Cambridge International Law Journal, Vol. 7 No. 2, pp. 268–283

# International criminal law and the role of non-state actors in preserving open source evidence

Róisín A Costello
Trinity College Dublin, Ireland

*This article analyses the current duties of non-state actors, specifically digital platform providers, to preserve and report content useful in the later prosecution of international criminal offences. The article illustrates the shortcomings of current legal mechanisms both at an international and national level by which such duties to preserve and/or report are imposed and proposes solutions which countenance a more developed role for the International Criminal Court in collecting and preserving open source evidence independent of non-state actor cooperation.*

**Keywords:** *international criminal law, open source evidence, non-state actors, subjects*

## 1 INTRODUCTION

In August 2017, YouTube removed several thousand video files from its platform as well as an unspecified number of user profiles. The content was automatically flagged and removed by the platform's algorithmic system which was reprogrammed to detect and remove content which violated the platform's 'Community Guidelines' as a result of being deemed to constitute inappropriate or extremist content. Many of the files removed documented the Syrian conflict including evidence of alleged international crimes as well as content which constituted a significant contribution to the historic record of the conflict.

While Syria is currently beyond the jurisdiction of the International Criminal Court (ICC),[1] the case raises a timely prompt to reflect on the duties of non-state actors (NSAs), specifically digital platform providers, to preserve and report content potentially relevant in subsequent international criminal prosecutions. For the purposes of this piece, such content will be referred to as open source evidence. This evidentiary category includes information and sources of information made by and available to the public through the use of public communication platforms and products and social media.[2]

As this article will examine, the ICC has demonstrated a willingness to engage with open source evidence. However, the dominance of NSAs both in controlling the access to and the preservation of this evidence is troubling, as the YouTube example

1. Despite Syria's status as a non-party, the ICC could obtain jurisdiction over Syria through a United Nations Security Council referral or an 'ICC referral', which would grant the Court retroactive jurisdiction to the day the Rome Statute entered into force, on 1 July 2002. The Security Council has referred situations to the ICC only twice, regarding Darfur in Sudan in 2005 and Libya in 2011.
2. Keith Hiatt, 'Open Source Evidence on Trial' (2016) 125 Yale Law Journal Forum 323, 323.


Journal compilation © 2018 Edward Elgar Publishing Ltd
The Lypiatts, 15 Lansdown Road, Cheltenham, Glos GL50 2JA, UK
and The William Pratt House, 9 Dewey Court, Northampton MA 01060-3815, USA

illustrates, and requires a means by which the ICC may either negate such a disproportionate influence or restrict its exercise.

In seeking to identify such a means of curtailing or circumscribing NSA dominance, the article will contend that neither direct action from the ICC through existing avenues nor intervention by States parties are sufficiently effective. The article therefore contends that the most viable solution is the development by the ICC of a means of proactive collection and solicitation of evidence. This would be accomplished through a popularly available system for submission of content from civilians and other interested parties in signatory states.

## 2 CONTEXT FOR THE EXAMINATION

The use of digital platforms and social media to document conflict and subsequent human rights abuses has increased steadily in the last decade. This trend has been fed by access to consumer goods with high quality recording and photography capabilities, as well as the greater availability of high-speed internet connections. Combined with a successful use of social media and digital platforms to agitate for political and social change there has been an increase in civilian use of digital recording and social media to document government action and civil unrest. The result has been a historic record of early twenty-first century conflicts which, with limited exception, is held and controlled by digital platform providers.

The importance of identifying a means of preserving open source evidence lies in this increasing prevalence of digital evidence and the predominantly digital record of modern conflict. This is particularly the case in conflicts characterised by the exclusion of third parties, including international media and human rights actors, from considerable areas of the conflict zone. This has been the case in Syria[3] where foreign observers' ability to monitor the conflict has been curtailed in significant portions of the country as a consequence of sieges by pro-government forces as well as actively hostile tactics employed by rebel groups towards foreign actors.[4]

In this context the importance of open source evidence has been elevated from supplementary to critical in establishing the events which take place in 'closed' conflict zones. Problematically, the augmented importance of open source evidence is not mirrored in the practical treatment of such content by digital platform providers which have adopted preemptive approaches to the deletion of content.

As a result of divergences in intermediary liability between jurisdictions, digital platform providers experience a functional incentive to delete content. In Europe, national approaches vary,[5] but follow, with varying degrees of stringency, the position endorsed by the European Court of Human Rights, in *Delfi v Estonia*.[6] This is a

3. 'Syria's War: Reporter's Nightmare', *The Economist* (London, 21 October 2013) <https://www.economist.com/news/middle-east-and-africa/21588121-difficulty-reporting-rebel-areas-has-let-regime-tell-its-own> accessed 26 July 2018.
4. 'Human Rights World Report 2017: Syria Events of 2016', Human Rights Watch (2017) <https://www.hrw.org/world-report/2017/country-chapters/syria> accessed 26 July 2018.
5. See, for example, the 2017 German Network Enforcement Act (*Federal Law Gazette*, 1 September 2017).
6. *Delfi AS v Estonia* App no 64569/09 (ECtHR, 10 October 2013) (imposed liability on intermediaries for defamatory comments posted on their site by anonymous third parties).

divergence from the approach of the United States which has, to date, favoured broad exemptions from liability for digital intermediaries.[7]

As a result of such divergences, digital platform providers experience a functional incentive to employ algorithms, as well as individual content monitors, to preemptively flag and remove content deemed offensive or inappropriate in response to user reports as well as on an independent basis. Such behaviour is designed, in part, to avoid a need for individualised jurisdictional responses to material which might attach liability for the platform providers. Digital platform providers thus seek to reduce compliance costs by adopting the narrowest definition of permissible content. In employing such preemptive removal models, platforms exercise significant control over open source evidence while obviating the liability associated with its content. The result is that large volumes of evidence useful to later international criminal prosecutions are vulnerable to deletion.

