Leiden Journal of International Law (2024), **37**, 228–250
doi:10.1017/S0922156523000444

ORIGINAL ARTICLE

INTERNATIONAL CRIMINAL COURTS AND TRIBUNALS

Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism

Elizabeth White*

Amsterdam Law School, University of Amsterdam, Nieuwe Achtergracht 166, 1018 WV Amsterdam, The Netherlands
Email: elizabeth.white@columbia.edu

Abstract

Digital open-source evidence has become ubiquitous in the context of modern conflicts, leading to an evolution in investigative practices within the context of mass atrocity crimes and international criminal law. Despite its extensive promulgation, international criminal tribunals have had few opportunities to address the admissibility of user-generated open-source evidence. Through semi-structured interviews with experts and analyses of primary and secondary sources, this article examines the current standards and practices governing the use of user-generated open-source evidence. Current practices illuminate a number of gaps in the realm of digital open-source evidence in international criminal law. This article posits the establishment of a standing international, investigative mechanism as a solution to a need for increased standardization and co-ordination within the realm of user-generated open-source evidence. By standardizing the collection and use of such evidence, investigative bodies will be prepared to more effectively serve the international justice community.

Keywords: digital evidence; international criminal investigations; open-source investigation; social media

1. Introduction

Over the course of late 2021, intelligence services noticed a concerning build-up of Russian resources and troops along the Ukrainian border.[1] As satellite images depicted increasingly unusual activity around the end of the year, concerns of an imminent attack began mounting.[2] Digital evidence of the changing landscape offered the international community foresight into what the coming months might bring.[3] This insight into future military actions, through satellite imagery and other forms of digital evidence, is a hallmark of the landscape of modern

*Thank you to Tomas Hamilton, Lori Damrosch, and Patryk Labuda for their review and insight throughout the drafting process; to my interviewees for their time and thoughtfulness in speaking with me; and to my anonymous reviewers for their comments. All errors are my own.

[1]S. Harris and P. Sonne, 'Russia Planning Massive Military Offensive against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns', *New York Times*, 3 December 2021, available at www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

[2]Ibid.

[3]Ibid.

warfare – a terrain void of the surprise element associated with the outbreak of previous conflicts.[4]

The utility of digital evidence did not, however, cease as the conflict intensified. Videos of developments in Ukraine quickly dominated Twitter, Facebook, and TikTok, among other social media platforms. Digital platforms showed footage of streets with cars replaced by tanks and armoured vehicles,[5] civilians huddling together to take refuge in subways stations,[6] and buildings aflame against smoke-covered skylines.[7] Not only did digital evidence offer warnings of attacks to come but also showed real-time indication of events on the ground.

Digital evidence is useful not only prospectively in conflict but also retrospectively. The promulgation of digital evidence in Ukraine currently is not exceptional but is rather indicative of what modern warfare will entail. There are more hours of video footage of the Syrian conflict than there have been hours of conflict,[8] and there is no reason to suspect that present, and future, conflicts will not be similarly documented. Digital evidence will serve as a historical record of conflicts for the affected communities, the world writ large, and, hopefully, the field of international criminal justice.

Despite the utility of digital evidence, it is not without its pitfalls. In the wake of a mass of new uploads, Twitter recently mistakenly suspended a number of accounts reporting from Ukraine.[9] Not only is this incident reflective of suboptimal moderation policies of social media platforms, but it is also an example of the potential weaponization of digital sources. The wrongfully-suspended accounts alleged that their accounts were removed due to an attack by Russian bots that had mass reported these accounts' content.[10] While Twitter denied evidence of a co-ordinated attack, it admitted that the accounts had been suspended 'in error', and subsequently reinstated many of the accounts.[11] This incident is not an unprecedented one – digital evidence is particularly unique in its volatility, both in terms of the ease with which it can be altered and with which it can be publicly removed. Whether in error or intentionally, in the case of moderation of hate speech or incitement to violence,[12] digital evidence can be permanently deleted at the click of a button.[13]

Evidentiary procedures in international criminal law were neither crafted with digital evidence nor the modern conflict in mind. Digital evidence is, in many respects, distinct from more traditional forms of evidence. Electronic, or digital, evidence is defined as '[i]nformation and data

[4]W. Watts, 'Here's the Technology Being Used to Watch Russian Troops as Ukraine Invasion Fears Linger', *MarketWatch*, 17 February 2022, available at www.marketwatch.com/story/how-fears-of-russian-invasion-of-ukraine-put-open-source-intelligence-in-spotlight-11645033603.

[5]E.g., Sky News (@SkyNews), 'People try to stop Russian tanks from advancing in Ukraine. Sky News has verified and located this video to Bakhmach, northeastern Ukraine. The tanks have similar circular markings that have previously been seen on Russian equipment', *Twitter*, 26 February 2022 available at twitter.com/SkyNews/status/1497672819429322757.

[6]E.g., M. Yam (@yamphoto), '3/2: Lena from Kyiv, wipes her brow in exhaustion, takes care of Max, 3, whom she has only known for a few days, while his parents are getting some rest, in a subway station where civilians are taking shelter from Russian air raids in #Kyiv, #Ukraine', *Twitter*, 2 March 2022 available at twitter.com/yamphoto/status/1499142393240641536.

[7]E.g., The New York Times (@nytimes), 'Video verified by The New York Times shows the bombardment of Chernihiv, Ukraine, on Thursday. As smoke cleared from the attack — which hit near apartments, pharmacies and a hospital — people are seen running in the street', *Twitter*, 3 March 2022 available at twitter.com/nytimes/status/1499414309645991957.

[8]A. Greenberg, 'Google's New YouTube Analysis App Crowdsources War Reporting', *Wired*, 20 April 2016, available at www.wired.com/2016/04/googles-youtube-montage-crowdsources-war-reporting/.

[9]E. Culliford, 'Twitter Says It Mistakenly Took Down Accounts Posting on Russian Military', *Reuters*, 23 February 2022, available at www.reuters.com/world/twitter-says-it-mistakenly-took-down-accounts-posting-russian-military-2022-02-23/.

[10]Ibid.

[11]Ibid.

[12]'Video Unavailable: Social Media Platforms Remove Evidence of War Crimes', *Human Rights Watch*, 10 September 2020, available at www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes.

[13]It is important to note that when a user, or content moderator, deletes content from the public sphere, the content is not necessarily permanently lost. Platforms may retain backup copies of deleted content that remain accessible, even if not to the public.

of investigative value that are stored in or transmitted by an electronic device'.[14] The rising use of digital evidence dovetailed with the emergence of open-source investigations (OSINT), or investigations that rely on publicly available digital information.[15] With OSINTs emerging as not only a prudent, but necessary, form of investigations in international criminal law, courts and investigative bodies are confronting unregulated and novel forms of evidence. Without significant internal guidance, a range of best practices regarding digital evidence has emerged from these investigative bodies.

The creation of a standing investigative mechanism has the potential to strengthen evidence collection and use across the international criminal justice system, particularly within the realm of open-source evidence. In the early years of the International Criminal Court (ICC or Court), concerns of ineffective investigations plagued its reputation.[16] In response, the Court began broadening its evidentiary sources, including increased reliance on information collected by third-parties.[17] Continuing this trend, notably with respect to open-source investigations involving user-generated evidence,[18] will further strengthen international criminal justice. Given the novelty of the use of user-generated open-source evidence before international criminal tribunals, despite the progress made by investigative bodies, there are a number of challenges with respect to the use of digital evidence. A standing investigative mechanism can facilitate greater standardization in the use of, and access to, evidence across the investigative community, allowing for an improvement in the quality of international criminal investigations and effective prosecutions.

2. Current evidentiary practices in international criminal law

2.1. Evidentiary standards set by courts

The renaissance of international criminal law took the turn of the twenty-first century by storm. Over the course of a decade, a flurry of internationalized courts – the *ad hoc* tribunals, the ICC, and hybrid courts – revitalized the field. Faced with the prospect of creating an internationalized court, the component parts of these courts reflect the compromises it took to create them. Notably, the rules of evidence of international courts, across the board, reveal a combination of civil and common law legal systems, with significant deference to Chambers to address the novel issues these courts would inevitably encounter. By design, the evidentiary rules of courts are limited but provide the standards through which digital evidence must be considered.

2.1.1. Rules of admissibility and exclusion

In adopting standards of evidence for the *ad hoc* tribunals, the drafters of their Rules of Evidence and Procedure prioritized flexibility. Given the limited precedent in the field of international criminal law prior to the establishment of the *ad hoc* tribunals, flexible rules of evidence allowed for judges to tackle issues of first impression without being bound by technical rules of evidence, similarly to the approach adopted by the Nuremberg tribunal.[19] Beginning with

[14]United States of America Department of Justice, 'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors', January 2007, available at www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors, at 72.

[15]UC Berkeley Human Rights Center, 'The New Forensics: Using Open-source Information to Investigate Grave Crimes', 2018 available at humanrights.berkeley.edu/sites/default/files/publications/bellagio_report_july2018_final.pdf, at 3.

[16]L. Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials', (2018) 41(2) *Fordham International Law Journal* 283, at 289.

[17]E. Baylis, 'Outsourcing Investigations', (2010) 14(1) *UCLA Journal of International Law and Foreign Affairs* 121, at 126–33.

[18]User-generated evidence is defined, for the purposes of this article, as content 'recorded on a device such as a smartphone by an ordinary citizen', with the potential for use as evidence in a future international criminal trial. R. Hamilton, 'User-Generated Evidence', (2018) 57(1) *Columbia Journal of Transnational Law* 1, at 3.

