ICTS, SOCIAL MEDIA, & THE FUTURE OF HUMAN RIGHTS

NIKITA MEHANDRU[1] AND ALEXA KOENIG[†]

INTRODUCTION

As communication increasingly shifts to digital platforms, information derived from online open sources is starting to become critical in creating an evidentiary basis for international crimes. While journalists have led the development of many newly emerging open source investigation methodologies, courts have heightened the requirements for verifying and preserving a chain of custody—information linking all of the individuals who possessed the content and indicating the duration of their custody—creating a need for standards that are just now beginning to be identified, articulated, and accepted by the international legal community. In this article, we discuss the impact of internet-based open source investigations on international criminal legal processes, as well as challenges related to their use. We also offer best practices for lawyers, activists, and other individuals seeking to admit open source information—including content derived from social media—into courts.

I. BENEFITS AND LIMITATIONS OF ONLINE OPEN SOURCE INFORMATION

A. Legal Uses of OSI in Evidence-Gathering

The use of online open source information[2] has a long history in intelligence gathering. Historically, online open source information was leveraged by intelligence agents and journalists to gather information on foreign actors. The Crimean War (1853–1856) was the first major

---

[1] Nikita Mehandru is currently a graduate student at the University of Pennsylvania. She holds a bachelor's degree in Economics and Government from Claremont McKenna College, and previously served as a research fellow at the University of California, Berkeley School of Law.

[†] Alexa Koenig is executive director of the Human Rights Center, co-founder of the Human Rights Investigations Lab, and a lecturer-in-residence at UC Berkeley School of Law. She has a BA in World Arts and Cultures from UCLA, a JD from the University of San Francisco, and a PhD in Jurisprudence and Social Policy from UC Berkeley.

[2] We define open source information as publicly-accessible information that can be acquired through observation, request, or payment. Information obtained by illegal means or through service of legal process is excluded. This definition is based on the forthcoming International Protocol on Open Source Investigations (2019).

conflict to be heavily documented by journalists through visual imagery and the written word, which in many ways engendered the modern military-media relationship.[3] For those who wanted to understand what was happening to whom and when, all they had to do was open a newspaper—a form of open source content. During World War II, President Roosevelt allotted emergency funds to monitor foreign broadcasts for intelligence purposes, ultimately leading to the creation of the Central Intelligence Agency. By the Cold War, television, phone lines, and radios were being exploited by both sides as a means for gathering open source intelligence.[4]

Criminal investigators typically use open source information for the following two reasons: (1) to discover new information relevant to their cases and (2) to verify and authenticate existing information (including witness testimony), mostly through the analysis of videos and photographs obtained via public, quasi-public, or private sources.[5] Discovery and verification can fulfill several needs related to producing reliable information helpful to legal process.[6]

First, regarding online discovery, open source methods can be especially helpful for generating lead, linkage and contextual information. Lead information is information that "leads" investigators to potential evidence, such as witnesses or documents.[7] For example, perpetrators who boast about their exploits on Facebook or Twitter might be geolocated based on identifying markers in the background of pictures, generating critical information about where they're located or where crucial events took place.[8] Open source information can also provide linkage evidence, enabling courts to effectively connect high-level perpetrators who may have ordered, condoned or failed to punish criminal activity to on the ground implementers. For example, open

---

[3] Alexa Koenig, Felim McMahon, Nikita Mehandru & Shikha Silliman Bhattacharjee, *Open Source Fact-Finding in Preliminary Examinations*, 2 QUALITY CONTROL IN PRELIMINARY EXAMINATION 681, 685 (2018).

[4] *Id.* at 687.

[5] *See The New Forensics: Using Open Source Information to Investigate Grave Crimes* (Human Rights Center, UC Berkeley School of Law, 2018), *available at* https://www.law.berkeley.edu/wp-content/uploads/2018/02/Bellagio_report_2018_9.pdf.

[6] *Id*.