## 3 A PROBLEM OF SUBJECTS

The inability of the ICC to ensure NSAs do not destroy, or to require NSAs to actively report, content useful in later international criminal prosecutions is the result of the traditional articulation of international law as the contractual relation between states. Under this conceptualisation, NSAs, in particular the corporate entities considered in this piece, are not considered subjects of the international legal system and are thus not bound by its requirements.[8]

Underlying the subjects-based model is a duplication of the national commitment to the public/private law distinctions in which only public actors (the state) are bound by the obligations, contractual in nature, which are imposed by the citizen–state relationship manifested within national constitutional documents. Such contractual relationships are predicated on a classical understanding of the character of, and the relationship between, the state and its subjects which views the state as the primary threat to the liberty of the individual.

In such circumstances, the public/private law distinction is both useful and necessary in delineating the obligations of the state in respect of its citizens. More fundamentally, the distinction limits the ability of the state to regulate the actions of private individuals in their interactions with each other. This understanding has subsequently been transposed to an international context.

The contours of this contractual state–subject model reflect the understanding of the roles of the state and citizen in seventeenth- and eighteenth-century Europe. However, they fail to appreciate the contemporaneous ability of NSAs to monopolise power over social groups and the extent to which individual rights may be vindicated or eroded through their terms of service and operational models.[9] This is particularly in evidence at an international level where the process of globalisation has been both fragmented and contradictory.

7. Intermediary liability is excluded under US law most notably through Communications Decency Act, s 230 and the Digital Millennium Copyright Act, s 512.
8. August Reinisch 'The Changing International Legal Framework for Dealing with Non-State Actors' in Philip Alston (ed), *Non-State Actors and Human Rights* (OUP, Oxford 2005) 37.
9. See, for example, Dimitra Kamarinou, Christopher Millard and W Kuon Hon, 'Privacy in the Clouds: an Empirical Study of the Terms of Service and Privacy Policies of 20 cloud service providers' (2015) 209 Queen Mary School of Law Legal Research Paper Series <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646447> accessed 26 July 2018.

The process has strengthened the power of individual states or states-groups while simultaneously enabling the rise of NSAs whose influence on the democratic process and individual rights has been significant.[10] The complex landscape which has resulted does not mirror the neat binary of governing and governed axiomatic in constitutional theory and transposed to the international order.[11]

The subjects-based articulation of international law has been repeatedly interrogated – notably by Clapham, who has questioned whether such binary axioms could endure in an international arena increasingly dominated by influential, international NSAs.[12] Elsewhere, Alston has noted this and queried whether the analytical frameworks underlying the subjects' model of international law must expand. Such an expansion is necessary, according to Alston, to account for the expanded range of actors implicated in the modern international legal landscape and with the result that normative frameworks must also be expanded.[13]

This subjects-based model complicates open source evidence collection by limiting the ability of international actors, in this case the ICC, to deal directly with NSAs. Under the model, international actors deal with NSAs as part of the relevant government's obligations to ensure its own compliance with those international treaties to which it is a party.[14]

This is substantively damaging to the assurance of international legal protections and in the context of this paper raises significant issues in imposing liability on NSAs to preserve and report content relevant to international criminal prosecutions. As a result, the paper now turns to examine the powers of the ICC in investigating and securing evidence through obligations of States parties.

## 4 EVIDENCE AND INVESTIGATION AT THE ICC

The ICC has displayed an explicit willingness to consider open source evidence in a series of orders and decisions, as this section will examine. Given the value attached to open source evidence by the ICC and the obstacle posed by the subjects-based articulation of international law, the section will then turn to analyse the power of the ICC to impose duties to report or preserve evidence on NSAs through States parties.

### 4.1 The use of open source evidence at the ICC

The ICC has recognised the need to engage with open source evidence, in particular social media, which it referred to in its 2016–2018 Strategic Plan, as a 'coming storm'.[15] While

10. See generally Andrew Clapham, *Human Rights Obligations of Non-State Actors* (OUP, Oxford 2010); Anne-Marie Gardner, 'Beyond Standards before Status: Democratic Governance and Non-State Actors' (2008) 34(3) Review of International Studies 531; Neli Frost, 'Transnational Corporations as Agents of Legal Change' (2016) 5(3) Cambridge Journal of International and Comparative Law 502; Oscar Schachter, 'The Decline of the Nation-State and its Implications for International Law' (1997) 36 Columbia Journal of Transnational Law 7.
11. Anne Peters, 'Membership in the Global Constitutional Community' in Jan Klabbers (ed), *The Constitutionalisation of International Law* (OUP, Oxford 2010) 154.
12. Philip Alston, 'The Not-a-Cat Syndrome: Can the International Human Rights Regime Accommodate Non-State Actors' in Klabbers (n 11) 3, 4, 23 and 27.
13. Ibid 20.
14. Ibid 20–21.
15. Peggy O'Donnell, Alexa Koenig, Camille Crittenden and Eric Stover, 'Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the ICC' (Human Rights Centre

the storm had arguably very much arrived by 2016, it is encouraging that the Court has expressed a particular awareness of its importance within the landscape of open source evidence.