[19]1945 Charter of the International Military Tribunal, 59 Stat. 1544, 82 UNTS 279, Art. 19.

the *ad hoc* tribunals,[20] the Rules of Procedure and Evidence of international justice mechanisms provide for broad admissibility of relevant evidence.[21] The general standard that has emerged for the admissibility of evidence across courts[22] is a tripartite test that considers the evidence's (i) relevance,[23] and (ii) probative value,[24] weighed against (iii) any potential prejudice.[25]

Despite the general admissibility of evidence, there are limited exclusionary rules prohibiting the introduction of evidence before international courts. The *ad hoc* and hybrid tribunals broadly prohibit the introduction of evidence 'obtained by methods which cast substantial doubt on its reliability or if its admission is antithetical to, and would seriously damage, the integrity of the proceedings'.[26] Similarly, the Rome Statute offers two situations where judges may determine the admissibility of evidence:

> Evidence obtained by means of a violation of this Statute or internationally recognized human rights shall not be admissible if: (a) The violation casts substantial doubt on the reliability of the evidence; or (b) The admission of the evidence would be antithetical to and would seriously damage the integrity of the proceedings.[27]

[20]Rule 89(C) of both the International Criminal Tribunal for the former Yugoslavia (ICTY) and International Criminal Tribunal for Rwanda (ICTR) Rules of Evidence and Procedure (RPE) provide that, '[a] Chamber may admit any relevant evidence which it deems to have probative value'. Rules of Procedure and Evidence of the ICTY, UN Doc. IT/32 (1994) (ICTY RPE), Rule 89(C); Rules of Procedure and Evidence of the ICTR, UN Doc. ITR/3 (1995) (ICTR RPE), Rule 89(c).

[21]Art. 69(4) of the Rome Statute provides for the general admissibility of evidence, but '[t]he Court may rule on the relevance or admissibility of any evidence, taking into account, *inter alia*, the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness'. 1998 Rome Statute of the International Criminal Court, 2187 UNTS, (Rome Statute), Art. 69(4). Extraordinary Chambers Court of Cambodia Internal Rules (Rev. 9, 2015) (ECCC), Rule 87.

[22]Art. 69(4) of the Rome Statute provides for the general admissibility of evidence, but '[t]he Court may rule on the relevance or admissibility of any evidence, taking into account, *inter alia*, the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness'. See Rome Statute, ibid., Art 69(4); ECCC, ibid., Rule 87; ICTY RPE, *supra* note 20, Rule 89(D); *Prosecutor v. Bagosora et al.*, Appeals Chamber, Decision on Prosecutor's Interlocutory Appeals regarding Exclusion of Evidence, Case Nos. ICTR-98-41-AR93 and ICTR-98-41-AR93.2, 19 December 2003, para. 16; *Prosecutor v. Édouard Karemera et al.*, Decision on the Prosecutor's Motion for Admission of Certain Exhibits into Evidence, Case No. ICTR-98-44-T, Trial Chamber III, 25 January 2008, para. 9.

[23]Relevant evidence is defined as, 'mak[ing] the existence of a fact at issue more or less probable', with regard to the facts of the case at issue. *Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui*, Decision on the Bar Table Motion of the Defence of Germain Katanga, Case No. ICC-01/04-01/07, Trial Chamber II, 21 October 2011, para. 16; *Prosecutor v. Thomas Lubanga Dyilo*, Decision on the Admissibility of Four Documents, Case No. ICC-01/04-01/06, Trial Chamber I, 13 June 2008, para. 24 (Lubanga Admissibility Decision).

[24]The probative value of evidence is determined by judges, 'on a case-by-case basis, in light of different criteria, such as its relevance, the source from which it originates, its direct or indirect nature, its credibility, reliability, trustworthiness and genuineness'. *Prosecutor v. Francis Kirimi Muthaura, Uhuru Muigai Kenyatta and Mohammed Hussein Ali*, Decision on the Defence Applications for Leave to Appeal the Single Judge's Order to Reduce the Number of Viva Voce Witnesses, Case No. ICC-01/09-02/11, Pre-Trial Chamber II, 1 September 2011, para. 26. Probative value is determined based upon relevance to the elements of the crime with which an accused is charged. *Prosecutor v. Bagosara et al.*, Decision on Admissibility of Proposed Testimony of Witness DBY, Case No. ICTR-98-41-T, Trial Chamber I, Decision on Admissibility of Proposed Testimony of Witness DBY, 18 September 2003, para. 4.

[25]*Prosecutor v. Delalic et al.*, Decision on the Motion of the Prosecution for Admissibility of Evidence, Case No. IT-96-21-T, Trial Chamber, 19 January 1998, para. 16; *Prosecutor v. Akayesu*, Judgement, Case No. ICTR-96-4-T, Trial Chamber, 2 September 1998, para. 136; *Ngeze and Nahimana v. Prosecutor*, Décision sur les appels interlocutoires, Separate Opinion of Judge Shahabuddeen, Case Nos. ICTR-97-27-AR72 and ICTR-96-11-AR74, Appeals Chamber, 5 September 2000, para. 19; *Prosecutor v. Bagosora et al.*, Decision on Prosecutor's Interlocutory Appeals regarding Exclusion of Evidence, Case Nos. ICTR-98-41-AR93 and ICTR-98-41-AR93.2, Appeals Chamber, 19 December 2003, para. 16; *Prosecutor v. Jean-Pierre Bemba Gombo*, Public Redacted Version of Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute, Case No. ICC-01/05-01/08-2299-Red, Trial Chamber III, 8 October 2012, para. 7.

[26]See ICTY RPE, *supra* note 20, Rule 95; see ICTR RPE, *supra* note 20, Rule 95. See also Rules of Procedure and Evidence of the Special Tribunal for Lebanon (STL RPE), Rule 162(A); *Prosecutor v. Delalic et al.*, Decision on Zdravko Mucic's Motion for the Exclusion of Evidence, Case No. IT-96-21-T, Trial Chamber, 2 September 1997, para. 43.

[27]See Rome Statute, *supra* note 21, Art. 69(7).

This exclusionary standard is discretionary, however, and permits judges 'to seek an appropriate balance between the statute's fundamental values in each concrete case'.[28] The Special Court for Sierra Leone (SCSL) similarly provides for the exclusion of evidence 'if its admission would bring the administration of justice into serious disrepute'.[29] The Extraordinary Chambers in the Courts of Cambodia (ECCC) specifically excludes statements obtained through 'inducement, physical coercion or threats thereof',[30] and evidence obtained through interceptions or recordings of conversations via telephone or electronic correspondence.[31] Accordingly, unless excluded on these bases, evidence is generally admitted to the record, with reliability dictating weight rather than admissibility.[32]

Without stringent rules governing admissibility of evidence, the jurisprudence of international criminal mechanisms has expounded somewhat upon the limited rules of evidence. Within the context of open-source evidence, however, given the limited exposure, the jurisprudence is also limited.[33] Across the courts, while judges may determine the admissibility of evidence at the time of submission or with the final judgment, relevant evidence is generally admitted to the record, with its weight determined in the final judgment.[34] However, notably, the admissibility of digital evidence has exceptionally been ruled upon prior to that judgment,[35] given the unprecedented nature of the source material before international courts. As such, should this practice continue, the specific considerations for digital evidence may continue to emerge. In the meantime, however, the general tripartite standard for the admissibility of evidence will continue to govern.

When considering the admissibility of open-source evidence, probative value is likely the most precarious element of the three. Across tribunals, jurisprudence has established that reliability and authenticity are two crucial components in the assessment of probative value.[36] While related concepts, reliable evidence is, at its base, what it proports to be, while authentic evidence has not been manipulated or tampered with. Reliability can be established through a variety of factors, including the origin, content, corroboration, truthfulness, voluntariness, and trustworthiness of the evidence.[37] Authenticity, on the other hand, can be established based on a number of internal, relating to the evidence itself, and external, relating to the collection and management of the

[28]*Prosecutor v. Thomas Lubanga Dyilo*, Decision on the Confirmation of Charges, Case No. ICC-01/04-01/06, Pre-Trial Chamber I, 7 February 2007, para. 84.

[29]Rules of Procedure and Evidence of the Special Court for Sierra Leone (SCSL RPE), Rule 95.

[30]See ECCC, *supra* note 21, Rule 21(3).

[31]Ibid., Rule 52.

[32]P. M. Wald, 'Rules of Evidence in the Yugoslav War Tribunal', (2003) 21(4) *Quinnipiac Law Review* 761.

[33]As 'none of the Chambers discussed the admissibility of social media evidence or specific evidentiary requirements . . . no authoritative guidelines could be reasonably deduced or formulated'. Leiden University, 'Leiden Guidelines on the Use of Digitally Derived Evidence', 2022, available at leiden-guidelines.netlify.app/guidelines/#d-scope-of-the-leiden-guidelines (Leiden Guidelines).

[34]L. Freeman, 'Hacked and Leaked: Legal Issues Arising From the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases', (2021) 25(2) *UCLA Journal of International Law and Foreign Affairs* (2021) 45, at 72.

[35]*Prosecutor v. Bemba*, Decision on Requests to Exclude Western Union Documents and other Evidence Pursuant to Article 69(7), Case No. ICC-01/05-01/13-1854, Trial Chamber VII, 29 April 2016; *Prosecutor v. Bemba* Decision on Requests to Exclude Dutch Intercepts and Call Data Records, Case No. ICC-01/05-01/13-1855, Trial Chamber VII, 29 April 2016 (Bemba Decision on Requests to Exclude); *Prosecutor v. Salim Jamil Ayyash et al.*, Decision on the Admissibility of Documents Published on the Wikileaks Website, Case No. STL-11-01/T/TC, Trial Chamber, 21 May 2015.

[36]*Prosecutor v. Dusko Tadić*, Decision on Defence Motion on Hearsay, Case No. IT-94-1-T, Trial Chamber, 5 August 1996, paras. 9, 15; *Prosecutor v. Zejnil Delalić et al.*, Decision on the Motion of the Prosecution for the Admissibility of Evidence, Case No. IT-96-21- T, Trial Chamber, 19 January 1998, para. 16; *Prosecutor v. Pauline Nyiramasuhuko et al.*, Decision on Pauline Nyiramasuhuko's Appeal on the Admissibility of Evidence, Case No. ICTR-98-42-AR73.2, Appeals Chamber, 4 October 2004, para. 7; see Lubanga Admissibility Decision, *supra* note 23, para. 18; *Prosecutor v. Édouard Karemera et al.*, Decision on Joseph Nzirorera's Appeal of Decision on Admission of Evidence Rebutting Adjudicated Facts, Case No. ICTR-98-44-AR73.17, Appeals Chamber, 29 May 2009, para. 14.