[7] *See generally* Alexa Koenig et al., *supra* note 3, at 694 (discussing the various uses of open source information for court-related purposes).

[8] *See* Aviva Rutkin, *Human Rights Squad Detects Abuse in Warzone Social Media Images*, NEWSCIENTIST (NOV. 11, 2016), https://www.newscientist.com/article/2112483-human-rights-squad-detects-abuse-in-warzone-social-media-images/.

sources, including social media platforms, can be used to help establish networks surrounding the accused, or to document relevant communications among disparate actors.[9] Video footage posted to social media can especially be helpful in establishing not just the *actus reas*—the physical act of the crime—but also the *mens rea*—the often hard-to-prove intent behind that act. For instance, the intent of the accused might be made clear through posts on social media that brag about the desire to kill all of the individuals who comprise a particular religious or ethnic group (possible genocide), or describe a systematic strategy for seeking revenge on a person or class of people (possible crime against humanity). Open source information can also be used to provide contextual information, offering insights into the who, when, or where of an incident, and/or providing information that corroborates witness testimony.[10] Given the plethora of problems with overreliance on witness testimony such as bribery, deception, or memory loss,[11] the move towards gathering and using digital data as a means to corroborate such testimony is promising.

Second, open source information can help with the verification of existing information, including data collected through online open sources, traditional legal investigations, and from activists on the ground. For example, source materials may include videos and photographs sent to human rights organizations or court investigators whose alleged content requires validation. Such verification and authentication are critical for non-governmental organizations and courts, as both must establish the credibility of the information they use.[12]

Citizens outside of conflict zones increasingly play a prominent role in both the discovery and verification process.[13] For example,

---

[9] *Id.*

[10] *See* Keith Hiatt, *Open Source Evidence on Trial*, 125 YALE L.J.F. 323, 323–24 (2016) (discussing the benefits of open source electronic evidence).

[11] *See generally* Laura Engelhardt, *The Problem with Eyewitness Testimony–Commentary on a Talk by George Fisher and Barbara Tversky*, 1:1 STAN. J. LEGAL STUDIES 25, 25–30 (1999), *available* at https://docplayer.net/33822926-The-problem-with-eyewitness-testimony.html.

[12] *See* Jeff Deutch and Hadi Habal, *The Syrian Archive: A Methodological Case Study of Open-Source Investigation of State Crime Using Video Evidence From Social Media Platforms*, 7 STATE CRIME: J INT'L STATE CRIME INITIATIVE 46 (2018); Rebecca J. Hamilton, *User-Generated Evidence*, 57 COLUM. J. TRANSNAT'L L. 1, 17–18 (2018).

[13] *See* Judy Woodruff, A New Generation of Human Rights Investigators Turns to High-Tech Methods, PBS NEWSHOUR (Feb. 13, 2017), http://www.pbs.org/newshour/bb/new-generation-human-rights-investigators-turns-high-tech-methods/ (interviewing civilian students in the United States about their documentation of conflict zones like Syria).

Bellingcat, an investigative network run by citizen journalists, has conducted open source investigations to establish responsibility for the downing of MH17 over Ukraine, as well as potential crimes committed during the Syria conflict.[14] Other groups, such as the University of California, Berkeley's Human Rights Investigations Lab and the University of Essex's Human Rights Centre,[15] rely on students to conduct the labor-intensive work of gathering and verifying information from public sources for advocacy and legal accountability purposes. Whether obtained online, directly from the source, or through an intermediary, students can verify and therefore help legitimize (or discredit) activist videos.[16]

Unfortunately, however, even when verified, photographs and videos may not be particularly helpful for courts if what the photographer or videographer captured provides little contextual, lead, or linkage information. As a result, the human rights organization, WITNESS, created the "Video as Evidence Field Guide," which offers useful guidance for first responders, activists, survivors, and others who hope to document violations via video in ways that maximize those videos' utility for courts.[17] Similarly, the International Bar Association launched a mobile application called "eyeWitness to Atrocities" to document violations and preserve that information for court purposes.[18] The application collects the date and location of recorded footage from three different sources and creates a digital fingerprint to prevent that

---

[14] Syrian Archive, *Medical Facilities Under Fire: Systematic Attacks During April 2017 on Idlib Hospitals*, BELLINGCAT (July 28, 2017), https://www.bellingcat.com/news/mena/2017/07/28/medical-facilities-fire-systematic-attacks-april-2017-idlib-hospitals-serving-one-million-syria/.