The Office of the Prosecutor (OTP) has also articulated a commitment to continued capacity building in science- and technology-based evidence collection. This is evidenced in the recruitment of experts and investment in specialised equipment as well as staff training and an increase in the use of technology in the legal process.[16] The OTP has also hired cyber-investigators and analysts to improve the ability of the office to identify, collect and process digital and online evidence.[17]

Beyond these practical developments, the ICC's commitment to engaging with new forms of technology in prosecutions has also been encouraging. The OTP has investigated a series of cases which relied on open source evidence. In the 2015 cases of *Banda Jerbo* and *Abu Garda*, which emerged subsequent to the conflict in Darfur, satellite imaging conducted by NSAs, including Google Earth, was used to track the burning and destruction of villages as well as population and troop movements.[18]

Subsequently, in *Al Mahdi*,[19] the ICC was presented with a significant quantity of open source evidence including satellite images taken from Google Earth as well as content from YouTube, and audio content sourced online.[20] The conflict in *Al Mahdi* occurred in 2012, during a period in which digital recording devices were in widespread use and satellite and drone technology were pervasive. In this respect the case offers a helpful insight, in light of the later approaches in *Bemba* and *Al-Werfalli*, regarding the necessity and prevalence of open source evidence in international criminal prosecutions.

The *Al-Werfalli* arrest warrant, issued by the Prosecutor on 1 August 2017 under Article 58[21] was notable for its reliance on open source evidence drawn from social media, specifically YouTube as well as five video files drawn from 'social media' generally.[22] However, the case of *Bemba et al*[23] is perhaps the most concrete example of reliance on social media evidence by the ICC to date.

In *Bemba*, the defendant was alleged, subsequent to other crimes of which he had been convicted, to have engaged in witness tampering.[24] Specifically, the Prosecution

School of Law University of California Berkeley, Workshop Report 7, 23 October 2012) <https://www.law.berkeley.edu/wp-content/uploads/2018/03/HRC_Beyond_Reasonable3.pdf> accessed 26 July 2018.

16. International Criminal Court Office of the Prosecutor, 'Office of the Prosecutor: Strategic Plan 2016–2018' ICC-ASP/14/22 (21 August 2015) 61.

17. Ibid 59–61.

18. *Prosecutor v Abdallah Banda Saleh Jerbo Jamus* (Judgment on Appeal) ICC-02/05-03/09 (28 August 2013); *Prosecutor v Bahr Idriss Abu Garda* (Decision on Confirmation of Charges) ICC-02/05-02/09 (7 March 2011).

19. *Prosecutor v Ahmad Al Faqi Al Mahdi* (Decision on Confirmation of Charges) ICC-01/12-01/15 (24 March 2016).

20. *Prosecutor v Ahmad Al Faqi Al Mahdi* (Decision on Confirmation of Charges) ICC-01/12-01/15-84-Red (24 March 2016).

21. *Prosecutor v Mahmoud Mustafa Busayf Al-Werfalli* (Warrant of Arrest) ICC-01/11-01/17 (15 August 2017) 8.

22. Ibid 8–9.

23. *The Prosecutor v Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu and Narcisse Arido* (Judgment) ICC-01/05-01/13 (19 October 2016).

24. Ibid.

argued that the defendant had bribed a witness to change their testimony.[25] In support of this allegation, the Prosecution submitted evidence of a wire transfer as well as pictures from Facebook showing the two witnesses alleged to have been bribed together.[26]

It is fair to impute a willingness on the part of the ICC based on these instances to engage with and rely on open source evidence in pursuing investigations and prosecutions.[27] However, while the Court has relied on emerging evidence formats in cases such as *Bemba*, *Al Mahdi* and the arrest warrant of *Mahmoud Al-Werfalli*, the means of ensuring that NSAs who control digital platforms preserve such evidence is less certain.

### 4.2 Powers of investigation

Under the Rome Statute, the OTP is charged with initiating the investigation of crimes[28] where a situation is referred by a State party or by the UN Security Council. An investigation may also be commenced *proprio motu*, when authorised by the Pre-Trial Chamber, subsequent to information received from sources including individuals and NGOs.[29] In the course of investigations, the Prosecutor is empowered subject to Article 15(2) to seek additional information from:

> [s]tates, organs of the United Nations, intergovernmental or non-governmental organizations, or other reliable sources that he or she deems appropriate and may receive written or oral testimony at the seat of the Court.[30]

If the Prosecutor believes there is a reasonable basis on which to proceed with the investigation, they may submit a request for authorisation to the Pre-Trial Chamber.[31] The Chamber shall then authorise the commencement of the investigation where it is satisfied as to the existence of a reasonable basis and the jurisdiction of the Court.[32]

The Prosecutor is also empowered under Article 54(3)(f) of the Rome Statute to take any measures or to request that any measures be taken to enforce the preservation of evidence. The Pre-Trial Chamber is similarly empowered under Article 56 to take

25. Ibid.
26. *Bemba* (n 23) 83.
27. Nor has engagement with open source evidence in prosecuting international crimes been limited to the ICC. At the national level, the 2013 decision of the District Court of Stockholm in the case of *Haisam Sakhanh* offers further support for the proposition that there is a general willingness to embrace open source evidence in international criminal prosecutions. Sakhanh was a Syrian with a Swedish residency permit and was arrested in Örebro in March 2016 as a result of suspicions that he had participated in executions carried out by an Islamist armed group in 2012 while in Syria. Video of an incident taken from social media was used as evidence in the subsequent District Court trial, see The Local, 'Swedish Court Hands Life Sentence to Syrian for War Crimes' (16 February 2017) <https://www.thelocal.se/20170216/swedish-court-hands-life-sentence-to-syrian-for-war-crimes> accessed 26 July 2018.
28. Rome Statute of the International Criminal Court (opened for signature 17 July 1998, entered into force on 1 July 2002) 2187 UNTS 90 (Rome Statute) art 15(1).
29. International Criminal Court, 'Office of the Prosecutor' <https://www.icc-cpi.int/about/otp> accessed 26 July 2018.
30. Rome Statute (n 28) art 15(2).
31. Rome Statute (n 28) art 15(3).
32. Rome Statute (n 28) art 15(4)(a).

those measures necessary to ensure the preservation of evidence which may not be available subsequently for the purposes of a trial.

