

224. *Id.*; Pauline Pfaff, *ASP20 Side Event: Using Digital Technology for War Crimes Documentation and Accountability*, PUB. INT'L L. AND POL'Y GRP. (Dec. 14, 2021), <https://www.publicinternationallawandpolicygroup.org/lawyering-justice-blog/2021/12/14/asp20-side-event-using-digital-technology-for-war-crimes-documentation-and-accountability>.

225. *Our Work*, *supra* note 222.

226. *eyeWitness to Atrocities App*, *supra* note 93; Pfaff, *supra* note 224.

227. Bergengruen, *supra* note 95.

228. *Id.*

229. *Id.*

230. *Id.*

231. *If You Became a Victim or Witness of Russia's War Crimes, Record and Send the Evidence!*, OFF. OF THE PROSECUTOR GEN., <https://warcrimes.gov.ua> (last visited Jan. 24, 2023); Bergengruen, *supra* note 95.

232. OFF. OF THE PROSECUTOR GEN., *supra* note 231.

233. See Stephanie van den Berg & Anthony Deutsch, *Explainer: How Are War Crimes in Ukraine Being Investigated?*, REUTERS (Mar. 17, 2023, 1:37 PM), <https://www.reuters.com/world/europe/how-are-war-crimes-ukraine-being-investigated-2023-02-23> (listing countries and other agencies inquiring into potential violations).

234. BERKELEY PROTOCOL, *supra* note 26, at v; Bergengruen, *supra* note 95.

B. Securing Digital Evidence During Storage

Once collected, digital evidence requires a system which can safely store and maintain the evidence.²³⁵ The ICC currently operates with an outdated mode of storage that is susceptible to malware.²³⁶ This system creates significant concerns about the safety of digital evidence stored at the ICC.²³⁷ The problem arises from the algorithm used as part of the ICC's verification process.²³⁸ The ICC's "e-Court Protocol" requires that all digital files are assigned a digital signature to verify the authenticity of the evidence.²³⁹ The algorithm which is used to verify these digital signatures is called MD5.²⁴⁰ This algorithm has been exposed by the Internet Engineering Task Force as being vulnerable to a sophisticated form of malware called Flame.²⁴¹

When the subjects of ICC investigations involve countries with the capacity to orchestrate cybersecurity attacks, like Russia, the security of any digital evidence at the ICC may be compromised due to the vulnerability of the MD5 hashing system.²⁴² The use of the outdated MD5 hashing system undermines the normative legitimacy of the Court because the evidence storage process is no longer secure.²⁴³ Additionally, the vulnerability of the system makes it increasingly difficult for the prosecution to guarantee the authenticity of digital evidence stored by the Court.²⁴⁴ If defendants challenge the authenticity of digital evidence on the basis of the system's vulnerability, digital evidence that has been correctly collected and preserved by the prosecution and other third-party actors may be dismissed because the evidence will not be able to be authenticated.²⁴⁵

Finally, a breach of the ICC's current storage system could result in a loss of both procedural and sociological legitimacy. The unauthorized sharing or discovery of confidential information can jeopardize an ongoing investigation or trial by providing bad actors with their personal information.²⁴⁶ This can also endanger witnesses, investigators, and victims.²⁴⁷ A data breach, depending on how significant, could violate the ICC's promise of a fair and expeditious trial,²⁴⁸ thereby

235. BERKELEY PROTOCOL, *supra* note 26, at 60–62.

236. Quilling, *supra* note 123.

237. *See id.* (describing ICC's data storage security system as insecure).

238. *See id.* (noting how ICC digital filing system's susceptibility to Flame malware reveals outdated state of system).

239. *Id.*

240. *Id.*

241. SEAN TURNER & LILY CHEN, UPDATED SECURITY CONSIDERATIONS FOR M5 MESSAGE-DIGEST AND THE HMAC-MD5 ALGORITHMS (2011), <https://datatracker.ietf.org/doc/html/rfc6151>; Quilling, *supra* note 123.

242. *Disinformation and Russia's War of Aggression Against Ukraine*, *supra* note 15; Quilling, *supra* note 123.

243. Quilling, *supra* note 123.

244. *See id.* (describing potential consequences of security breach for ICC).

245. *Id.*

246. *Id.*

247. *Id.*

248. *Id.*

undermining the procedural legitimacy of the Court.