[15] Amnesty International's Digital Verification Corps is a consortium of university students trained in open source verification and discovery who provide critical capacity for Amnesty researchers. The program launched in Fall 2016 and by Fall 2017 consisted of participants from five universities, including the University of California, Berkeley, the University of Essex, the University of Pretoria, the University of Cambridge, and the University of Toronto, with additional universities slated to join in 2017-2018.

[16] Rutkin, *supra* note 8.

[17] *Video as Evidence Field Guide*, WITNESS, https://vae.witness.org/video-as-evidence-field-guide/ (last visited Mar. 18, 2019).

[18] *Collect Verifiable Photos and Videos*, *FAQs*, EYEWITNESS, http://www.eyewitnessproject.org/ (last visited Oct. 2, 2017); *see also* Hamilton, *supra* note 12, at 17–18.

information from being edited. The software also establishes and preserves a chain of custody.[19]

B. Benefits

Though open source information has been systematically mined from the Internet by human rights advocates and international criminal investigators for a relatively short time, its potential contribution to the field is apparent. Examples of this contribution include providing "access" to conflict zones that cannot be physically accessed for security, diplomatic, or logistical reasons, engaging civilians on the ground, and enabling stronger investigations by generating information that corroborates or discredits witness testimony and other evidence.

Recently, open source information has provided a means to access information in remote conflict zones in Libya,[20] Syria,[21] Cameroon,[22] and Myanmar.[23] This includes not only photographs and videos as mentioned above, but also data derived from crowdsourcing tools such as Wikimapia or satellite imagery provided through online platforms such as Google Earth. Satellite imagery is increasingly available through public platforms at no or low cost and may also be available through closed or open sources. It can help establish the location of an atrocity and show changes to a particular location over time (such as before and after visuals of a hospital bombing).[24] This

---

[19] *See* Hamilton*, supra* note 12, at 18 (explaining how material is automatically encrypted before being stored in a "secure evidence locker" and catalogued by a team of attorneys).

[20] *How a Werfalli Execution Site Was Geolocated*, BELLINGCAT (Oct. 3, 2017), https://www.bellingcat.com/news/mena/2017/10/03/how-an-execution-site-was-geolocated/.

[21] *See*, *e.g.*, ANNA BANCHIK ET AL., CHEMICAL STRIKES ON AL LATAMINAH (Human Rights Center, UC Berkeley School of Law, 2018), *available at* https://humanrights.berkeley.edu/publications/chemical-strikes-al-lataminah.

[22] Conor Fortune, *Digitally Dissecting Atrocities—Amnesty International's Open Source Investigations*, AMNESTY INT'L (Sept. 26, 2018), https://www.amnesty.org/en/latest/news/2018/09/digitally-dissecting-atrocities-amnesty-internationals-open-source-investigations/; *Cameroon Atrocity: Finding The Soldiers Who Killed This Woman,* BBC NEWS (Sept. 24, 2018), https://www.bbc.com/news/av/world-africa-45599973/cameroon-atrocity-finding-the-soldiers-who-killed-this-woman.

[23] Steven Stecklow, *Why Facebook is Losing the War on Hate Speech in Myanmar,* REUTERS (Aug. 15, 2018), https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/.