In conducting such investigations, Rule 104(2) of the ICC Rules of Procedure and Evidence empowers the Prosecutor to seek additional information from states, organs of the United Nations, intergovernmental and non-governmental organisations, or other reliable sources deemed appropriate. Article 64(6)(b) also permits the Trial Chamber to request assistance from states in the production of evidence. These obligations are complementary to the obligations of States parties under Articles 86 and 87 of the Rome Statute to cooperate fully with the Court in its investigation and prosecution of crimes, and under Article 88 to ensure that there are procedures available at a national level to ensure cooperation.

Additionally, according to Article 70(1)(c), destroying, tampering with or interfering with the collection of evidence is deemed a crime against the administration of justice over which the ICC enjoys subject-matter jurisdiction. In accordance with Article 70(4), States parties must not only criminalise such conduct under their national law, but also, on the court's request, submit cases of this sort to their relevant authorities for the purpose of prosecution.

The Prosecutor may, thus, pursue NSAs through a request for any evidence held by them under Rule 104(2). However, as NSAs are not bound to comply with such a request, the functional utility of the rule is questionable. Alternatively, the Prosecutor may seek to secure evidence held by NSAs. This would be achieved through the obligations imposed directly on States parties. However, this avenue assumes that there are in place in States parties national legal systems, measures which permit such evidence to be obtained, or to impose sanctions on NSAs where it is destroyed.[33] As the proceeding part will illustrate, such laws are not always present despite the requirements of Article 70(4). Moreover, even where such provisions are in place, states must still contend with their inability to exercise jurisdiction over NSAs.

Faced with dilemmas in ensuring NSA compliance, the International Criminal Tribunal for the former Yugoslavia (ICTY) pursued two alternative approaches. First, the Tribunal entered bilateral agreements to pursue cooperation which resulted in some 20 individual agreements.[34] Second, the ICTY requested assistance from intergovernmental organisations where such organisations were located in UN member states.[35]

The possibility that the ICC might enter cooperation agreements with NSAs seems, if not likely, then certainly pragmatic, given the reputational damage to NSAs from publicity associated with declining to cooperate with the Court. However, this remains a 'soft' inducement to cooperation and, given the existing requirements of States parties under the articles and rules outlined above, would be of marginal benefit.

### 4.3 Evidentiary Protocols for open source evidence

Once open source evidence has been obtained the issue for the ICC is whether such evidence can be used. While open source evidence is not difficult to access, as it is

33. Rod Rastan, 'Testing Cooperation: The International Criminal Court and National Authorities' (2008) 21 Leiden Journal of International Law 431, 434 and 453.
34. International Criminal Court, 'Member States Co-Operation' <http://www.icty.org/en/documents/member-states-cooperation> accessed 26 July 2018. See also, Guido Acquaviva, 'Non-State Actors from the Perspective of International Criminal Tribunals' in Jean d'Aspremont (ed), *Participants in the International Legal Systems: Multiple Perspectives on Non-State Actors in International Law* (Routledge, London 2013) 185.
35. Ibid.

generally already in the public realm, its use is contingent on authentication.[36] Thus, while such evidence appears to have few practical acquisition procedures, legally its collection is troubled by concerns over integrity, compatibility and standardised authentication procedures.[37] The majority of efforts at the ICC to date have focused on compatibility – notably through the 'e-Court Protocol'.

There is currently no designation of what constitutes admissible evidence within the ICC Rules of Procedure and Evidence. Rather, the Rules establish a framework of evidentiary analysis in accordance with which evidence is admitted or rejected based on its relevance, probative value and prejudicial impact.[38] In addition, the Court has developed standard procedures for uploading and presenting evidence, in the form of the e-Court Protocol.

The Protocol provides for direct disclosure, in-court provision of digital materials and consistent information exchange.[39] It is notable that while the Protocol offers some authentication, by specifying that metadata should be attached to digital files for example,[40] it is largely limited to harmonising the format, storage and presentation of digital evidence within the Court system. The Protocol does not address the probative value of digital evidence which under Rule 63(2) remains flexible, broadly drawn and subject to the graduated grounds for action under the Rome Statute.

Under Articles 53(1)(a) and 58(1)(a), the standard required for the instigation of an investigation or issuance of an arrest warrant is 'reasonable grounds to believe'. As evidenced by the *Al-Werfalli* arrest warrant, open source evidence would likely satisfy this standard where it was furnished in a format and retrieved from a source that was *prima facie* reliable. To confirm charges the prosecution must then furnish evidence to the Court on which basis they can establish there exist 'substantial grounds to believe' that the accused perpetrated the alleged crimes under Article 61(5). This is an augmentation of the standard required for arrests and investigations and would require, in accordance with the e-Court Protocol, open source evidence be provided which had attached metadata.

Finally, in order to issue a conviction, Article 66(3) requires that the Prosecutor prove beyond a reasonable doubt that the accused perpetrated the crimes alleged. At this juncture, open source evidence would likely require additional corroboration.