C. Verification of Digital Evidence and Deepfakes

While user-generated content is not inherently less reliable than other forms of open source evidence used in ICC cases, the verification of this content differs from that of physical sources.²⁴⁹ One difficulty of verification is that digital sources increasingly exist exclusively in digital form with no original physical source against which to verify the evidence provided.²⁵⁰ For example, in *Prosecutor v. Lubanga*, the video depicting child soldiers was originally taken from a VHS tape.²⁵¹ Because a physical version of the VHS tape existed, the video was able to be verified without using advanced digital techniques.²⁵² This is no longer the standard and most digital evidence is “born-digital.”²⁵³ Born-digital refers to items that are created in digital form.²⁵⁴ Unlike the *Lubanga* video which was originally recorded on a physical VHS tape and could later be digitized for storage,²⁵⁵ videos filmed on a civilian’s cell phone exist exclusively in a digital format, meaning there is no physical original.²⁵⁶ While in the *Lubanga* case, the original VHS was used to confirm the authenticity of the video itself,²⁵⁷ items that are born-digital must be confirmed through different means because there are no physical originals with which to compare digital evidence.²⁵⁸ Thankfully, tools for digital means of verification have continued to advance and are widely available to flag the manipulation or fabrication of digital evidence.²⁵⁹

Verification is vital when addressing another growing concern: deepfakes.²⁶⁰ Deepfakes are created by pitting two neural networks against each other to generate increasingly realistic fakes, the product of which makes it seem as though a false event actually occurred.²⁶¹ One of the most famous examples of a deepfake is a viral

249. *Id.*

250. *Id.*

251. *Id.*

252. *Id.*

253. *Id.*

254. Ricky Erway, *Defining “Born Digital”*, ONLINE COMPUTER LIBRARY CENTER, Nov. 2010 at 1, <https://www.oclc.org/content/dam/research/activities/hiddencollections/borndigital.pdf>.

255. Quilling, *supra* note 123.

256. See *What Does “Born Digital” Mean?*, PRIMARY SOURCES AT YALE, <https://primarysources.yale.edu/what-does-born-digital-mean> (last visited Nov. 19, 2023) (defining born-digital items).

257. Quilling, *supra* note 123.

258. *Id.*

259. See Joshua Rothman, *In the Age of A.I., Is Seeing Still Believing?*, THE NEW YORKER (Nov. 5, 2018), <https://www.newyorker.com/magazine/2018/11/12/in-the-age-of-ai-is-seeing-still-believing> (discussing how verification tools, including analysis of geolocation data, cell tower information, barometric-pressure sensor data, and computer-vision tests, are used to authenticate digital evidence by storing approved images on Bitcoin and Ethereum blockchains, facilitating easy sharing through a dedicated webpage to confirm their authenticity).

260. See Hamilton, *supra* note 92, at 218 (discussing deepfakes as barrier to authenticating digital evidence).

261. See Koenig, *supra* note 206, at 252.

video which seemingly depicts Morgan Freeman delivering a haunting speech welcoming viewers to the era of “synthetic reality.”²⁶² There are some nearly imperceptible glitches in the movement of the AI-generated Freeman’s face, but this deepfake is widely recognized as one of the most sophisticated, sparking fears amongst online viewers about the damage this kind of technology could do.²⁶³ While the Freeman deepfake does not try to fool its viewers and is titled *This is not Morgan Freeman*,²⁶⁴ other deepfakes are not so up front about their veracity or lack thereof.

People have already created deepfakes to push false narratives about the Russia-Ukraine war.²⁶⁵ One deepfake depicts Zelensky instructing Ukrainians to surrender to Russia, while another shows Putin declaring peace with Ukraine.²⁶⁶ Both videos are low resolution, leading to them being quickly called out as fakes.²⁶⁷ However, experts still express concerns about the damage these deep fakes can cause due to their rapid spread of disinformation online.²⁶⁸ In a world grappling with the rise of the troubling “fake-news phenomena,” deepfakes could play a key role in the spread of disinformation and may even incite violence.²⁶⁹ However, educating relevant actors and leveraging technology-based solutions can mitigate the potential dangers of deepfakes in international criminal tribunals.²⁷⁰ While the ability to create deepfakes and fabricated digital images has advanced, a wide range of private actors has already developed verification protocols.²⁷¹