[24] *See* AAAS Sci. Responsibility, Human Rights & Law Program, *Conflict in Aleppo, Syria: A Retrospective Analysis,* AM. ASS'N FOR THE ADVANCEMENT OF SCI., https://www.aaas.org/aleppo_retrospective (last visited Aug. 3, 2018)

temporal mapping can assist in the development of an event chronology (for example, showing the before and after of razed villages), or can be used to help predict future events and plan for interventions.[25]

One organization that has effectively used open source information is the Syrian Archive, an organization dedicated to preserving evidence of human rights violations committed by all sides of the conflict in Syria.[26] The Archive has gathered more than 1,400,000 videos, some of which have been verified and appear to depict chemical weapons attacks that violate international law.[27] This is invaluable documentation given the increasingly hostile propaganda efforts of some of the world's most powerful political players.[28] The Archive leverages both Syrian-based human rights advocates as well as remote media activists, journalists, and lawyers to document, preserve, and verify information related to the conflict, underscoring the incredible potential impact of coordinated civilian efforts.[29]

C. Limitations

Despite its many strengths, open source information is also subject to serious limitations. For example, the engagement of everyday citizens in documenting atrocities through video and photography may prove to be a double-edged sword. Video evidence can expose potential witnesses and the videographer, endangering their families and communities.[30] Thus, taking steps to ensure adequate protection of individuals is critical, and the potential risks involved in storing or releasing images or video content must be carefully calibrated.[31] Mitigating the risk of endangering witnesses and civilian investigators

---

(discussing the efforts of Amnesty International, USA to use satellite images to document more than one hundred instances of damage to buildings).

[25] Steven Livingston, *Satellite Imagery Augments Power and Responsibility of Human Rights Groups*, BROOKINGS (June 23, 2016), https://www.brookings.edu/blog/techtank/2016/06/23/satellite-imagery-augments-power-and-responsibility-of-human-rights-groups/.

[26] *About*, SYRIAN ARCHIVE, https://syrianarchive.org/ (last visited Mar. 3, 2019).

[27] *Id.*

[28] *Id.*

[29] *See id*.

[30] *Ethical Guidelines for Using Videos in Human Rights Reporting*, WITNESS, https://witness.org/portfolio_page/ethical-guidelines-for-using-videos-in-human-rights-reporting-and-advocacy/ (last visited Sept. 14, 2017).

[31] *See* THE ENGINE ROOM, DATNAV: HOW TO NAVIGATE DIGITAL DATA FOR HUMAN RIGHTS RESEARCH 34 (2017), *available at* https://www.theengineroom.org/wp-content/uploads/2017/01/en-datnav-report_high-quality_web_.pdf (discussing the importance of content verification and the "Do-No-Harm" principle).

remains one of the most challenging aspects of this work. Further, when users choose to remain anonymous, the process by which to admit such user-generated evidence may be ambiguous as judges wrestle with assigning probative value to the information.[32]

In addition, the likelihood of acquiring and potentially using misinformation found online is relatively high, so verification of that content is crucial. Some of the most common pitfalls of open source information include misattribution, staging, and technical manipulation.[33] Misattribution occurs frequently and involves deliberately or inadvertently recycling online content with the wrong date, time, or location.[34] Staging transpires when one party attempts to frame another by "staging" and filming an event that never occurred, or edits a video to mislead viewers about what actually took place. Technical manipulation involves manipulating photos and videos with Photoshop or other photo editing tools (e.g., swapping out military insignia).[35] Further, generative adversarial networks are increasingly being used to generate "deep fakes," artificially-generated videos that suggest someone said or did something that never occurred in real life.[36] Given the vast number of ways digital content can be altered, information derived from open sources must be handled carefully, especially if used to demonstrate the "truth" of what took place. "Ground truthing"—having those on the ground in a conflict zone confirm the accuracy of open source analysis—and engaging in verification processes that focus on both source and content analysis remain critical components of ensuring the validity of open source content.

---

[32] *See* Hamilton, *supra* note 12, at 49–50.

[33] THE ENGINE ROOM, *supra* note 30, at 35.