Given this context, the expansion of the Prosecutor's powers to actively gather the evidence currently held by NSAs would be the most achievable and effective measure available.

36. See *Prosecutor v Popovic et al* (Decision on Admissibility of Intercepted Communications) ICTY-05-88-T (7 December 2007) 4, 22, 26, 33–35.
37. Hiatt (n 2) 326, 329; International Bar Association, 'Evidence Matters in ICC Trials' (August 2016) 18–20; Aida Ashouri, Caleb Bowers and Cherrie Warden, 'An Overview of the Use of Digital Evidence in International Criminal Courts' (Salzburg Workshop on Cyber Investigations, 2013) <https://core.ac.uk/download/pdf/33336993.pdf> accessed 26 July 2018.
38. See Rules 64, 68 and 72 of the ICC Rules of Procedure and Evidence, reproduced from the Official Records of the Assembly of States Parties to the Rome Statute of the International Criminal Court, First session, New York, 3–10 September 2002 (ICC-ASP/1/3 and Corr.1) part II.A.
39. See International Criminal Court, 'The Use of e-Court Technology at the International Criminal Court' (27 June 2008) <https://aija.org.au/wp-content/uploads/2018/03/KeddieFlores2.pdf> accessed 26 July 2018.
40. *Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui* (Prosecutions Communication of e-Court Protocol Metadata to the Defence) ICC-01/04-01/07 (23 June 2008).

## 5 ENFORCING PRESERVATION AND REPORTING OF OPEN SOURCE EVIDENCE

Globalisation and digitisation have fostered an international landscape in which NSAs operate from multiple jurisdictions, a model that makes it difficult to secure the preservation of content held by NSAs despite the requirements of the Rome Statute that States parties develop a scheme of enforceability within their jurisdictions. The international character of digital platform providers and their parent NSAs is further complicated by the predominantly North American origin and incorporation of such platforms.

Despite a broad pattern of ratification among members of the international community, the United States is one of a number of jurisdictions that are not party to the Rome Statute and is unusual in having previously signed the Statute and subsequently withdrawn its intent to ratify.[41] While the Obama administration re-established a relationship with the ICC as an observer, the US seems unlikely to reorientate its foreign policy position in the near future.

As a result, any implicit good faith that might exist with respect to the cooperation of observing parties with an investigation by the Prosecutor is absent. This is problematic, as a majority of digital platform NSAs are headquartered or incorporated in the US and locate some, if not all, of their servers in that jurisdiction. The result is that, even given the presence of EMEA[42] headquarters in other jurisdictions, material hosted or controlled by NSAs may be placed beyond the reach of a State party.

The logical response in light of existing obligations under the Rome Statute and such jurisdictional complications is simply to pursue the NSA in question through its EMEA headquarters. In this respect, Ireland (as a location of a significant proportion of EMEA headquarters) is a signatory to the Rome Statute, having ratified in 2002, and would be in a position to seek content held by such NSAs pursuant to a request for cooperation from the Prosecutor and the issue of a valid warrant at a domestic level. However, this avenue is not without challenges.

The principle underlying the law of state responsibility is that states cannot be held responsible for the acts of private or non-state actors.[43] However, the ICC is a hybrid system in that it relies on the cooperation of States parties in the apprehension and surrender of accused persons, to render legal assistance during investigations, and in the enforcement of its judgments.[44] The most clearly accepted basis on which to impose duties on NSAs to report or preserve evidence useful to international criminal investigations is, thus, through national criminal and or civil penalties present in domestic legislation, as required by Articles 70 and 86.

This would appear to be achieved most readily through relevant ICC-related legislation or, alternatively, through the enforcement of 'generic' national legislative provisions concerning the destruction of evidence or obstruction of criminal investigations resulting from a failure to report a crime. Such provisions are not unusual.

41. A position it shares with Sudan and Israel.
42. Europe, Middle East and Africa.
43. Cedric Ryngaert, 'State Responsibility and Non-State Actors' in Math Noortman, August Reinisch and Cedric Ryngaert (eds), *Non-State Actors in International Law* (Hart, Oxford 2017) 163. Note, however, that under article 8 of the Draft Articles on state responsibility on attribution, states may be liable for acts committed by persons or groups where conduct was directed or controlled by the state.
44. Mahmoud Cherif Bassiouni, *Introduction to International Criminal Law* (2nd edn, Martinus Nijhoff Publishers, Dordrecht 2003) 495.

The jurisdiction with disproportionate influence over the success of such an enforcement strategy is Ireland, where the majority of NSAs with the potential to offer open source data have based their EMEA headquarters.[45] This is due largely to the non-signatory status of the United States where such NSAs are otherwise based and which renders Ireland, as a State party to the Rome Statute, the *de facto* jurisdiction of enforcement for such compliance.

In Ireland, under s 19(1) of the Criminal Justice Act 2011,

> [a] person shall be guilty of an offence if he or she has information which they believe or know might be of material assistance (a) in preventing the commission of an offence, or (b) securing the apprehension, prosecution or conviction of any other person for a relevant offence …[46]

Under the Act it is also an offence pursuant to s 17 to 'falsify, conceal, destroy or dispose of a document or record which an individual knows or suspects would be relevant to an on-going investigation'.[47]

The ability of Irish authorities to utilise these provisions to require NSAs to preserve or report evidence of an international criminal offence is limited by the absence of international criminal offences from the definition of 'relevant offence' provided for in Schedule 1 of the Act. Moreover, even where such an inclusion was effected by amendment, there remain barriers to the use of the Act in this manner to bodies corporate.