For example, InVID, Project Maru, and Project Angora are three different programs that can determine the veracity of a digital image or video using simple, already-available technology to spot fakes.²⁷² The ICC can adopt these protocols to assist in verification. While creators of deepfakes will continue to innovate to circumvent detection, verification technologies and careful observation are currently sufficient to detect most, if not all, fakes.²⁷³ Additionally, while deepfakes are a novel development supported by technological developments, falsified evidence

262. Diep Nep, *This Is Not Morgan Freeman – A Deepfake Singularity*, YOUTUBE (July 7, 2021), <https://www.youtube.com/watch?v=oxXpB9pSETo>.

263. Ciarán Daly, ‘Most Realistic Deepfake’ Ever Terrifies Viewers Who Wonder ‘Is Morgan Freeman Real’, DAILY STAR (Dec. 20, 2022, 4:23 PM), <https://www.dailystar.co.uk/tech/news/most-realistic-deepfake-ever-terrifies-28780484>.

264. Diep Nep, *supra* note 262.

265. Rachel Metz, *Deepfakes Are Now Trying to Change the Course of War*, CNN BUSINESS (Mar. 25, 2022, 11:39 AM), <https://edition.cnn.com/2022/03/25/tech/deepfakes-disinformation-war/index.html>.

266. *Id.*

267. *Id.*

268. *Id.*

269. Hany Farid, *Digital Forensics in a Post-Truth Age*, 289 FORENSIC SCI. INT’L 268, 268 (2018), <https://farid.berkeley.edu/downloads/publications/fsi18.pdf>.

270. Koenig, *supra* note 206, at 254.

271. *See id.* (calling on scientific community to take aggressive action to develop more efficient methods to authenticate digital content and combat proliferation of fake media).

272. *Id.*

273. *Id.* at 255 (noting that danger of being fooled by fakes is mainly confined to journalists who must verify videos within minutes).

itself is not an unknown issue for courts.²⁷⁴ Combatting deepfakes requires sufficient allocation of resources to train justice-sector actors and invest in technology that can detect manipulation of digital evidence. Education of judicial actors should also cover a wide range of topics, including relevant guidance drafted by nongovernmental organizations that discuss collecting, storing, and preserving digital evidence.

While complications do arise from the use of user-generated digital evidence, the ICC can mitigate many of these difficulties through clear guidance and standardization, adequate education of judicial actors, and security assessments of its current systems. By taking these steps now, the Court can best position itself to deal with future cases, like atrocities arising from the Russia-Ukraine war, involving large amounts of user-generated digital evidence.

VI. RECOMMENDATIONS FOR THE ICC'S PROCESS

As a leader in international criminal prosecutions, the ICC can address the challenges posed by digital evidence by strengthening the current standards administered by the Court.²⁷⁵ The ICC currently has the Trust Fund for Advanced Technology and Specialized Capacity (“the Fund”) which implements a two-prong plan of action.²⁷⁶ First, contributions to the Fund establish technological infrastructure to assist the Court in utilizing digital evidence.²⁷⁷ Additionally, national experts provide expertise and serve as advisors to the Office of the Prosecutor in specified areas of their work.²⁷⁸ These positions are filled by experts from a variety of State Parties who have volunteered to assist the Prosecutor.²⁷⁹ The Fund is certainly a step in the right direction for the ICC and should seek to address current shortcomings of the Court in handling digital evidence.

Using contributions to the Fund, the ICC should do three things to address user-generated digital evidence and secure its greater legitimacy in the process. First, it must ensure the standardization of protocols for handling digital evidence. Due to its limited resources,²⁸⁰ the ICC often relies on third-party actors. Clear guidance must be delineated to advise any third-party actors in this space. Second, in addition to collaborating with national experts as laid out in the Fund’s plan, the ICC should educate current judicial actors, including judges, to provide them with a baseline understanding of the complexities of digital evidence. Third, and finally, the ICC must update its current digital storage system, which has been proven to be insecure.

274. Quilling, *supra* note 123.

275. Mehandru & Koenig, *supra* note 145.

276. *Statement on State Parties Support*, *supra* note 178.