[37]Leiden University, 'Report on Digitally Derived Evidence in International Criminal Law', 2019, available at leiden-guidelines.com/assets/DDE%20in%20ICL.pdf.

evidence, indicators.[38] For digital evidence, relevant internal indicators relate to the creation of the evidence, such as geolocation, source codes, and metadata.[39] To date, the ICC has primarily relied upon geolocation[40] and expert testimony reports[41] to establish internal indicators. External indicators include the provenance and chain of custody of evidence.[42] The *ad hoc* tribunals generally admit evidence when corroborated by external indicators, such as expert testimony and corresponding transcripts.[43] Additionally, while 'nothing in the Statute or the Rules expressly states that the absence of information about the chain of custody ... affects the admissibility or probative value of Prosecution evidence',[44] tribunals have broadly emphasized the importance of proof of chain of custody in determining authenticity,[45] particularly for digital evidence.[46]

Given the nature of open-source evidence, while there are specific issues that are notably under addressed in the realm of digital evidence,[47] investigators must exercise particular diligence in ensuring, establishing, and conveying the reliability and authenticity of evidence in order to ensure its admissibility. Throughout the collection, storage, and admission processes, ensuring that markers of reliability and authenticity remain intact is of the utmost importance for the use of open-source evidence.

2.1.2. Determination of weight

Even if Chambers determine that evidence is admissible, this finding has 'no bearing on the final weight to be afforded to it, which will only be determined by the Chamber at the end of the case when assessing the evidence as a whole'.[48] While the admissibility of all evidence is determined on the basis of standardized evidentiary tests,[49] the determination of weight is a more subjective and comprehensive analysis, and varies across categories of evidence.[50] Evidence falls into four general categories of evidence: testimonial, documentary, physical, and forensic.[51] Generally, digital open-

[38]A. Ashouri, C. Bowers and C. Warden, 'An Overview of the Use of Digital Evidence in International Criminal Courts', (2014) 11 *Digital Evidence and Electronic Signature Law Review* 115, at 118.

[39]UC Berkeley Human Rights Center and Office of the High Commissioner of Human Rights, 'Berkeley Protocol on Digital Open-source Investigations: A Practical Guide on the Effective Use of Digital Open-source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law', 2020, paras. 183–194, available at www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source (Berkeley Protocol).

[40]*Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud*, Public redacted version of the Decision on Prosecution's proposed expert witnesses, Case No. ICC-01/12-01/18-989-Red, Trial Chamber X, 21 October 2020, paras. 110, 112.

[41]*Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, Second Warrant of Arrest, Case No. ICC-01/11-01/17-13, Pre-Trial Chamber, 4 July 2018, para. 18; *Prosecutor v. Ahmad al-Faqi al-Mahdi*, Transcripts of 22 August 2016, Case No. ICC -01/12-01/15, Trial Chamber VIII, 22 August 2016, at 29, lines 3–6, 10, at 46, line 1, at 47, lines 20–21, at 99, lines 20–23, and at 100, lines 8–21.

[42]N. Mehandru and A. Koenig, 'ICTS, Social Media & The Future of Human Rights', (2019) 17 *Duke Law & Technology* 129, at 144.

[43]*Prosecutor v. Karemera, et al.*, Judgement and Sentence, Case No. ICTR-98-44-T, Trial Chamber III, 2 February 2012, para. 598; *Prosecutor v. Bagosara et al.*, Judgement and Sentence, Case No. ICTR-98-41-T, Trial Chamber I, 18 December 2008, paras. 493–494; *Prosecutor v. Radoslav Brdanin*, Judgement, Case No. IT-99-36-T, Trial Chamber II, 1 September 2004, para. 34; *Prosecutor v. Zdravko Tolimir*, Judgement, Case No. IT-05-88/2-T, Trial Chamber II, 12 December 2010, paras. 63, 64, 68, 70.

[44]*Prosecutor v. Thomas Lubanga Dyilo*, Decision on Confirmation Charges, Case No. ICC-01/04-01/06, Pre-Trial Chamber I, 29 January 2007, para. 96.

[45]*Prosecutor v. Brdanin and Talic*, Order on the Standards Governing the Admission of Evidence, Case No. IT-99-36-T, Trial Chamber II, 15 February 2002, para. 18.

[46]R. Braga da Silva, 'Updating the Authentication of Digital Evidence in the International Criminal Court', (2021) *International Criminal Law Review* 1.

[47]See Section 3.1, *infra*.

[48]*Prosecutor v. Bemba*, Decision on the admission into evidence of items deferred in the Chamber's 'Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute', Case No. ICC-01/05-01/08, Trial Chamber III, 27 June 2013, para. 9.

[49]See Section 2.1.1, *supra*.

[50]See Freeman, *supra* note 16, at 295.

[51]Ibid.

source evidence posted on social media platforms constitutes documentary evidence.[52] In the context of documentary evidence, Chambers will consider the evidence's 'provenance, source or author, as well as their role in the relevant events, the chain of custody from the time of the item's creation until its submission to the Chamber, and any other relevant information'.[53] Further, in addition to being components relevant to probative value, the authenticity and reliability of evidence are also relevant to its weight.[54]

Across the range of international courts, the standards considered by Chambers in assessing the admissibility and weight of digital evidence remain largely opaque. While the full scope of the role of digital evidence has not yet been addressed, it is also likely that the opacity of decisions regarding digital evidence is due to the way that Chambers assess the evidence. The reality is that international criminal judges are not experts in digital evidence, nor the indicators needed to verify it,[55] and to that end are largely reliant on expert testimony or other corroboration[56] to determine the weight of digital evidence, precluding a need for significant discussion of the factors in case law. Further, Chambers have explicitly stated that 'it will consider all the standard evidentiary criteria for each item of evidence submitted, though it may not necessarily discuss in the judgment every submitted item'.[57] As such, practitioners should proactively take all possible steps to ensure the clarity of the authenticity and reliability of evidence to rebut any potential concerns.

2.1.3. Storage of evidence

Due to the broad admission of evidence before international tribunals, the evidentiary record must be carefully retained so that judges are able to determine the associated weight of evidence. To that end, the retention of evidence throughout the judicial process is of the utmost importance. Prior to the commencement of proceedings, the official investigation rests within the purview of the Prosecutor, where they are 'responsible for the [preservation and retention], storage and security of information and physical evidence obtained'.[58] Once proceedings commence, however, the Registrar obtains the responsibility of retaining and preserving the record.[59] The Registrar must 'preserve a full and accurate record of all proceedings', as well as 'retain and preserve all physical evidence offered during the proceedings'.[60] Even after many iterations of revisions, the International Residual Mechanism for Criminal Tribunals' (IRMCT) RPE refer only to physical evidence.[61] Distinct from the *ad hoc* tribunals, the ICC RPE refer, in establishing the Registrar's duty of retention, to not only physical evidence, but 'all the evidence and other materials offered during the hearing',[62] broadly encompassing digital evidence in addition to more traditional forms of evidence.

[52]Ibid., at 297.

[53]*Prosecutor v. Bemba*, Judgment pursuant to Article 74 of the Statute, Case No. ICC-01/05-01/08-3343, Trial Chamber III, 21 March 2016, para. 247; Lubanga Admissibility Decision, *supra* note 23, para. 30.

[54]*Prosecutor v. Bemba*, Public Redacted Version of the First Decision on the Prosecution and Defense Requests for the Admission of Evidence, Case No. ICC-01/05-01/08-2012, Trial Chamber III, 15 December 2011, para. 15.

[55]See Freeman, *supra* note 16, at 312.

[56]See notes 40, 41, *supra*.

[57]*Prosecutor v. Said Kani*, Directions on the Conduct of Proceedings, Case No, ICC-01/14-01/21-251, Trial Chamber VI, 9 March 2022, para. 16.

[58]See ICTY RPE, *supra* note 20, Rule 41; ICTR RPE, *supra* note 20, Rule 41; Rules of Procedure and Evidence of the International Criminal Court (ICC RPE), Rule 10; STL RPE, *supra* note 26, Rule 64; SCSL RPE, *supra* note 29, Rule 41(A).

[59]See ICTY RPE, *supra* note 20, Rule 81; ICTR RPE, *supra* note 20, Rule 81; ICC RPE, *supra* note 58, Rules 137–138; STL RPE, *supra* note 26, Rule 139; SCSL RPE, *supra* note 29, Rule 81. The ECCC, distinctly, places the responsibility of the retention and preservation of evidence, 'including physical evidence, statements and documents obtained in the course of preliminary investigations, judicial investigations, trials, and appeals', with the Office of Administration. See ECCC, *supra* note 21, Rule 9(6).

[60]Ibid.

[61]Rules of Procedure and Evidence of the International Residual Mechanism for Criminal Tribunals, UN Doc. MICT/1/Rev.7 (4 December 2020), Rule 95(C) (IRMCT RPE).

[62]See ICC RPE, *supra* note 58, Rule 138.

Despite the novelty of digital evidence at the time of the creation of the *ad hoc* tribunals, these courts introduced an electronic document management system to organize and retain evidentiary materials.[63] Consequently, when the IRMCT established its own rules of evidence, it created a rule requiring the Prosecutor to 'make available to the Defence, in electronic form, collections of relevant material held by the Prosecutor, together with appropriate computer software with which the Defence can search such collections electronically'.[64] This effort, while clearly a recognition of the need for electronic storage and sharing of documents, only scratched the surface of the role of technology before international courts. Similarly to the IRMCT, the ICC also adopted a regulation providing for the electronic management of the Court. Regulation 26 requires that the Court 'establish a reliable, secure, efficient electronic system', to be implemented by the Registry, in order to 'ensure authenticity, accuracy, confidentiality and preservation of judicial records and material'.[65] As such, '[i]n proceedings before the Court, evidence other than live testimony shall be presented in electronic form whenever possible'.[66] The ICC also developed an 'e-Court Protocol', which establishes specific standards for digital evidence in order to 'ensure authenticity, accuracy, confidentiality and preservation of the record of proceedings'.[67] The standards, however, largely offer guidance on the storage and format of evidence,[68] rather than admissibility standards. Recently, the Office of the Prosecutor announced the creation of a new access link, OTPLink, to facilitate submission of evidence.[69] In response to common issues associated with digital evidence, OTPLink allows any witness with a web-enabled device to securely submit evidence, uses a combination of machine learning and artificial intelligence to review and sort submissions, and creates a digital chain of custody in line with the Court's standards.[70] With the passage of time since the *ad hoc* tribunals' establishment and the associated technological advancements, the ICC certainly offers additional insight into international tribunals' handling of digital evidence, but the still limited case law regarding digital evidence leaves open a number of remaining issues.