Section 22 of the Act provides:

> [W]here an offence under the Act is committed by a body corporate with the consent, connivance or wilful neglect, of a director or officer that individual shall be guilty of an offence and may be proceeded against and punished as if he or she were guilty of the first-mentioned offence.[48]

In the case of YouTube, where deletion was conducted as a consequence of algorithmic programming which identified blanket categories of offensive or violent material rather than material related to a specific conflict or group, it is unlikely that the threshold for officer liability would be satisfied. Absent a significant amendment of the 2011 Act, it is thus necessary to identify an alternative means of regulating NSA behaviour in relation to open source evidence in Ireland.

The most obvious avenue would be through the use of the International Criminal Court Act 2006 which transposes into Irish law the requirements of the Rome Statute and provides for means of national enforcement. Under the Act, s 51(1)(c)[49] and s 51(5)[50] provide for the issuing of a warrant for the production of, or access to, records or documents where the ICC requests State cooperation. However, the Act does not provide for an offence of failure to report or preserve evidence as is provided for under the 2011 Act.

45. Such companies include Google, Facebook, LinkedIn, Twitter and Dropbox, all of whom locate some if not all (in the case of Dropbox) of their servers in the United States.
46. 2011 Criminal Justice Act (CJA 2011) s 19(2), pursuant to which a person guilty of an offence under the section is liable on summary convention to a fine or 12 months in prison or both, and on conviction on indictment to a fine or prison term not exceeding five years or both.
47. CJA 2011, s 17.
48. CJA 2011, s 22.
49. International Criminal Court Act 2006 (ICCA 2006) s 51(1)(c).
50. ICCA 2006, s 51(5).

In light of Ireland's status as a dualist system,[51] it would thus appear that to provide an effective means of mandatory reporting or preservation, Irish law would require an amendment of the 2011 Act to include reference within the schedule of relevant crimes to offences under the International Criminal Court Act 2006. Even where such an amendment were affected, a further jurisdictional issue would arise.

While the EMEA headquarters of an NSA may be located in Ireland, or indeed any ICC State party, the servers on which the content sought is stored may not be similarly located. In such circumstances the national authorities, in seeking to cooperate with the Prosecutor's investigation, may find content is stored on servers outside its jurisdiction. Indeed, the servers used by Google Inc., YouTube's parent company, are located in numerous data centres worldwide. Although five are in states which have both signed and ratified the Rome Statute,[52] the remaining ten are in jurisdictions which have not,[53] including Google's five largest servers, which are located in North America.[54]

The recent US Supreme Court case of *United States v Microsoft*[55] had the potential to offer some comparative clarity on the ability of states to seek information stored on servers in other jurisdictions. The case asked the Court to consider the power of a warrant, issued by a New York court, to operate extraterritorially to require disclosure by Microsoft of files held on servers located in Ireland. However, the case was declared moot in April following Congressional passage of the CLOUD Act 2018 and so any insight into reciprocal treatment by the judiciary of foreign warrants for material stored on US servers has not emerged.[56]

The 2001 Mutual Legal Assistance Treaty (MLAT)[57] between the United States and Ireland similarly provides no immediate solution. The MLAT provides for search and seizure under Article 14 of information justifying action under the laws of the requested party[58] where the request relates to powers of search and seizure exercisable in the requesting state.[59] However, given the absence of a legal basis to prosecute destruction or failure to report evidence of international criminal offences under Irish law, the MLAT provides no solution. Equally, the MLAT would not offer a proactive ability to impose an obligation, but merely to retrospectively seek the evidence on request from the ICC and, thus, fails to solve the problem of NSA control examined here.

51. Fiona de Londras, 'Dualism, Domestic Courts and the Rule of International Law' in Mortimer Sellers and Tadeusz Tomaszewski (eds), *The Rule of Law in Comparative Perspective* (Springer, Wien 2010) 217; Alan D P Brady and James Mehigan, 'Universal Jurisdiction for International Crimes in Irish Law' (2008) 43(1) Irish Jurist 59, 80.
52. Chile, Finland, Belgium, Ireland and The Netherlands.
53. Other than its servers in North America, Google has servers in Singapore, which is neither a party nor a signatory, and Taiwan, which is not a signatory or party and suffers from a uniquely complicated relationship with both the United Nations and its neighbouring non-signatory state of China.
54. In Oregon, Georgia, Virginia and North and South Carolina.
55. *United States v Microsoft Corporation*, 584 US (2018). The United States Supreme Court declared the case moot, see <https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf> accessed 26 June 2018.
56. The Clarifying Lawful Overseas Use of Data Act HR 4943 (CLOUD Act) <https://www.congress.gov/bill/115th-congress/house-bill/4943> accessed 26 July 2018.
57. Mutual Legal Assistance Treaty between the United States of America and Ireland (adopted 18 January 2001, entered into force 11 August 2009), Treaties and other International Acts Series 13137.
58. Ibid art 14(1).
59. Ibid art 14(2).

## 6 A NEW ROLE FOR THE ICC

Given the inapplicability of international criminal law to NSAs and the barriers to States parties' ability to require NSAs to preserve or report open source evidence in the context examined, a solution which safeguards open source evidence is required. The unilateral power such NSAs possess to permanently delete content which will be increasingly central in the future of international criminal prosecutions further increases the necessity for such safeguards.