277. *Id.*

278. *Id.*

279. *See id.* (noting that Bulgaria, Canada, Denmark, Estonia, Finland, France, Germany, Latvia, Lithuania, New Zealand, Poland, Sweden, Netherlands, and United Kingdom expressed intention to make national experts available to Prosecutor).

280. *See* Quilling, *supra* note 123, at 10 (describing ICC as a “tightly resourced” organization).

A. Standardizing Protocols for Collection of Digital Evidence

One significant development in the use of digital evidence for international criminal prosecutions is the release of the Berkeley Protocol on Digital Open Source Investigations (the Berkeley Protocol).²⁸¹ Released by the Human Rights Center at the University of California Berkeley School of Law and the Office of the United Nations High Commissioner for Human Rights (OHCHR), the Berkeley Protocol provides international standards for conducting online research and for gathering, verifying, and storing digital evidence.²⁸² This protocol, designed specifically with international criminal and human rights investigations in mind, is informative to actors within the ICC system.²⁸³ The Berkeley Protocol defines technical terminology, details specific technological requirements for successful investigations, and outlines the procedural process for online investigations.²⁸⁴ The Protocol intertwines legal considerations, like the chain of custody, verification, and credibility, with discussions of certain risks, such as the necessity of storage backups and the challenge of degradation of evidence.²⁸⁵ While the Protocol provides more general advice for a variety of actors and not just those collecting evidence for criminal trials,²⁸⁶ the ICC can use the Protocol to develop training programs and guidelines for investigative actors who are specifically focused on criminal accountability.

The Berkeley Protocol is a valuable tool for the ICC and other actors, such as civil society organizations, which rely on it to assist with open source investigations.²⁸⁷ The scale of these investigations has grown as the amount of digital content available to investigators has increased, requiring collaboration by a variety of actors.²⁸⁸ However, many of these new actors who are conducting investigations, including activists, journalists, and members of civil society, are not educated in legal evidentiary standards.²⁸⁹ This can lead to mismanagement of important evidence and inadmissibility of evidence in court.²⁹⁰ For this reason, the Court must take steps to educate actors conducting investigations about relevant legal standards. The Fund could fill this gap by creating an advisory panel that uses the Berkeley Protocol to offer clear guidance to civil society organizations and governments on the best techniques for collecting digital evidence.

Second, the ICC should ensure that it also has the capacity to conduct digital investigations without needing to rely on third parties. While civil societies can fill in gaps where the ICC does not have the resources or the grant of jurisdiction to

281. BERKELEY PROTOCOL, *supra* note 26, at v.

282. *Id.*

283. *Id.* at 4.

284. *See generally id.*

285. *Id.*

286. *Id.*

287. Quilling, *supra* note 123, at 8.

288. *See id.* (arguing that ICC should evaluate open source information with caution and account for the actors involved, new technologies, and possibility of manipulation).

289. *Id.*

290. *See id.* (noting possibilities for forgeries and digital evidence manipulation).

investigate,²⁹¹ the ICC should also be prepared to assist and understand how to handle digital evidence. Knowing that digital evidence will only become more common, the ICC should create an investigative team that can partner with civil society organizations and assist in accessing, verifying, and storing digital evidence. This investigative team can gain knowledge about investigating and collecting evidence and assist in standardizing the process of collecting digital evidence, particularly user-generated evidence, which is at risk of being removed due to websites' content moderation and, as such, is important to capture in a timely manner. This investigative team should understand the basic technology needed to conduct investigations and advise NGOs and other actors on proper digital investigation standards, ensuring that digital evidence is collected correctly.²⁹²

B. Education of Judges and Prosecutors

Once evidence is collected according to international standards for use in prosecutions, judicial actors must also have the tools to properly rule on this evidence in court. The novelty of digital evidence is a concern in this regard. Judges and prosecutors may be unfamiliar with the complex technological nature of the evidence, resulting in them neglecting or assigning low probative value to this evidence.²⁹³ As user-generated digital evidence has already played a role in several recent cases, the ICC must ensure that judicial actors are educated on the benefits and complications of this kind of evidence. Digital evidence can remedy issues arising from an overreliance on witness testimony, which has plagued previous international criminal cases.²⁹⁴

The ICC should educate judges and prosecutors on the intricacies of digital evidence. While expert witnesses can provide insight for judges who decide the admissibility and weight of digital evidence, judges must have general background knowledge of how digital evidence is collected, verified, and stored to make informed decisions. The education of judges and other judicial actors would promote more standardization and increase the predictability of the evidentiary value of digital evidence.²⁹⁵ Because judges have great discretion in ruling on the admissibility of evidence, the proper function of judges is crucial to the ICC's legitimacy.