2.2. Evidentiary practices employed by investigative bodies

Following the emergence of international tribunals, the international criminal justice community, deterred by the hurdles associated with the establishment of those tribunals, turned towards other avenues for accountability. In both the public and private spheres, a number of investigative bodies emerged to document atrocity crimes in an effort to pave the way for future judicial efforts. Given their emphasis on investigative work, and their subsequent co-operation with international tribunals, these investigative bodies offer insight into the collection and management of digital evidence.

2.2.1. Public investigative efforts

Following the resurgence of international criminal tribunals at the turn of the twenty-first century, the United Nations (UN) General Assembly (UNGA) began playing a more active role in

[63]T. H. Peterson, 'Temporary Courts, Permanent Records', *United States Institute of Peace*, August 2006, available at www.usip.org/sites/default/files/resources/sr170.pdf, at 4.

[64]See IRMCT RPE, *supra* note 61, Rule 73(B).

[65]Regulations of the Court, UN Doc. ICC-BD/01-05-16 (6 December 2016), Reg. 26(1)–(2).

[66]Ibid., para. 26(4).

[67]International Criminal Court, Registry, Unified Technical Protocol ('E-court Protocol') for the Provision of Evidence, Witness and Victims Information in Electronic Form, ICC Doc. ICC-01/09-02/11-48-Anx1, available at www.icc-cpi.int/sites/default/files/RelatedRecords/CR2019_00267.PDF (E-Court Protocol).

[68]Ibid.

[69]ICC, 'ICC Prosecutor Karim A.A. Khan KC Announces Launch of Advanced Evidence Submission Platform: OTPLink', 24 May 2023, available at www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink.

[70]Ibid.

international criminal accountability.[71] Until that point, the UN Security Council (UNSC) bore primary responsibility for the creation of international criminal tribunals under its Chapter VII enforcement powers.[72] Given the stalemate often associated with the UNSC,[73] the UNGA opted to establish the United Nations' International, Impartial, and Independent Mechanism for Syria (IIIM) rather than waiting for the establishment of an *ad hoc* criminal tribunal.[74] As such, distinct from international courts, the IIIM was established as a fact-finding body intended to support future criminal trials but without the mandate to prosecute themselves.[75] While authorization by the UNGA offered the IIIM the advantage of a less contentious, and timelier, establishment process, investigative mechanisms are not without their own challenges. Notably within the context of evidence collection, without UN Charter Chapter VII authorization or authorization by the Syrian regime,[76] the IIIM cannot access Syrian territory and is therefore entirely reliant on digital evidence, accessible from outside of Syria, and co-operation from unassociated actors located within, or outside of, Syria.[77]

The establishment of the IIIM was subsequently followed by a number of similar fact-finding missions. Among others, the UNSC established, at the request of the Iraqi Government, the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/Islamic State in Iraq and the Levant (UNITAD) in 2017.[78] The Human Rights Council (HRC) established the Independent Investigative Mechanism for Myanmar (IIMM) in 2018.[79] Finally, most recently, the HRC established an independent, international Commission of Inquiry on Ukraine in 2022.[80] Each of these fact-finding missions, like the IIIM, is distinct from a criminal tribunal in that they have no judicial, but only an investigative, mandate.[81]

The investigative mechanisms are each responsible for the collection, storage, and preservation of their respective materials. Generally, these mechanisms adopt a similar general standard for evidence collection: compliance with international standards.[82] The IIIM publicly describes its procedures as being, 'in accordance with international criminal law standards … [and] tak[ing] appropriate measures to respect and ensure respect for the confidentiality, privacy, interests and personal circumstances of victims, and taking into account the nature of the crime'.[83] Similarly, the IIMM adopts procedures 'consistent with the UN Charter, UN rules, regulations, policies and good practices, relevant international law and jurisprudence, notably the security and well-being of victims and witnesses and the right to a fair trial and other due process provisions'.[84] Finally, UNITAD provides for similar considerations, also providing for the relevance of jurisprudence:

[71]M. Burgis-Kasthala, 'Assembling Atrocity Archives for Syria', (2021) 19 *Journal of International Criminal Justice* 1193, at 1199.

[72]Ibid.

[73]Ibid., at 1200.

[74]General Assembly, International, Impartial and Independent Mechanism to Assist in the Investigation and Prosecution of Persons Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011, A/RES/71/248.

[75]Ibid., para. 4.

[76]IIIM, Report of the International, Impartial and Independent Mechanism to Assist in the Investigation and Prosecution of Persons Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011, A/75/ 311 (2020).

[77]See Burgis-Kasthala, *supra* note 71, at 1201.

[78]Security Council, Security Council Resolution 2379 (2017) [on establishment of an Investigative Team to Support Domestic Efforts to Hold the Islamic State in Iraq and the Levant Accountable for Its Actions in Iraq], S/RES/2379.

[79]Human Rights Council, Situation of Human Rights of Rohingya Muslims and Other Minorities in Myanmar, A/HRC/RES/39/2.

[80]Human Rights Council, Situation of Human Rights in Ukraine Stemming from the Russian Aggression, A/HRC/RES/49/1.

[81]See note 74, *supra*, para. 4; note 78, *supra*, para. 5; note 79, *supra*, para. 22; note 80, *supra*, para. 9.

[82]See notes 83, 84, 85, *infra*.

[83]'Frequently Asked Questions', *International, Impartial, and Independent Mechanism*, available at iiim.un.org/faq/.

[84]'Evidence Collection and Case Building', *Independent Investigative Mechanism for Myanmar*, available at iimm.un.org/evidence-collection-and-case-building/.

> The Investigative Team has adopted procedures for collecting, preserving and storing evidence and materials that are in line with the highest possible standards, consistent with the UN Charter, UN policies and best practice, relevant international law, including international human rights law, notably the right to a fair trial and other due process provisions, as well as the relevant jurisprudence . . . [85]

The mechanisms also provide for a baseline of consideration of storage and preservation of materials, from acquisition until transfer,[86] using electronic databases and other information management tools.[87] While these baseline standards regarding evidence collection and storage are consistent across investigative mechanisms, there remains significant discretion left to the bodies themselves to develop actionable standards and practices for evidence collection.[88]

2.2.2. Private investigative efforts

In addition to the emergence of investigative bodies within the structure of the UN, a number of private organizations, including NGOs, governmental organizations, and educational institutions, have emerged as contributors to the realm of international criminal investigations. NGOs focused on OSINT, such as Bellingcat,[89] the Commission for International Justice and Accountability (CIJA),[90] the Syrian Archive,[91] and WITNESS,[92] among more traditional human rights NGOs such as Amnesty International,[93] TRIAL International,[94] and Public International Law & Policy Group (PILPG),[95] have begun bringing digital evidence investigations into the mainstream. These efforts are augmented by the aid of other similarly motivated institutions, like UC Berkeley School of Law Human Rights Center,[96] the Public Interest Advocacy Centre,[97] the Nuremberg Principles Academy,[98] and the Digital Verification Unit at the University of Essex's Human Rights Centre.[99]

The efforts of these private investigative bodies have made significant contributions to the standardization of investigative standards. Noting the lack of guidelines for the collection and use

[85]'Collect, Store, and Preserve Evidence to the Highest Possible Standards', *Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL*, available at www.unitad.un.org/content/collecting-storing-and-preserving-evidence.

[86]See note 83, *supra*.

[87]See note 84, *supra*.

[88]See generally B. Dvoskin, 'Expert Governance of Online Speech', (2023) 64(1) *Harvard International Law Journal* 85.

[89]'Guides', *Bellingcat*, 2022, available at www.bellingcat.com/category/resources/how-tos/?fwp_tags = osint.

[90]'What We Do', *Commission for International Justice and Accountability*, available at cijaonline.org/model-of-work.

[91]'Methods and Tools', *Syrian Archive*, available at syrianarchive.org/en/about/methods-tools.

[92]'Witness Resources', *WITNESS*, available at www.witness.org/resources/.

[93]'Amnesty International and Advocacy Assembly Launch New Online Courses on Open-source Human Rights Investigations', *Amnesty International*, 15 January 2021, available at www.amnesty.org/en/latest/news/2021/01/amnesty-international-and-advocacy-assembly-launch-new-online-courses-on-open-source-human-rights-investigations/.

[94]J. Sané and K. Yoshida, 'La preuve audiovisuelle devant les instances internationales : techniques et admissibilité', *TRIAL International*, 2019, available at trialinternational.org/wp-content/uploads/2019/12/Manuel-pratique-preuve-audiovisuelle.pdf.

[95]'Human Rights Documentation Solutions: Phase I Report', *Public International Law & Policy Group*, November 2022, available at www.publicinternationallawandpolicygroup.org/hrds-phase-i-report-launch.

[96]See Berkeley Protocol, *supra* note 39.

[97]'Investigating Perpetrators', *Public Interest Advocacy Centre and the UC Berkeley School of Law Human Rights Center*, available at piac.asn.au/wp-content/uploads/2023/03/Investigating-Perpetrators_PIAC-HRC_2023.pdf.

[98]'Digital Evidence', *International Nuremberg Principles Academy*, available at www.nurembergacademy.org/projects/detail/45ed2d129b0e19459764c4684e317a95/digital-evidence-23/; 'Private Investigations in International Criminal Justice', *International Nuremberg Principles Academy*, available at www.nurembergacademy.org/projects/detail/9c75eeaee0bd858dfdaeaca1ead42e55/private-investigations-in-international-criminal-justice-24/.