[34] *See*, *e.g.*, Eliot Higgins, *Misattribution, Verification, ISIS, and Madaya*, BELLINGCAT (Jan. 11, 2016), https://www.bellingcat.com/resources/case-studies/2016/01/11/misattribution-verification-isis-and-madaya/; *see also* UNDERSTANDING AND ADDRESSING THE DISINFORMATION ECOSYSTEM, KNIGHT FOUNDATION (Dec. 15–17, 2017), *available at* https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v4.pdf.

[35] *See, e.g.*, Maya Miller, *BuzzFeed Editor: How to Live in a World of Misinformation and Fake News*, WTTW (Feb. 14, 2017), https://news.wttw.com/2017/02/14/buzzfeed-editor-how-live-world-misinformation-and-fake-news (discussing the use of photo editing software to generate misinformation).

[36] K. Alexa Koenig, "*Half the Truth is Often a Great Lie": Deep Fakes, Open Source Investigations, and International Criminal Law*, AM. J. INT'L L. (forthcoming 2019).

D. The Need for Open Source Information: Shortcomings of Witness Testimony

Despite the many challenges found in validating digital evidence, weaknesses inherent to witness testimony make the move toward incorporating other forms of information vital. Triangulation of physical, documentary, and testimonial evidence remains the gold standard; as a form of documentary evidence, open source information can be helpful for corroborating witness testimony and developing the strongest possible narrative in court.

In recent years, the International Criminal Court (ICC) has recognized the need to diversify its evidence due to witness tampering and other witness-related challenges, specifically noting witness intimidation and protection as key challenges in its 2012–2015 Strategic Plan.[37] Later, in its 2016–2018 Strategic Plan, the Office of the Prosecutor (OTP) of the ICC found that witness interference—the act of altering or attempting to alter the content of a witness's testimony, or helping to prevent a witness from testifying—may have occurred in eight of the first nine cases at the ICC.[38] The OTP states that "almost all cases in the confirmation of charges and trial phases have been or are confronted with incidents of obstruction of justice—in particular witness tampering."[39] Witness interference is thus a serious threat to the Court's legitimacy and effective functioning. In the 2012 *Lubanga* case, the chamber concluded that nine out of the thirty-six witnesses were not credible after it was found that prosecution intermediaries may have coached their witnesses, child soldiers, to lie about their identities and experiences.[40] In the 2016 *Bemba* case, five defendants, including Jean-Pierre Bemba himself, were convicted of coercing fourteen witnesses into providing false testimony.[41] Such distortions undermine the rule of law and can lead to wrongful convictions or acquittals. Furthermore, the failure to protect witnesses testifying at the ICC can have grave consequences for the safety and well-being of witnesses, their families, and communities.

---

[37] INT'L BAR ASS'N, EVIDENCE MATTERS IN ICC TRIALS 21 (2016).

[38] OPEN SOC. JUSTICE INITIATIVE, WITNESS INTERFERENCE IN CASES BEFORE THE INTERNATIONAL CRIMINAL COURT 2–3 (Nov. 2016), https://www.opensocietyfoundations.org/sites/default/files/factsheet-icc-witness-interference-20161116.pdf [hereinafter *Briefing Paper*].

[39] INT'L CRIMINAL COURT: OFFICE OF THE PROSECUTOR, STRATEGIC PLAN 2016–2018 13 (2015), *available at* https://www.icc-cpi.int/iccdocs/otp/en-otp_strategic_plan_2016-2018.pdf.

[40] *See Briefing Paper*, *supra* note 37, at 4–5.

[41] *Id.* at 4.