As the ICC grapples with digital evidence and the rapid development of new technologies, continued judicial education is required to ensure judges know how to properly assess this data. Scholars have recommended that judges should at least be familiar with "data security, metadata, data storage, digital forensics," and

291. See Hamilton, *supra* note 75, at 5 (noting that international criminal law typically has relied on third-party organizations to provide investigation assistance).

292. *Id.*

293. See *id.* at 45 (describing issue of how judges will interpret or weigh user-generated evidence).

294. See *supra* Part III.B for a discussion on the *Lubanga* and *Ngudjolo* cases.

295. See Pfaff, *supra* note 224, at 5 (noting that specialized training for judges and other actors has added benefit).

authentication methods for digital evidence.²⁹⁶ This education can be provided under the ICC's requirement of continued judicial education²⁹⁷ and is incredibly important to ensure that the ICC can continue to innovate and administer justice.

As previously established, ICC investigations and trials often commence years after the initial incident.²⁹⁸ Commencing training for judges before any trials related to atrocities committed during the Russia-Ukraine war could provide the first opportunity for judges educated about digital evidence to rule on the weight of this evidence.

C. Security Assessment of the ICC's Databases

Efforts to maintain the ICC as a legitimate international body must address the insecurity in the current MD5 hashing system. The ability to store and utilize evidence furthers the procedural legitimacy of the Court. While all digital storage systems are theoretically susceptible to cyberattacks, the ICC cannot be a mechanism for justice where its storage systems are known to be outdated and highly vulnerable to attacks.²⁹⁹ The ICC must adopt a storage system that is secure and flexible enough to be updated when subsequent technological advances are made.³⁰⁰ While carrying out the first prong of the Fund's plan, the ICC should consult with international standards bodies on the best practices for digital storage systems, including the determination of which other organizations are using secure algorithms.³⁰¹ Candidates for consultation include the International Organization for Standards, the Institute for Electrical and Electronics Engineers, and the Internet Engineering Task Force.³⁰² Specifically, the Internet Engineering Task Force recommends a "modular" implementation scheme so that new algorithms can be accommodated seamlessly when older algorithms become outdated.³⁰³ A system should be implemented to ensure security for currently stored digital evidence and future evidence that will arise from the Russia-Ukraine war, as well as future conflicts and atrocities.

In maintaining a proper and secure system, the ICC should put into place a cybersecurity maintenance process to support any security systems. In the guidelines for civil society organizations, the ICC emphasizes performing a security assessment before engaging in the collection of online evidence.³⁰⁴ The ICC must follow these guidelines and conduct an evaluation of its systems to mitigate any cybersecurity

296. Quilling, *supra* note 123, at 10.

297. International Criminal Court, *Code of Judicial Ethics*, art. 7(2). No. ICC-BD/02-01-05.

298. See Gumpert & Nuzban, *supra* note 154, at 1 (noting *Nyiramasuhuko* trial where those accused were arrested between 1995-98 and their trial began in 2001).

299. See Quilling, *supra* note 123, at 7 (arguing that ICC's under-preparedness undermines its credibility and capacity to handle cases).

300. *Id.*

301. *Id.* at 10.

302. *Id.*

303. RUSS HOUSLEY, GUIDELINES FOR CRYPTOGRAPHIC ALGORITHM AGILITY AND SELECTING MANDATORY-TO-IMPLEMENT ALGORITHMS 3 (2015), <https://www.rfc-editor.org/rfc/pdf/rfc7696.txt.pdf>.

304. GUIDELINES FOR CIVIL SOCIETY ORGANIZATIONS, *supra* note 67, at 34.

risks³⁰⁵ and to prevent manipulation of digital evidence. Additionally, through contributions to the Fund, the ICC should put into place a regular cybersecurity review by experts to ensure the continued sufficiency and security of its systems. The ICC could implement these changes through the Fund's two-pronged approach.