[99]F. Aahsberg et al., 'Introductory Guide to Open-source Intelligence and Digital Verification', *University of Essex Human Rights Centre Clinic*, 2018, available at www1.essex.ac.uk/hrc/documents/Introductory_Guide_to_Open_Source_Inteligence_and_Digitial%20Verification.pdf.

of digital evidence, the Berkeley Protocol on Digital Open-source Investigations (Berkeley Protocol) created a 'set of minimum standards for the collection, analysis, and preservation of digital open-source information'.[100] Initiated at a point in time when there were no systematized guidelines in place to govern the use of digital evidence, the focus on minimum standards created a common baseline to which investigative bodies could adhere, rather than a set of best practices.[101] Subsequently, Leiden University developed the Leiden Guidelines on the Use of Digitally Derived Evidence (Leiden Guidelines), which seek 'to assist practitioners by comprehensively outlining the essential elements which should be considered before submitting [digitally derived evidence] to an international criminal court or tribunal'.[102] However, these guidelines notably omit discussion of open-source evidence, and particularly social media posts, given the lacuna in jurisprudence on the issue.[103] Given this reality, investigative bodies still have significant discretion to adopt their own practices, resulting in the emergence of varied, albeit broadly stronger,[104] investigative standards, particularly within the realm of open-source evidence.

Further, some investigative efforts provide a uniquely hands-on approach to aiding citizen investigators. EyeWitness to Atrocities, an initiative of the International Bar Association, created a mobile application through which users can record and upload photos, audio, and video.[105] Once uploaded to the application, a master version of the media is saved to a secure server, along with affiliated metadata.[106] EyeWitness's secure server also strives to protect the chain of custody of its evidence.[107] Finally, eyeWitness allows users to upload media anonymously.[108] Once housed in eyeWitness's server, employees can access the material to review and categorize for use in future criminal investigations. CameraV, an application developed by The Guardian Project in collaboration with WITNESS, took a similar approach to documenting citizen investigator's work.[109] However, while applications like eyeWitness and CameraV can serve a meaningful purpose for civilian investigators, it is not a panacea for open-source investigations. The reality is that the average citizen will turn to more familiar applications over specialized investigative applications,[110] and investigative applications were not developed to replace, but rather support, the role of traditional social media outlets.[111] Effectively interfacing with those traditional social media platforms will continue to be an essential component of international criminal investigations, notwithstanding the progress of investigative bodies and other efforts.

[100]D. Murray, Y. McDermott and A. Koenig, 'Mapping the Use of Open-source Research in UN Human Rights Investigations', (2022) *Journal of Human Rights Practice* 1, at 2.

[101]E. Douek and Q. Jurecic, 'Bringing Evidence of War Crimes From Twitter to the Hague', *Lawfare Podcast*, 14 April 2022, available at www.lawfaremedia.org/article/lawfare-podcast-bringing-evidence-war-crimes-twitter-hague.

[102]See Leiden Guidelines, *supra* note 33, Introduction.

[103]Ibid.

[104]CIJA, for example, maintains a policy of collecting both incriminating and exculpatory evidence to safeguard the legitimacy of its practices. See Burgis-Kasthala, *supra* note 71, at 1211.

[105]'eyeWitness User Guide', *eyeWitness*, available at www.eyewitness.global/documents/How-To-Info-Booklet.pdf.

[106]'Using Metadata to Prove the Reliability and Validity of Footage', *eyeWitness*, available at www.eyewitness.global/Using-metadata.

[107]Ibid.

[108]'What Happens When You Upload Footage to EyeWitness to Atrocities?', *eyeWitness*, available at www.eyewitness.global/documents/What-happens-when-you-upload-footage.pdf.

[109]'InformaCam: Verified Mobile Media', *Guardian Project*, available at guardianproject.info/archive/informacam/; L. van der Velden, 'Forensic Devices for Activism: Metadata Tracking and Public Proof', (2015) 2(2) *Big Data & Society* 1.

[110]A. Banchik, 'Throwing Keywords at the Internet: Emerging Practices and Challenges in Human Rights Open-source Investigations', 13 August 2019, available at repositories.lib.utexas.edu/handle/2152/76187.

[111]Interview B, 13 May 2022. Interview with the author (Interview B). While social media platforms were created to facilitate ease in content sharing, investigative applications, like eyeWitness, originated as a means of ensuring authentication from creation. To that end, social media platforms cater to individual users, investigative applications interface primarily with organizations whose focus is creating authentic content.

3. Challenges in digital evidence collection in international criminal law

To date, there remains a number of unanswered questions in the realm of digital evidence in international criminal investigations. Efforts, particularly by private investigative bodies, have contributed significantly to the emergence of standards for the collection of digital evidence. These sources, however, are most instructive to user-generated evidence in the most formal sense: where citizens seek out to collect evidence with the purpose of aiding investigations *ex ante*. As such, there remain particular issues with respect to user-generated evidence that have not yet been sufficiently addressed, either by international courts or investigative bodies.[112]

3.1. Evidentiary standards of admissibility

In addition to the political compromise associated with the formation of international courts, the complex nature of international criminal cases is served well by limited evidentiary constraints. To that end, some practitioners take the view that user-generated evidence is not dissimilar in any meaningful way from more traditional forms of documentary evidence and therefore fits into the pre-existing evidentiary framework established by international courts.[113] However, the reality is that there are particular elements of user-generated evidence that are unique to this type of evidence, and there are a few unanswered questions with respect to the admissibility of user-generated evidence in international courts, namely with respect to anonymous digital evidence and consistency in the preservation of the chain of custody. These questions may well be answered by international courts themselves in due course through case law, but relying on the courts themselves is not the only way to obtain standardization. Consistency in the presentation of evidence to international tribunals could present courts with a reasonable framework for the admissibility of user-generated evidence going forward, allowing investigative bodies to similarly influence admissibility standards without the addition of a formal rule. Irrespective of the final approach taken, a more complete understanding of the role of authorship and chain of custody in the context of user-generated evidence is a crucial step in its admissibility before international courts.

3.1.1. Authorship

The role of authorship of content within the context of admissibility of user-generated evidence raises a number of unanswered questions. The nature of digital evidence, particularly when gathered from an open-source platform rather than directly from an individual, may render the determination of authorship challenging. While content itself may be publicly available, the underlying information, namely the original creator, may not be.[114] Even when the original creator posts content themselves, users may opt to post that evidence anonymously. There are legitimate reasons, both with respect to practicality and privacy,[115] for users to submit evidence anonymously.

Despite international court's preference to date for authored evidence,[116] there are genuine reasons to maintain the anonymity of user-generated evidence. Firstly, in the context of user-generated evidence gathered through open-source investigations, the initial author of digital

[112]These gaps are not exhaustive of the relevant challenges in the field of open-source investigations. The recognition of the role that bias plays in open-source investigations, the techniques and tools needed to verify information, ensuring the equality of arms in the collection of open-source evidence, and the admissibility of illegally obtained but subsequently leaked information, among others, remain largely unaddressed, but are outside of the scope of this article. See Y. McDermott, A. Koenig and D. Murray, 'Open-source Information's Blind Spots: Human and Machine Bias in International Criminal Investigations', (2021) 19(1) *Journal of International Criminal Justice* 85; Freeman, *supra* note 16.

[113]Interview A, 14 April 2022. Interview with the author (Interview A).

[114]L. Laving, 'The Reliability of Open-source Evidence in the International Criminal Court', *Lund University*, 2014, available at lup.lub.lu.se/luur/download?func = downloadFile&recordOId = 4457910&fileOId = 4457912, at 37.

[115]See Berkeley Protocol, *supra* note 39, at 15–16.

[116]*Prosecutor v. Laurent Gbagbo*, Decision Adjourning the Hearing on the Confirmation of Charges, Case No. ICC-02/11-01/11, Pre-Trial Chamber I, 3 June 2013.

evidence may be difficult, if not impossible, to discern.[117] Further, authors of digital evidence are subject to security concerns, in a similar manner as more traditional witnesses.[118] While more traditional witnesses consent, at least to a degree, to involvement the judicial process, the same is not necessarily true for the creators of digital content, particularly of social media posts. While authors of digital evidence may not be obligated to travel, either in-person or virtually, to the seat of a court for the use of their evidence,[119] providing evidence is not without its dangers. Particularly when an author's name is tied to evidence, there are still considerable risks for users posting content that then becomes evidence, from the filming of the incident through to the aftermath of a potential trial.[120] Even when evidence is provided anonymously, determined individuals can use the date, time, and other data to identify the author of the content.[121] Despite the respite that anonymity can provide to authors of user-generated evidence, courts' preference for authored evidence is also mirrored in private investigative efforts' preferences.[122] Given this reality, authorship of content is relevant not only to the admissibility of content but also to the consent of the author to the admission of that evidence.

The question of consent within the realm of open-source evidence remains underdeveloped. While courts have admitted, and referenced, anonymous evidence, particularly in the context of NGO reports with anonymous testimonial evidence,[123] the admissibility of anonymous digital evidence is likely not legally impeded, so long as indicia of reliability[124] can be effectively established without knowledge of the creator. That does not, however, render creator consent irrelevant. The Berkeley Protocol raises additional considerations with respect to creator consent. Implicit in the definition of open-source content is its publicity – the Berkeley Protocol itself defines open-source information as 'publicly available information that any member of the public can observe, purchase or request without requiring special legal status or unauthorized access'.[125] While information may be publicly available on the internet, the data may have been uploaded by a third-party without proper permissions, leading to possible legal and ethical restrictions on its use.[126] For that reason, the Berkeley Protocol recommends that investigators obtain the consent

[117]See Berkeley Protocol, *supra* note 39, at 63. Bellingcat provides an example of the reality of authorship in a digital age. In an initial version of an article, describing the use of video to find an execution, Bellingcat credited Mohammed Al-Ghali as a creator of this content. After Al-Ghali reached out, clarifying that he only reposted the content, Bellingcat added an addendum to the article, clarifying the misrepresentation. 'How a Werfalli Execution Site Was Geolocated', *Bellingcat*, 3 October 2017, available at www.bellingcat.com/news/mena/2017/10/03/how-an-execution-site-was-geolocated/.

[118]See Hamilton, *supra* note 18, at 35–7.

[119]See Mehandru and Koenig, *supra* note 42, at 133.

[120]See Hamilton, *supra* note 18.

[121]S. Dubberley and G. Ivens, 'Outlining a Human-Rights Based Approach to Digital Open-source Investigations: A guide for human rights organisations and open-source researchers', *University of Essex, Human Rights, Big Data and Technology Project*, 30 March 2022, available at repository.essex.ac.uk/32642/.

[122]See Interview B, *supra* note 111.

[123]Ibid.