### 6.1 Existing alternatives

At present, certain alternatives do exist. Returning to the Syrian example cited at the outset of this piece, the impact of YouTube's deletion in 2017 may have been mitigated somewhat by the previous establishment of the 'International, Impartial and Independent Mechanism to Assist in the Investigation and Prosecution of Those Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011' (IIIM) in December 2016, by UN General Assembly Resolution 71/248. The IIIM was tasked with collecting, consolidating, preserving and analysing evidence of

> violations of international humanitarian law and human rights violations and abuses and to prepare files in order to facilitate and expedite fair and independent criminal proceedings, in accordance with international law standards, in national, regional or international courts or tribunals that have or may in the future have jurisdiction over these crimes, in accordance with international law.[60]

The IIIM draws on social media and open source information to build its cases. In this respect it would be hoped that the content removed by YouTube had been identified, duplicated and saved by the body or the parallel activity of organisations such as the Syrian Archive and the Commission for International Justice and Accountability (CIJA) or the United Nations Independent International Commission of Inquiry on Syria. However, the model offers little beyond what currently exists at the ICC itself and as a consequence is not helpful in building a new institutional model.

Elsewhere the International Bar Association (IBA) established the EyeWitness Project alongside its EyeWitness to Atrocities application for the purpose of authenticating and securely storing open source video evidence of human rights abuses, specifically the crimes of genocide, war crimes, torture and crimes against humanity.[61] The application was developed subsequent to the challenges encountered by the IBA's Executive Director in authenticating footage of Sri Lankan troops executing Tamil prisoners in 2010.[62]

The application automatically records metadata associated with the files collected to verify the date, time and location of footage and has a unique identifying code in each file which forms a 'digital fingerprint' protecting it from further editing.[63] Footage

60. UNGA Res 71/248 (11 January 2017) UN Doc A/RES/71/248.
61. On the EyeWitness Project and app, see <http://www.eyewitnessproject.org/eyewitness-faqs/> accessed 26 July 2018.
62. Rebecca Lowe, 'Witnessing Atrocity' (International Bar Association, 11 June 2015) <https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=11e76b66-d949-4738-9347-e67fbfbb9441> accessed 26 July 2018.
63. Ibid.

captured using the app is securely stored through a partnership with LexisNexis, on secure LexisNexis servers located within the European Economic Area.[64] At first blush it might seem EyeWitness has solved the problem of NSA control by creating a means of reporting content in a manner which is secure and attaches legally sufficient means of verification and keeps the evidence on servers located in ICC member states.

However, several problems persist, with the result that this is not necessarily the case. First, EyeWitness is a company limited by guarantee, incorporated in England and Wales and as such is also an NSA. While the express aim of the company is to enhance cooperation and its servers are located within the European Union meaning it would be unable to put its files beyond the reach of the ICC, it does not solve the issue posed by NSAs in relation to open source evidence more generally.

Additionally, the practical reality is that, for a majority of civilians in conflict zones, YouTube will be a familiar platform, with a degree of 'brand recognition' not enjoyed by the app. This will necessarily be reflected in challenges promoting its use. In this respect, the cultural ubiquity and familiarity of YouTube remains a significant stumbling block to countering NSA control of open source evidence.

A further issue to consider is the use of LexisNexis' servers, which LexisNexis has offered through its partnership with the IBA in the app's development. Were the entity which owned the servers to go into liquidation, the servers could be subject to sale or where they were secured under lease, the lessee could be blocked from access and their contents wiped. In either event it would appear, without view of the specific contractual terms of the agreement between LexisNexis and EyeWitness that the use of a third party to store content is complex and potentially problematic.

The final issue, and the most significant obstacle to a *de facto* adoption of the IBA model as a solution is that it collects video footage only. While video footage is certainly an important source of open source evidence, it is not the exclusive source. Thus, while the IBA's approach is certainly instructional, it does not offer a comprehensive solution.

### 6.2 A model for the ICC

In light of the difficulties which this piece has outlined, the most predictable means of ensuring open source evidence is preserved is through the creation of an online curatorial system under the auspices of the OTP by which individuals or interested parties might upload or record audio, video or image files as appropriate, providing a scope for collection not present with the IBA app at present.[65]

Creating a curatorial system within the ICC would not necessitate an expansion of the OTP's powers, in as much as the office is currently empowered to receive and subsequently investigate complaints made under Article 15. Nor would such a development be unprecedented; indeed, it would act as an expansion of accepted practice in engaging with open source evidence.

An independent, 'in-house' system would also provide greater certainty around the chain of custody and the integrity of evidence by ensuring that content files, metadata and locational information were hosted in a single location, in a harmonised format and under ICC control. In this respect, the model used by the IBA is sound.[66] However, the

64. Ibid.

65. See EyeWitness to Atrocities App <https://play.google.com/store/apps/details?id=com.camera.easy> accessed 26 July 2018.

66. It should be noted that the terms of the user agreement which accompanies the EyeWitness application are quite problematic. First, the agreement notes that the images and recordings

collection of the evidence by a third party (the IBA) and the potential exposure of the evidence to claims of bias given the stated aim of the IBA to ensure the prosecution of international crimes make the neutral institutional setting of the ICC more appropriate.

A reporting mechanism at the international level of the ICC is also preferable to individual national measures due to practical concerns about the collection of content under the same conditions and in similar formats. It is additionally desirable given the long-term need to consider that, were a conflict to begin in a signatory state, a national mechanism would be functionally redundant at best or, at worst, offer a means for one party to a conflict to actively track and persecute those allied with opposition groups.

This is not to suggest national institutional collection would damage the authenticity of the evidence collected. Indeed, in accordance with the principle of positive complementarity, it is the policy of the ICC to encourage states and institutions to develop their own investigative and prosecutorial capabilities.[67] However, it is suggested that unbridled deference to the principle of positive complementarity in the collection of open source evidence conveniently ignores the practical realities of national political will and resources implicated in arguments for systematised collection of open source evidence.