VII. THE FUTURE OF ATROCITY PROSECUTIONS: UKRAINE AS A CASE STUDY

The atrocities committed during the Russia-Ukraine war will present the ICC with an opportunity to implement the recommendations set forth above. The current conflict involves widespread public awareness of atrocities viewed on social media, as discussed in this Comment. Further, the warrant against Putin indicates the ICC's intention to hold even the most senior and powerful perpetrators accountable.³⁰⁶ However, bringing Putin to justice presents a great challenge for the ICC, one which may determine the future legitimacy of the Court in the eyes of member states to the Rome Statute and the whole international community. While warrants are ordinarily kept confidential, an ICC press release noted that the existence of the warrants was disclosed in hopes that public awareness might contribute to the prevention of further atrocities.³⁰⁷

The symbolic nature of the warrants also matters deeply to Ukrainian victims suffering atrocities at the hands of Putin's soldiers.³⁰⁸ The warrant brands Putin a war criminal, delegitimizing him in the international sphere, and spotlights the heinous crimes being committed against the Ukrainian people.³⁰⁹ Further, the warrants will isolate Putin from the rest of the world and restrict his travel to ICC member states who are now under treaty obligation to arrest him.³¹⁰ Both international and domestic leaders, who have previously been willing to associate with Putin, may, in light of the negative optics, reconsider their relationships and refrain from fraternizing with a war criminal.

However, the warrants are not without vocal opposition from Russia. The country's U.N. representative, Vasily Nebenzya, has already stated that they consider all documents from the ICC to be "void" and that "[t]he ICC is on the road to self-destruction" in terms of credibility and international recognition.³¹¹ Indeed, when the Court attempts to exert jurisdiction over a national of a State which has not accepted the Court's jurisdiction, criticisms that the Court is overstepping its power have been raised in the past by powerful nations like the United States.³¹² In this

305. See Quilling, *supra* note 123, at 10.

306. Rebecca Hamilton, *The ICC Goes Straight to the Top: Arrest Warrant Issued for Putin*, JUST SEC. (Mar. 17, 2023), <https://www.justsecurity.org/85529/the-icc-goes-straight-to-the-top-arrest-warrant-issued-for-putin>.

307. *ICC Judges Issue Arrest Warrants*, *supra* note 1.

308. Hamilton, *supra* note 306.

309. *Id.*

310. Pomper, *supra* note 2.

311. *Russian Hawks Threaten Nuclear Strikes Over Putin Hague Warrant*, THE MOSCOW TIMES (Mar. 20, 2023), <https://www.themoscowtimes.com/2023/03/20/russian-hawks-threaten-nuclear-strikes-over-putin-hague-warrant-a80544>.

312. See *supra* notes 28–38 and the accompanying text for a discussion on criticisms of the court's jurisdiction.

way, Putin's indictment and the subsequent case before the ICC will also play an important role in determining the legitimacy of the Court.³¹³ While the question of jurisdiction persists and will likely be determined by the reactions of member states to the Rome Statute,³¹⁴ issues surrounding the use of digital evidence arise in proving the case against Putin.

Based on the wealth of digital information available and the hints that the prosecution may already be relying on this evidence to issue the warrant for Putin,³¹⁵ it is likely that digital evidence will be used during any trial prosecuting war crimes occurring during the Russia-Ukraine war. In fact, digital evidence, particularly user-generated evidence, will be a powerful tool for prosecutors because it can combat several shortcomings of traditional evidence. User-generated evidence can preserve evidence at the moment an event occurred.³¹⁶ While investigators have been on site in Ukraine to collect evidence of potential crimes,³¹⁷ many areas continue to be inaccessible to ICC investigators until a significant amount of time after the initial event has occurred.³¹⁸ As time lapses between the commission of the crime and the investigation, the risks of physical evidence being destroyed increase.³¹⁹

A good example of this is the air strike on the Mariupol Theater.³²⁰ On March 16, 2022, the theater, which had been serving as the city's main bomb shelter for more than a week, was hit by a Russian airstrike, with evidence pointing to the strike intentionally targeting the structure housing civilians.³²¹ After Russian troops gained control of that area of the city, they began to clear the ruins and dismantle evidence of the strike.³²² Using cell phone photos and videos taken by survivors and witnesses, the Center for Spatial Technologies is creating a 3D model of the theater and an archive dedicated to documenting the atrocity.³²³ The Center for Spatial Technologies' work highlights the hopes for user-generated evidence—that this kind of digital media can document atrocities which might otherwise be lacking in physical evidence, whether because perpetrators attempt to cover up their actions or because a significant period of time has passed before investigators are allowed on-site to collect evidence.