In addition, memories can be fallible under the best of circumstances; time and trauma can further exacerbate challenges with input, storage, and recall. Substantial literature exists on the fallacies of human memory and the tendency to erroneously recollect events.[42] In the 2016 ICC case, *Prosecutor v. Ntaganda*, forensic psychologist Dr. John Charles Yuille provided his expert opinion on methods of recall:

> "[H]uman memory is reconstructive . . . . We don't play a tape back. We recreate a memory at the time of recall. And when we recreate the memory, there are two different forms that the memory can take. One form is where the person . . . remember[s] the event as they originally . . . perceived it. So they're looking through their eyes and recalling the event as it unfolded in front of them. There is a second kind of recall in which a person will recall an event but see themselves in it, that is they don't perceive it as they originally did. It's as if they were at a different place in the room and watching it unfold and they actually see themselves in the event."[43]

The malleability of memory was similarly underscored in a 1998 study by Elizabeth Loftus, a leading cognitive psychologist who illustrated the ability of a third party to introduce false facts and alter how subjects remembered various events.[44] This phenomenon was later dubbed the "misinformation effect."[45]

External interference is just one form of memory distortion; memories can be distorted even at their inception.[46] In addition, bias can distort recall. Further, while confidence and accuracy tend to correlate, witness confidence levels are often higher for incorrect information than correct information when misleading information is injected into conversations.[47] Thus, the malleability of the human mind, coupled with the potential of witness intimidation and suggestion by third parties, as well as cognitive biases, necessitates corroborating information.

In cases facing dismissal due to evidentiary deficiencies, open source information may prove pivotal to preventing a case from being dismissed due to insufficient evidence. Most recently, evidentiary deficiencies proved determinative in the cases of Gbagbo and Blé Goude at the International Criminal Court in January 2019. The two defendants had been charged with crimes against humanity—including murder and

---

[42] *See generally* Engelhardt, *supra* note 11.
[43] Prosecutor v. Bosco Ntaganda, ICC-01/04-02/06), Trial Hearing, p. 27, ¶¶2–11 (Apr. 18, 2016).
[44] Engelhardt, *supra* note 11, at 26.
[45] *Id.*
[46] *Id.* at 27.
[47] *Id.* at 28.

rape—allegedly committed in Cote d'Ivoire in 2010 and 2011 during the aftermath of the country's 2010 presidential election.[48] In the acquittal, the Court noted that prosecutors had failed to provide sufficient evidence to suggest their culpability.[49] Indeed, evidence can be particularly difficult to obtain in the aftermath of conflict. Witnesses may fear retribution and refrain from coming forward, and supporting documentation may have been destroyed, be inaccessible, or be otherwise nonexistent.[50] Investigators may also simply fail to gather all available information from both offline and online sources.

Today, citizens and journalists are increasingly documenting human rights violations from the frontlines and sharing that information online.[51] Once such documentation undergoes an extensive verification process by an established expert or expert community, such online information can be helpful for strengthening cases and should be admissible in court, especially if witnesses can testify to its veracity

II. RECOMMENDATIONS FOR LAWYERS SEEKING TO INCORPORATE OPEN SOURCE EVIDENCE IN INTERNATIONAL CRIMINAL TRIALS

As noted above, online open source investigative methods relevant to international criminal investigations have largely been pioneered by investigative journalists, the intelligence community, and human rights activists. However, international investigators and prosecutors are increasingly recognizing that the protocol for determining what online content is potentially relevant, how information is captured and preserved, and how such information is presented in court can radically differ when used for legal as opposed to intelligence or advocacy purposes.[52] Thus, there is a significant need for standards that bring consistency to the field so that (1) international investigators can manage online content to maximize its potential value, and (2)

---

[48] INTERNATIONAL CRIMINAL COURT, SITUATION IN COTE D'IVOIRE: PROSECUTOR V. LAURENT GBAGBO AND CHARLES BLÉ GOUDÉ (2019), *available at* https://www.icc-cpi.int/CaseInformationSheets/gbagbo-goudeEng.pdf.

[49] *See, e.g.*, Oumar Ba, *The International Criminal Court just acquitted the former Ivory Coast president. What happens now?*, WASHINGTON POST (Jan. 22, 2019), https://www.washingtonpost.com/news/monkey-cage/wp/2019/01/22/the-international-criminal-court-just-acquitted-the-former-ivory-coast-president-what-happens-now/?utm_term=.774e53a0a9b3.