[124]*Prosecutor v. Bagosora*, Decision on the Request to Admit United Nations Documents into Evidence Under Rule 89 (C), Case No. ICTR-98-47-T, Trial Chamber I, 25 May 2006, para. 4; *Prosecutor v. Bagosora et al.*, Decision on Admission of Tab 19 of Binder Produced in Connection with Appearance of Witness Maxwell Nkole, Case No. ICTR-98-47-T, Trial Chamber I, 13 September 2004, para. 8; *Prosecutor v. Delalic et al.*, Decision on Application of Defendant Zejnil Delalie for Leave to Appeal against the Decision of the Trial Chamber of 19 January 1998 for the Admissibility of Evidence, Case No. IT-96-21, Appeals Chamber, 4 March 1998, para. 18; *Prosecutor v. Kordk and Cerkez*, Decision on Prosecutor's Submissions Concerning 'Zagreb Exhibits' and Presidential Transcripts, Case No. IT-95-14/2-T, Trial Chamber, 1 December 2000, paras. 43-44; *Prosecutor v. Brdanin and Talic*, Order on the Standards Governing the Admission of Evidence, Case No. IT-99-36, Trial Chamber II, 15 February 2002, para. 20.

[125]See Berkeley Protocol, *supra* note 39, at 6.

[126]One such legal restriction is the law of intellectual property. While laws vary across jurisdictions, most jurisdictions provide copyright protections to the creator of content to prevent its subsequent use without the creator's permission. Some jurisdictions offer exceptions to this need for consent; notably, when information is used for socially beneficial purposes, such as law enforcement, creator consent is not needed. However, within the context of international criminal law, the issue of intellectual property and creator content has not been addressed. Ibid., at 6, 29–30.

of the persons involved in the creation of the content.[127] As such, creator consent remains a best practice, if not a requirement,[128] for investigative efforts prior to the use of data.

3.1.2. Chain of custody

A chain of custody is defined as the 'chronological documentation of the sequence of custodians of a piece of information or evidence, and documentation of the control, date and time, transfer, analysis and disposition of any such evidence'.[129] The Berkeley Protocol provides that in order for information to be admissible as evidence, prosecutors and counsel must typically establish the chain of custody of the content.[130] While many forms of evidence require the establishment of a chain of custody as a marker of authenticity, establishment of the chain of custody for digital evidence is particularly technical in comparison.

The chain of custody of digital evidence can be established through two main procedures. The first approach, which replicates a traditional manner of verifying an unbroken chain of custody, relies upon the testimony of the individuals who controlled the possession of the evidence from acquisition through trial.[131] By testifying to the collection, storage, and preservation of the evidence, the chain of custody, and thus the reliability, of the evidence can be established.[132] Alternatively, technology itself can similarly establish the consistency of evidence throughout its lifecycle. When content is removed from a platform, a unique identifier, known as a hash, can be generated.[133] By cross referencing the hash at the time of the acquisition of the content with the hash at the time of presentation to the court, consistency in the two identifiers can demonstrate consistency in the content across time.[134] While both methods can demonstrate an unbroken chain of custody, ensuring that continuity in the first place is a more challenging. The task of ensuring that continuity is based more in policy and practice than in technology, and those practices become more difficult to regulate as the storage of digital evidence becomes more complex.[135] When an original piece is saved locally and subsequently untouched, with access and modification occurring only to a copy,[136] the chain of custody can effectively be maintained without issue. However, given the amount of digital content to which investigative bodies have access, local storage spaces may prove to be insufficient going forward. As investigative bodies turn towards cloud storage for content, new concerns regarding the maintenance of a chain of custody may emerge. Where there is a lack of encryption or a third-party storage platform is used, potential accessors to the content become outside of the control of the investigative body.[137] Given the lack of case law on the subject, it is possible that even opening the access of the content in this manner to external actors may complicate the maintenance of a chain of custody for international courts. For this reason, the question of ensuring effective storage of potential evidence is of the utmost importance.

3.2. Evidence storage

Effective storage of digital information is paramount to its eventual use as evidence. As recognized across international courts, retention and storage of evidence is a foundational requirement of the

[127]Ibid., at 67.
[128]See Interview B, *supra* note 111.
[129]See Berkeley Protocol, *supra* note 39, at 61–2.
[130]Ibid., at v.
[131]See Ashouri, Bowers and Warden, *supra* note 38, at 115.
[132]Ibid.
[133]See Braga da Silva, *supra* note 46, at 15.
[134]Ibid.
[135]See note 95, *supra*.
[136]See Interview A, *supra* note 113; Interview B, *supra* note 111.
[137]Interview B, ibid.

judicial process.[138] For international courts, effective storage of evidence permits judges to make informed decisions regarding weight at the conclusion of a trial.[139] For investigative bodies, effective storage of information will permit its subsequent use in a criminal trial by avoiding manipulation and ensuring continuity in the chain of custody. Given the volume of potential evidence that is being generated in the context of modern conflict, ensuring effective storage and access of those materials is paramount to the eventual increased use of user-generated evidence before international courts.

3.2.1. Storage of evidence

A prominent issue with the use of open-source evidence is the sheer volume of content. Storage of content comes at significant financial cost, requiring investigative bodies to make difficult decisions regarding storage. For some, with particularly stretched budgets, in-house preservation is impossible, and evidence is maintained only to the extent that it remains accessible online.[140] For others with more resources to dedicate to the preservation of evidence, tools of preservation include both internal and third-party resources.[141] Internally, investigators save certain files locally on their own computers, or re-upload them to personal YouTube or Vimeo accounts for, at least temporary, safeguarding.[142] Externally, platforms such as Google Drive or the Internet Archive's Wayback Machine offer cost-effective mechanisms for storing data.[143] Finally, bodies with the most resources can create customized, or original, platforms for storage. By creating a private, encrypted storage platform, investigative bodies can most effectively store and protect information.[144] The Syrian Archive, for example, is working proactively to compile an archive of open-source information. By scraping platforms for relevant content, the Syrian Archive is able to store potential evidence in advance of the opening of a formal investigation.[145]

Given the budgetary and operational differences between investigative bodies, the evidence storage and management platforms similarly vary significantly. Even more concerningly, evidence storage practices can vary within those individual organizations. Practitioners suggested that a lack of standard operating procedures (SOPs), even internally, creates *ad hoc* storage policies.[146] A lack of standardized storage procedures can render subsequent analyses of data more difficult to conduct, result in duplication of materials, and may even compromise the evidence itself. Given these realities, ensuring more standardized storage policies should be a priority for investigative bodies.

3.2.2. Access of evidence

Once evidence is maintained in a repository, there are a number of unanswered questions with respect to the access of that information. In the simplest of storage options, where information is held in-house on a local hard drive, access of evidence is similarly simple and can be limited to employees of an investigative body. With any added complications, however, that access can become more contentious.

The danger of ubiquitous access to evidence is twofold. Firstly, the access of evidence can raise important ethical concerns. The 'Do No Harm' principle acknowledges that any international

[138]See Section 2.1.3, *supra*.

[139]Ibid.

[140]A. Banchik, 'Disappearing Acts: Content Moderation and Emergent Practices to Preserve At-Risk Human Rights-Related Content', (2021) 23(6) *New Media & Society* 1527, at 1536.

[141]Ibid.

[142]Ibid., at 1537.

[143]Ibid.

[144]See Interview B, *supra* note 111.

[145]See Banchik, *supra* note 140, at 1532.

[146]See Interview A, *supra* note 113.

involvement into conflict becomes part of that conflict and therefore produces both negative and positive impacts.[147] Under the principle, any intervener should minimize any potential, even if inadvertent, harm they may cause.[148] Within the context of open-source investigations, and more specifically the access of that information, the primary potential harm is the violation of the right to privacy. The right to privacy is established in a variety of domestic and international sources and is laid out in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), stating that '[n]o one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon their honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.[149] Investigators' use, even of publicly posted information, of digital content, particularly in a subsequent criminal trial, may constitute a violation of the right to privacy.[150] In order to respect that right, investigators must strive to obtain the informed consent[151] of the content creator when possible, acknowledging that evidence may be promulgated anonymously, rendering the acquisition of informed consent difficult, if not impossible, in certain contexts.

A violation of the right to privacy is not only problematic with respect to individual rights but also to the admissibility of any associated evidence. As laid out in Article 69(7) of the Rome Statute, evidence obtained in violation of a human right may preclude its admissibility.[152] The right to privacy, as an internationally recognized human right,[153] would fall within the purview of this article. However, the Court has provided additional insight into which violations would be sufficiently severe to justify exclusion. A violation of a right only affects the reliability of evidence where full respect to that right would have resulted in a difference in the content of the evidence.[154] In the case of a violation of the right to privacy in the context of open-source evidence, digital content would be consistent, regardless of whether it was obtained in respect or in violation of that right.[155] To that end, the right to privacy in the context of open-source investigations would likely not preclude the admissibility of digital evidence under Article 69(7), though a definitive answer to the question is unclear until international courts are in a position to address the question.

Further to protections of the right to privacy, ubiquitous access to digital information raises concerns with respect to the safekeeping of any potential evidence. Access to information necessitates a balance between the benefits that increased access to materials provide and the security of any potential evidence. Without the ability to share information, investigative bodies are likely to be overlapping, if not repeating, the work of their counterparts. Given the budgetary restraints associated with each of these organizations, avoiding this duplication would serve those organizations, as well as the broader international criminal justice community, more effectively. Overbroad access, on the other hand, would counter efforts to reduce duplicative work. If hostile actors have access to potentially valuable evidence, the content could be subject to alteration or removal, precluding its future use as evidence.[156] As with evidence storage more broadly,

[147]M. Anderson, Do No Harm: How Aid Can Support Peace – Or War (1999).

[148]Ibid.

[149]1966 International Covenant on Civil and Political Rights, 999 UNTS 171 (ICCPR).

[150]Q. Eijkman and D. Weggemans, 'Open-source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability?', (2013) 24(4) *Security and Human Rights* 285, at 292.

[151]Informed consent consists of four component parts: notice or disclosure, capacity or understanding, voluntariness, and competence. Z. Rahman and G. Ivens, 'Ethics in Open-source Investigations', in S. Dubberley, A. Koenig and D. Murray (eds.), *Digital Witness: Using Open-source Information for Human Rights Investigation, Documentation, and Accountability* (2020), 249.

[152]See Rome Statute, *supra* note 21, Art. 69(7).