313. *E.g.*, Prince Zeid Raad Al Hussein et al., *The International Criminal Court Needs Fixing*, ATLANTIC COUNCIL (Apr. 24, 2019), <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-international-criminal-court-needs-fixing/>.

314. Jackson, *supra* note 44.

315. Khan, *supra* note 5.

316. Mehandru & Koenig, *supra* note 145.

317. *Proposed Programme Budget for 2023 of the International Criminal Court*, *supra* note 156.

318. Gumpert & Nuzban, *supra* note 154.

319. Hamilton, *supra* note 75, at 14.

320. Lori Hinnant et al., *AP Evidence Points to 600 Dead in Mariupol Theater Airstrike*, AP NEWS (May 4, 2022, 7:12 AM), <https://apnews.com/article/russia-ukraine-war-mariupol-theater-c321a196fbd568899841b506afc7a1>.

321. *Id.*

322. *Id.*

323. *Mariupol Drama Theater*, SPATIAL ARCHIVE, <https://theater.spatialtech.info> (last visited Nov. 16, 2023).

The Mariupol Theater strike also highlights a tragic reason for user-generated evidence; many victims may not survive atrocities. Ukrainian officials stated that at least 300 people were killed in the strike, but survivors also indicated that the death toll could be as high as 1,000.³²⁴ Additionally, the Russia-Ukraine War, like other serious conflicts that come before the ICC,³²⁵ has displaced almost 14 million people.³²⁶ Identifying witnesses who have been displaced or locating them after a significant period of time has passed between the crime and the ICC's investigations is often incredibly difficult. User-generated evidence provides an alternative way to present evidence where witnesses may not have survived or may not be identifiable.

The use of this content is not only a necessary step in the innovation and development of the ICC. It is also integral to maintaining the ICC as a legitimate judicial body. Nearly since its inception, the ICC has faced a myriad of criticisms, many of which are directed at the legitimacy of the Court.³²⁷ The ICC has taken a very public step by issuing the warrant for Putin's arrest. Given the controversial nature of the jurisdiction over Putin, the legitimacy of the Court will suffer if it tries and fails to hold Putin accountable. To ensure accountability for the atrocities being committed in Ukraine, the Court must effectively utilize the myriad of digital evidence available, including user-generated evidence. As the ICC generally operates on an extended timeline, there is ample time for the Court to prepare for the inclusion of this evidence. In particular, the Court should begin developing educational programs for prosecutors and judges based on existing guidelines such as the Berkeley Protocol. This will allow judges to be better prepared to rule on the admissibility of user-generated evidence. In particular, this education can help to inform the second prong of the three-part test where judges assign probative value.³²⁸ The more knowledge judges have about proper standards for verification and storage of digital evidence, the better equipped they are to understand and assess the veracity of a piece of evidence. This, in turn, assists the Court in assigning the evidentiary weight of a piece of evidence.

324. Hugo Bachege, *Russia's Attack on Mariupol Theatre a Clear War Crime, Amnesty Says*, BBC NEWS (June 30, 2022), <https://www.bbc.com/news/world-europe-61979873>.

325. See *The Rwandan Genocide and Its Aftermath*, THE STATE OF THE WORLD'S REFUGEES 245, 246 (2000) <https://www.unhcr.org/en-ie/3ebf9bb60.pdf> (noting 2 million refugees outside Rwanda and 1.5 million people internally displaced at end of 1994); *Democratic Republic of Congo: Internally Displaced Persons and Returnees* (July 2022), OCHA SERVICES RELIEF WEB (Aug. 18, 2022), <https://reliefweb.int/report/democratic-republic-congo/democratic-republic-congo-internally-displaced-persons-and-returnees-july-2022> (noting 5.5 million people currently displaced in Democratic Republic of Congo); *Internally Displaced Persons and Returnees in Libya, July 2021*, OCHA SERVICES RELIEF WEB (Jul. 31, 2021), <https://reliefweb.int/report/libya/internally-displaced-persons-and-returnees-libya-july-2021> (noting approximately 245,000 persons displaced in Libya in 2021).