First, and as detailed further below, the infrastructure and expertise necessary to establish and maintain a system for the collection of open source evidence is not insignificant. At a national level, this would require the existence of a budget sufficient to establish such a capacity as well as the political will to allocate funds to such a project. Additionally, differing national approaches to the collection and formatting of such evidence as well as national priorities in relation to which conflicts evidence should be collected on could lead to a potential duplication of collection of evidence in relation to some conflicts, and the neglect of others with an associated misallocation of resources.

Even were such issues overcome by a harmonised approach to collection between jurisdictions, national collection models are vulnerable to geopolitical and national bias. Governments whose own troops are engaged in actions bringing them within the jurisdiction of the court are unlikely to want to collect or preserve evidence of such activities. States whose neighbours are engaged in such activities may also find that it is undesirable to maintain a rigorous collection mechanism where it brings an associated risk of economic or political retaliation. These geopolitical and national barriers to reliance on individual national approaches are not insignificant. While individual national initiatives are desirable, they are unlikely to be sufficient.

In turning to address the more viable ICC model, several concerns would have to be addressed in the structure and design of a reporting mechanism. First, in recognition of the reality that communications infrastructure may be adversely affected during

submitted to EyeWitness using the app can be used for purposes other than prosecution which include raising awareness. Elsewhere in the document the user agreement notes that the user must comply with all laws and regulations in force in the jurisdiction in which the app is being used. In general, the law would require the consent of the data subjects – not only those making but also those that feature in an image or recording. Obtaining this is *prima facie* problematic, if not impossible, in many of the circumstances in which this app will be used. Moreover, it is likely that in an extended conflict in which the state is a party there may be additional laws prohibiting the use of such recording equipment or the recording of certain actions or individuals in an extended conflict. It is unclear what the effect of a breach of these terms would be, and whether it would affect the viability of the evidence obtained; presumably not, but the terms are problematic given the doubt they impose on the legitimate use of the application.

67. See generally Fidelma Donlon, 'Positive Complementarity in Practice' in Carsten Stahn and Mohamed M El Zeidy (eds), *The International Criminal Court and Complementarity: From Theory to Practice* (CUP, Cambridge 2011) 920.

conflict, the ICC would be required to employ a model that was mobile-compatible and capable of operating on a minimal bandwidth through an always-on design which would be compatible with both Android and Apple operating systems.

The model would also be required to permit individuals to submit files confidentially. Anonymous submissions would be problematic, though the use of IP addresses and metadata, as with EyeWitness, would ameliorate this significantly. Equally, a secure submission channel could permit individuals to submit content attached, ideally, to a picture of an item of official identification or, alternatively, a filled form which would be more helpful in authentication and identification of witnesses at a later stage.

In this respect the security of the submission channel and of the storage and use of the submissions would be paramount. It follows that any privacy policy attached to the system would need to exclude the use of cookies and other analytical tools including unique device or in-App identification measures in order to preserve the privacy and safety of those concerned.

The finances involved in establishing and running a secure system for confidential submissions will be significant. Highly skilled staff with the expertise to employ cyber-security measures sufficiently sophisticated to successfully repel attempts to access or corrupt the digital files held by the ICC will be required. In this respect, the ICC-operated model would likely suffer difficulties in securing financing.

More difficult to address than the practical concern of financing and the more general concerns of designing a reporting mechanism is the popular recognition of the system. In discussing the IBA app, it was noted that the most significant issue appears to be one of 'brand recognition'. YouTube is recognisable on a cross-cultural basis while the IBA app is known, even among the legal community, only to those with a specific interest in legal technologies or international criminal law. This challenge persists with the current proposition.

It is tentatively submitted that the ability of the ICC to broadcast the availability of the reporting system would be somewhat broader than that of the IBA. This is a result of the officially cooperative nature of its relationship with the UN under the UN–ICC Relationship Agreement. The presence of the UN in jurisdictions where conflict is occurring, or where conditions are conducive to the outbreak or escalation of conflict as well as the cultural capital and practical information dissemination networks enjoyed by the UN in both international and local communities further support this view.[68]

## 7 CONCLUSION

The ICC currently lists open investigations in 11 jurisdictions and preliminary examinations in 10 others.[69] Of these, the conflicts in Ukraine, Iraq and Afghanistan in particular have been characterised for much of their duration by expansive use of drone technologies and civilian documentation of the conflicts. As time passes, the number of cases listed which occurred during periods or in areas not characterised by widespread use of mobile recording technology will decline further.

68. Negotiated Relationship Agreement between the United Nations and the International Criminal Court (adopted and entered into force 4 October 2004) 2283 UNTS 195.
69. International Criminal Court, 'Situations under Investigation' <https://www.icc-cpi.int/pages/situations.aspx> accessed 26 July 2018; International Criminal Court, 'Preliminary Examinations' <https://www.icc-cpi.int/pages/pe.aspx> accessed 26 July 2018.

The ICC has demonstrated a willingness to engage with new technologies including open source evidence. However, the dominance of NSAs in controlling access to and preservation of this evidence is troubling and requires a means by which the ICC might conceivably either negate such a disproportionate influence or restrict its exercise.

In seeking to secure such a means, neither direct action from the ICC under the current model nor intervention by States parties appears equal to the task. This paper, therefore, contends that the most viable solution is for the ICC to develop its own powers of proactive collection and solicitation of evidence through a popularly available system for submission of content from civilians and other interested parties.