[153]See ICCPR, *supra* note 149. The right to privacy has also been recognized as an internationally recognized right in ICC case law. See Bemba Decision on Requests to Exclude, *supra* note 35, paras. 10, 14, 30.

[154]*Prosecutor v. Thomas Lubanga Dyilo*, Decision on the admission of material from the 'bar table', 24 June 2009, Case No. ICC-01/04-01/06-1981, Trial Chamber I, paras. 85–86.

[155]See Laving, *supra* note 114, at 27.

[156]See note 95, *supra*.

investigative bodies weigh these competing interests differently, resulting in a range of strategies regarding the sharing of information. Some organizations emphasize the security of their content, by opting to collect and store data locally, disconnected from the internet.[157] Despite the importance of ensuring the security of content, there is an increasing recognition among investigative bodies that there is a need for further co-ordination and co-operation – a feat which is only possible with increased access to potential evidence.

3.3. Corporate reliance

Within the realm of evidence obtained from social media platforms, investigative bodies are largely reliant on the platforms themselves to obtain crucial information.[158] That reliance presents itself in two main contexts: firstly, social media platforms have significant control over the scope and enforcement of their content moderation policies, resulting in the potential loss of valuable evidence; and secondly, access to that removed content, and underlying metadata of both removed and public content, is similarly controlled by the platforms themselves. In order to make use of the wealth of potential evidence privy to social media platforms, investigative bodies should aim to establish co-operative policies with these corporations.

3.3.1. Content moderation policies

Content moderation is defined as 'the process by which Internet companies determine whether user-generated content meets the standards articulated in their terms of service and other rules'.[159] In response to increasing levels of extremist content, voluntary agreements[160] and punitive measures[161] entice social media platforms to strengthen their moderation policies.[162] The legal obligations binding content moderation policies are quite limited,[163] so as evidenced by the definition itself, each platform can, and does, establish its own standards for content moderation.[164] Content moderation can be conducted in two broad contexts: *ex post* or *ex ante* posting.[165] Users of a platform can flag content for removal once posted, known as *ex post* moderation, and the platforms' content moderators will review a user's flagging against the platform's policies to verify content's violation of or alignment with the policies. Flagging, and review, for removal is not only performed by individuals but is increasingly automated.[166]

In the context of *ex post* moderation, investigators can, at least potentially, access and preserve content prior to its flagging and subsequent removal. In order to ensure the preservation of evidence, investigators are their own best resource at present: 'you can't trust others to ensure its existence'.[167] Ensuring preservation by an individual investigator, however, is easier said than

[157]Ibid.

[158]See generally R. Hamilton, 'Future-Proofing U.S. Law for War Crimes Investigations in the Digital Era', (2023) 57(4) *Georgia Law Review*.

[159]Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/38/35 (6 April 2018), at 3, fn. 2.

[160]See Banchik, *supra* note 140, at 1530.

[161]Ibid.

[162]Ibid.

[163]H. Hubley, 'Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations', (2022) *International Criminal Law Review* 1, at 4.

[164]Ibid.

[165]Ibid., at 6.

[166]See Hubley, *supra* note 163, at 7.

[167]See Banchik, *supra* note 140, at 1535.

done. Generally, social media platforms do not permit direct downloads from their website;[168] investigators, rather, have to rely upon external websites or software to download content.[169] The introduction of a third-party software potentially raises complications regarding the maintenance of the chain of custody, but without case law on the precise issue, it remains an open question as to how courts will treat evidence downloaded through such a platform. In addition to downloading content, investigators can also create stable links to the content, or simply capture a screengrab, though both of these options introduce the possibility of losing the metadata associated with the content.[170]

Ex ante moderation of content, on the other hand, presents particular difficulties for international criminal investigations. While investigators notably aim to save information as soon as possible, where content is moderated prior to posting, an investigator loses the opportunity to access evidence. At present, social media platforms are neither required to disclose their moderation policies nor moderated content.[171] The relevance of the loss of moderated content prior to posting relies largely on the platform's moderation policies and those influencing them. While content moderation is likely a necessary safeguard in a world of misinformation and content inciting crimes, they can also be assumed for nefarious purposes. In addition to civilian users or platform employees flagging content for removal, state actors have also taken advantage of moderation policies.[172] Through a variety of mechanisms, including formal requests, governmental referral units, and more inventive tactics, state actors have the capacity to directly influence the moderation of content.[173] Outside of this direct involvement in content moderation, given the flexibility of moderation policies, state actors often exercise political force to shape these policies.[174] The involvement of state actors in the regulation of social media platforms is neither surprising nor unwarranted, but there are indications that the moderation of content by state actors does not always result in expected outcomes. In examples raised by practitioners, there have been cases where content showing military vehicles or weapons, but was otherwise nonviolent, was removed, whereas violent content without those state connections was left untouched, raising suspicions of state involvement in content moderation.[175] Particularly within the realm of atrocity crimes, where state actors are often directly or indirectly involved in the perpetration of crimes, state actor's involvement in the moderation of potential evidence in these cases raises significant concern.

3.3.2. Investigative access to content

In light of the necessity of content moderation, and the reality that social media platforms will continue to moderate their content, investigative bodies must work co-operatively within that framework. Social media platforms are privy to a large repository of valuable information – even in the case of a lack of publicly available metadata, it may still be accessible, at least for a period of time.[176] Social media companies maintain a repository of metadata of uploaded media, but the preservation of that content is neither uniform nor particularly clear.[177] Under

[168]Directly downloading content from social media platforms is generally a violation of their terms and conditions and is also possibly a copyright violation. Ibid., at 1535–6.
[169]Ibid.
[170]See Hubley, *supra* note 163, at 17.
[171]See Banchik, *supra* note 140, at 1534.
[172]Ibid., at 1533.
[173]Ibid.
[174]Ibid., at 1534.
[175]Ibid., at 1534–5.
[176]See Hubley, *supra* note 163, at 8–9.
[177]Ibid.

Article 54(3)(f) of the Rome Statute, the Prosecutor is authorized to take measures, or request that measures be taken, to preserve evidence.[178] As such, the Prosecutor has the ability to request that social media platforms preserve evidence, but this avenue remains discretionary, as well as limited.

In order to reduce costs associated with data storage and increase the accessibility of data, social media platforms make use of cloud computing.[179] Rather than storing data on a local hard drive in a singular location, data is stored in centres in multiple countries.[180] Traditionally, prosecutors rely on Mutual Legal Assistance Treaties (MLATs), which are bilateral frameworks for co-operation in law enforcement,[181] to access and collect extra-territorial evidence. MLATs are, however, designed for use by states and, given their bilateral nature, can vary between jurisdictions. Further, unlike more traditional forms of evidence, within the realm of cloud computing, prosecutors likely need to make use of multiple MLATs to access all needed data.[182] Given the lack of standards for MLATs, co-ordinating data collection across jurisdictions for a state prosecutor is a challenging undertaking.

For international courts and investigators working outside the framework of states, the process for accessing data is even less regulated. Under Rule 104(2) of the ICC RPE, the Prosecutor may seek additional information from third parties, including 'States, organs of the United Nations, intergovernmental and non-governmental organizations, or other reliable sources'.[183] As such, international tribunals can directly request information from social media platforms.[184] The willingness of platforms to comply with those requests is, however, a manner of internal policy, which is 'largely a matter of company discretion'.[185] For civil society organizations, the avenues for co-operation with social media platforms are more limited still.[186] The existing legal avenues for content sharing between investigative bodies and social media platforms leaves investigative bodies largely reliant on the platforms for co-operation.

4. Standardizing open-source investigations

Despite the ongoing work of public and private investigative bodies alike, the most significant issue to the admissibility of open-source evidence is the *ad hoc* nature of investigations. International courts' treatment of authorship and chain of custody in the admissibility and weight of potential evidence will likely be assessed on a case-by-case basis in the immediate future. Across investigative bodies and courts, the practices for the storage of evidence and the subsequent access of that information vary significantly. Similarly, social media platform's content moderation policies and co-operative policies with law enforcement and civil society differ. Creating standardization across these gaps will strengthen the admissibility and the quality of potential evidence for international criminal investigations.

Scholars, in the wake of the establishment of a handful of *ad hoc* investigative mechanisms, have begun considering the establishment of a Standing Independent Investigative

[178]R. Costello, 'International Criminal Law and the Role of Non-State Actors in Preserving Open-source Evidence', (2018) 7(2) *Cambridge International Law Journal* 268, 273.

[179]M. Watney, 'Law Enforcement Access to Evidence Stored Abroad in the Cloud', (2016) *European Conference on Cyber Warfare and Security* 288.

[180]Ibid., at 288.

[181]Ibid., at 290.

[182]Ibid.

[183]See ICC RPE, *supra* note 58, Rule 104(2).

[184]See Douek and Jurecic, *supra* note 101.

[185]K. Westmoreland, 'Are Some Companies "Yes Men" When Foreign Governments Ask for User Data?', *Stanford Law School Center for Internet and Society*, 30 May 2014, available at cyberlaw.stanford.edu/blog/2014/05/are-some-companies-yes-men-when-foreign-governments-ask-user-data.

[186]M. Rajagopalan, 'The Histories of Today's Wars Are Being Written on Facebook and YouTube. But What Happens When They Get Taken Down?', *BuzzFeed News*, 22 December 2018, available at www.buzzfeednews.com/article/meghara/facebook-youtube-icc-war-crimes.

Mechanism.[187] Similarly to the considerations that preceded the establishment of the ICC, co-ordinating international investigations in a singular mechanism may serve the international community more effectively than the continued establishment of *ad hoc* investigative mechanisms. Currently, human rights activists, journalists, and lawyers are all contributing to open-source investigations. Creating a centralized investigative mechanism would ensure that all information gathered would be geared towards a trial standard, rather than the standards associated with advocacy or journalist. Further, by co-ordinating investigations, a standing mechanism could avoid repetition of work, both in and across investigations. At present, when a new investigative mechanism is established, there are significant financial costs and time restraints associated with its start-up – funding, staff, and systems must be acquired prior to the initiation of any investigative work.[188] With a standing mechanism, the administrative and organizational framework would already be in place when a situation arises meriting further investigation, allowing for more cost-effective and timelier investigations.