326. See *Ukraine Refugee Situation*, UNHCR OPERATIONAL DATA PORTAL, <https://data.unhcr.org/en/situations/ukraine> (last updated Dec. 27, 2022) (listing nearly 8 million refugees from Ukraine recorded across Europe); see also UKRAINE INTERNAL DISPLACEMENT REPORT: NOVEMBER/DECEMBER 2022 at 1, INT'L ORG. FOR MIGRATION (2022) (noting 5.9 million internally displaced people across Ukraine).

327. Takemura, *supra* note 159, at 4.

328. Rome Statute of the International Criminal Court, *supra* note 21, art. 69(4).

Additionally, if the ICC takes steps to improve its cybersecurity, it will be prepared for any potential attacks to destroy or compromise digital evidence. This is particularly relevant in the case of the Russia-Ukraine war because Russia has been known to engage in malicious cyber activities for a variety of reasons, including to harm international adversaries.³²⁹ Putin's arrest warrant sparked immediate outrage from Russian officials, with extreme reactions including bomb threats towards the ICC.³³⁰ It is clear that Putin and his accomplices view the Court as an adversary. As the ICC continues its investigation into the crimes committed during the Russia-Ukraine war—as it should—the Court must prepare for the possibility of cyberattacks by improving the security for digital evidence storage. If the ICC does not address the weaknesses in this security, such as the outdated hashing system,³³¹ evidence necessary to bring perpetrators to justice may be compromised. However, if the ICC updates these systems and maintains adequate security, it can preserve and protect necessary evidence for the Russia-Ukraine war and future atrocities.

If the Court proceeds with an investigation and subsequent trial of Putin and other war criminals without the use of digital evidence, it may fail to hold these actors accountable. In the case of the Mariupol Theater strike, if Russian troops destroy existing physical evidence and if videos taken by witnesses are ruled inadmissible in court, the ICC may be left with only witness testimonies. Considering the difficulties the Court faces in identifying and locating witnesses, as well as the criticisms of overreliance on witness testimonies in past cases, witness testimonies might not be sufficient to hold the perpetrators accountable.³³² As such, a crime that has been widely reported and witnessed around the world may go unpunished.³³³ A failure of the ICC to obtain justice for these victims will, in turn, negatively impact the legitimacy of the Court, causing stakeholders, such as witnesses and State Parties, to lose faith in the Court and cease cooperating in subsequent investigations.

As an increasing number of states are insulating themselves from international law, the question of legitimacy and judicial processes comes to the forefront, particularly when acts by aggressor states are broadcast across social media and seen worldwide on a level that has not been possible in the past.³³⁴ The ICC must be able to utilize the new digital evidence available to it effectively and fairly. The Russia-Ukraine war presents the Court with an opportunity to show the world its longevity and legitimacy for holding perpetrators accountable during this and future conflicts.

329. *Russia Cyber Threat Overview and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia> (last visited Nov. 16, 2023).

330. Beyza Binnur Donmez, *ICC Expresses Concern About Russian Threats Over Putin Warrant*, ANADOLU AGENCY (Mar. 23, 2023), <https://www.aa.com.tr/en/europe/icc-expresses-concern-about-russian-threats-over-putin-warrant/2853704>.

331. Quilling, *supra* note 123, at 5.

332. Freeman, *supra* note 22, at 305.

333. *See, e.g.*, Hinnant et al., *supra* note 320; Bachega, *supra* note 324.

334. Johnson, *supra* note 11.

VIII. CONCLUSION

The ICC faces an uphill battle to maintain its legitimacy and implement practices that will propel it into the future through the utilization of user-generated evidence in atrocity prosecutions. The globally witnessed Russia-Ukraine war provides an important opportunity for the ICC to standardize its processes for handling, storing, and using digital evidence. However, if the ICC fails to take these necessary steps, the Court faces the potential to lose both normative and sociological legitimacy, leading to a lack of support and funding from State Parties. To be a respected international tribunal that provides justice to victims of the gravest crimes, the ICC must not disregard technological advances. Instead, the ICC must invest in policies that recognize the necessity and benefits of admitting user-generated evidence to prosecute atrocity cases.