An underexamined benefit of a standing investigative mechanism is the role it could play in standardizing the collection and use of open-source evidence. A number of scholars have called for a collective repository of digital evidence, also referred to as a digital locker.[189] The idea of a digital locker is not only compatible with, but would be a crucial component of, a standing investigative mechanism. On a smaller scale, some organizations have begun operationalizing the idea of an evidence repository. Within the context of the European Union, Europol is working to develop a database for international crimes, through which members can request and share evidence between national law enforcement agencies.[190] Similarly, the Syrian Archive has created a repository of content related to human rights abuses committed in Syria.[191] By co-ordinating the storage of content, the Syrian Archive has been able to efficiently filter and cross-reference data, allowing for a more effective conceptualization of the scale and scope of incidents.[192] Using these initiations as a model for the broader international criminal justice community, a standing international investigative mechanism can offer a framework through which a digital locker could be established.

Co-ordinating investigations into a singular mechanism could also alleviate some of the pressures associated with investigative work. Access to funding is a significant concern for investigative bodies broadly[193] – secure storage solutions are expensive to implement, and scarce resources can preclude the existence of an effective data management system.[194] Allowing investigative work to share resources, including hardware, storage space,[195] and staff, would allow

[187]K. Abbott and S. Zia-Zarifi, 'Is It Time to Create a Standing Independent Investigative Mechanism (SIIM)? Part I', *OpinioJuris*, 10 April 2019, available at opiniojuris.org/2019/04/10/is-it-time-to-create-a-standing-independent-investigative-mechanism-siim/; C. Hale and L. Sadat, 'How International Justice Can Succeed in Ukraine and Beyond', *JustSecurity*, 14 April 2022, available at www.justsecurity.org/81086/how-international-justice-can-succeed-in-ukraine-and-beyond/.

[188]Ibid.

[189]UC Berkeley Human Rights Center, 'Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes', 2021, available at humanrights.berkeley.edu/sites/default/files/digital_lockers_report5.pdf.

[190]E. Baker et al., 'Joining Forces: National War Crimes Units and the Pursuit of International Justice', (2020) 42(3) *Human Rights Quarterly* 594, 614.

[191]J. Deutch and H. Habal, 'The Syrian Archive: A Methodological Case Study of Open-Source Investigation of State Crime Using Video Evidence from Social Media Platforms', (2018) 7(1) *State Crime Journal* 46, 51.

[192]Ibid.

[193]See note 95, *supra*.

[194]Ibid.

[195]Partnerships between international criminal bodies and technology organizations date back to the first international criminal tribunal. IBM created a technology for simultaneous interpretation specifically for the Nuremberg Trials, which is still used by the UN today. See Freeman, *supra* note 16, at 300. Similar collaborative efforts between software companies and an investigative mechanism would enhance the use of software and storage. By adopting an ongoing partnership, the provenance and chain of custody of evidence stored with the software company could be more readily established before international courts than with *ad hoc* storage solutions.

even a limited budget to go further than it would on an *ad hoc* basis. Further, by co-ordinating work internally within one framework, a standing mechanism could also more effectively create a shared SOP for documentation, storage, and analysis of digital evidence.

By having a centralized investigative body, co-operation with social media platforms would also be streamlined. Given the lack of official avenues for co-operation with non-state actors,[196] investigative bodies are forced to work on an *ad hoc* basis, largely subject to the acquiescence of social media platforms. While a standing investigative body would not be privy to more official co-operative measures, it would allow for a singular set of agreements between the investigative mechanism and social media platforms. Under a memorandum of understanding, such as those entered into by select states or corporations and the ICC,[197] a more official agreement could bind social media platforms to share content and affiliated information with the investigative body, subject to certain conditions. The terms under which information would be shared, such as who could request it, what categories of content could be shared, and how intellectual property, privacy, and national security laws would be implicated, are likely to be contentious, though the prospect of undergoing those negotiations for one investigative mechanism is more palatable than the alternative.

Additionally, a standing investigative mechanism could facilitate the equality of arms. The principle of equality of arms is a crucial component of any fair trial.[198] Given the inherent power imbalance associated with the Prosecution's initiation of a case, in addition to the practical imbalance in resources, the ICC enshrined protections in the Rome Statute to attempted to alleviate this tension, particularly with respect to the collection of evidence: namely, the Office of the Prosecutor has a duty to investigate both incriminating and exonerating circumstances equally,[199] and to disclose any evidence material to the preparation of the defence.[200] While these protections are crucial, they are minimum standards and do not fully remedy the power imbalance. By creating a standing mechanism, defence counsel could access a full repository of evidence, and associated metadata, allowing for a more streamlined sharing of evidentiary materials at lower cost to all parties.

A centralized investigative body could also aid in the rise of domestic prosecutions of atrocity crimes and strengthen the complementarity of the Court. One practitioner expressed a need not only for standardized investigations but also a replicable investigative framework.[201] Given the linguistic, cultural, and budgetary considerations associated with investigations, even a standing mechanism would involve co-operation with other bodies and could not be exhaustive of all potential investigations. To that end, being able to export the processes created by a standing mechanism would serve domestic prosecutions by allowing for a timelier initiation of, and more effective, investigations.

Despite the role it could play in standardization, a standing investigative mechanism is certainly not a panacea to investigative standardization. The establishment of a standing mechanism would be a feat of significant political will, not without questions of its own. As with

[196]See Section 3.2.2, *supra*.

[197]E.g., International Criminal Court, Press Release, 'ICC - The Registrar Signs a Memorandum of Understanding Regulating the Establishment and Functioning of the Court on the Territory of the Central African Republic', ICC Doc. ICC-20071018-255, available at www.icc-cpi.int/news/icc-registrar-signs-memorandum-understanding-regulating-establishment-and-functioning-court; International Criminal Court, Press Release, 'ICC Prosecutor and World Bank Vice-Presidency to Cooperate on Investigations', ICC Doc. ICC-OTP-20091012-PR462, available at www.icc-cpi.int/news/icc-prosecutor-and-world-bank-vice-presidency-cooperate-investigations.

[198]See, *inter alia*, Universal Declaration of Human Rights, UNGA Res. 217A(III), UN Doc. A/810 (1948), Arts. 10–11; see ICCPR, *supra* note 149, Art. 14; 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and No. 14, ETS 5 (1950), Art. 6; 1969 American Convention on Human Rights, 1144 UNTS 123 (1969), Art. 8; 1981 African Charter on Human and Peoples' Rights, 1520 UNTS 217 (1981), Art. 7.

[199]See Rome Statute, *supra* note 21, Art. 54(1)(a).

[200]Ibid., Art. 67(2).

[201]See Interview A, *supra* note 113.

any investigative body, policies would need to be developed regarding a number of standards – some questions include which conflicts would merit investigation and storage of potential evidence, and how they would be referred to the mechanism; how, and what, evidence would be transmitted to judicial bodies; what platform would be best suited to handling the storage of data; and what work processes would govern the handling, verification, and canvassing of potential evidence. Most crucially, a standing mechanism would require a significant amount of funding, and it would likely be reliant, like the ICC, upon voluntary contributions.

Further, the creation of an investigative mechanism and an associated evidence repository would not preclude the existence of other investigative bodies. Those investigative bodies would likely be served by the work of the standing mechanism, given its role in the increased standardization of best policies and practices, but many of the existing constraints faced by investigative bodies would endure. Notably, private investigative bodies would still face significant barriers to content sharing with social media platforms. While working with the standing mechanism may encourage social media platforms to increase content sharing with civil society more broadly, the reality is that the collaboration would still be on the platform's terms. Investigative bodies would still face budgetary and storage concerns internally, but the existence of a standing mechanism could serve as a partial solution to those challenges, given the fact that bodies could outsource their storage needs to the mechanism, facilitating both a budgetary ease and increased co-operation amongst bodies. While a standing investigative mechanism would not alleviate all challenges faced by investigative bodies at present with respect to the lack of standardization, the contribution it could make to the efficiency and effectiveness of the international criminal justice community, particularly within the realm of open-source evidence, is significant.

5. Conclusion

As user-generated evidence continues to emerge from the landscape of the modern conflict, it is only a matter of time before international courts have to face difficult questions regarding the use of digital evidence. Given the relative novelty of digital evidence before international courts, case law and statutory rules provide limited guidance. Investigative bodies, therefore, have driven the determination of the future role, and standards for admissibility, of digital evidence. Despite the progress made by these investigative bodies, the work has been largely unco-ordinated, resulting in a range of best practices and guidelines in the realm of open-source evidence.

While the RPEs and statutes of international courts provide broad guidance for the admissibility of evidence, the particulars of digital evidence leave uncertain its future role in international criminal cases. Particularly with respect to the role of authorship and the establishment of the chain of custody in the digital realm, without specific guidance from evidentiary rules, the standards of admissibility for digital evidence remain both discretionary and uncertain until international courts face these questions directly.

Even in the absence of direct guidance on the standards for admissibility of digital evidence, there are steps the investigative community can take to pave the way for its eventual use in court. Ensuring adequate storage of digital evidence will protect the chain of custody of evidence while avoiding potential manipulation to the content. Reaching consensus on the access of that stored information – notably, who and under what circumstances – will require balancing the need for increased co-operation between investigative bodies and the need to protect the creators of content and evidence itself from harm.

Finally, enabling the admissibility of digital evidence requires access to the evidence in the first instance. Currently, social media platforms have access to, and are in control of, a vast amount of data. The use of content moderation policies endangers the loss of potentially crucial evidence. Challenges to obtaining access to that content and affiliated information is a significant roadblock

to the potential role of digital evidence. Establishing a co-operative regime with social media platforms must be a priority for investigative bodies going forward.

Broadly, the international criminal investigative community would benefit from increased standardization. With a range of unanswered questions, unco-ordinated efforts have led to *ad hoc* approaches by investigative bodies. The prospect of creating a standing international, investigative mechanism will enable this standardization, by allowing a singular investigative body to guide the creation of best practices for the collection, storage, access, and use of digital evidence. Using this model of a standing investigative mechanism, the field of international criminal justice could facilitate increasingly effective and efficient investigations in the face of the novel challenge, and opportunity, of digital user-generated evidence.

Cite this article: White E (2024). Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism. *Leiden Journal of International Law* **37**, 228–250. https://doi.org/10.1017/S0922156523000444