[50] UNIV. OF CAL. BERKELEY SCH. OF LAW: HUMAN RIGHTS CTR., DIGITAL FINGERPRINTS: USING ELECTRONIC EVIDENCE TO ADVANCE PROSECUTIONS AT THE INTERNATIONAL CRIMINAL COURT 3 (2014), *available at* https://www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf.

[51] *See* Hamilton, *supra* note 12, at 3–4.

[52] Alexa Koenig et al., *supra* note 3, at 694.

judges and other decision-makers know how to evaluate the reliability of that information and assign it appropriate weight.[53]

Ideally, such standards would operate at a high level, addressing the big picture of how an investigation should be conducted, how digital information should be stored, how to preserve a digital chain of custody, and how to think about the legal and ethical responsibilities that court actors may have to those who forward information for court purposes or to those who are otherwise connected to that information. The standards should not get into the details of which software to use or the exact methods of analysis because the various tools and methods change quickly. Doing so would potentially render the standards obsolete. Instead, the focus should be on basic principles of data collection, storage, analysis, and presentation.

In October 2017, eighteen experts from around the world—including international prosecutors, digital forensics experts, open source investigators, academics, diplomats and activists—gathered in Bellagio, Italy to discuss the growing practice of conducting open source investigations for international accountability purposes, and to begin a dialogue around the development of legal standards, including a possible protocol.[54] Participants included representatives from the ICC, the Commission for International Justice and Accountability, the Geneva Academy, the Association for the Study of War Crimes, WITNESS, Amnesty International, and the Syrian Archive.[55] Consensus was reached on several key issues. For instance, the parties agreed upon definitions relevant to open source investigations conducted for international legal purposes and several recommended outputs for helping to advance this field of practice, including an international protocol designed to increase the quality and consistency of the use of open source methods for evidence collection and verification.[56] As a result, the Human Rights Center at the University of California, Berkeley began drafting an international protocol with support from a wide circle of advisors, with a probable release date by 2020. The protocol will be translated into multiple languages for the broadest possible application. The audience will include first responders, NGOs, court actors, national war crimes teams, activists, and others who are not operating under a specific Standard Operating Procedure (SOP).

---

[53] THE NEW FORENSICS USING OPEN SOURCE INFORMATION TO INVESTIGATE GRAVE CRIMES, *supra* note 5, 15–17, 19.
[54] *Id.* at 13.
[55] *Id.* at 14.
[56] *Id.*

The experts also agreed upon the need to develop a community of practitioners that can peer review online open source investigations, including the potential development of an ongoing roster of experts.[57] At a minimum, this community will attempt to advance relevant methods, encourage ethical practice, and identify individuals with specific methodological expertise.[58]

In addition to reaching consensus on key definitions, the group agreed on principles that should—at a minimum—underlie the protocol. These include the need for[59]:

1. preservation (to ensure that information that is uploaded to the internet is not lost to history if, for example, it is removed by platforms for violating terms of service agreements or community guidelines, or for other purposes);
2. legality (to ensure that investigations do not fall afoul of human rights norms, privacy considerations, or the law);
3. transparency of methods (any expert in open source investigations should be able to understand the methods that were used and explain them to a court; ideally, peer investigators should be able to replicate the investigation process and reach similar conclusions);
4. security (a mitigation of harm provision that should take into consideration the physical, digital, and psycho-social well-being of the investigator, the investigated, the person who created and/or posted the item to the internet, and anyone featured within that item); and
5. objectivity (when conducted by legal investigators, the investigation should not favor either side, but instead should focus on both incriminating and exonerating information).

An overarching consideration is ethics, which may manifest in different ways across these five principles. Moreover, creative thinking and mastering diverse verification techniques can heighten the reliability of the evidence. On the discovery side, it is important to assess how

---

[57] *Id.* at 13.
[58] *Id.*
[59] *Id.* at 8–11.

people in a given community communicate and turn to those sources for potential information; for example, turning to Twitter makes little sense if no one in that community uses it. It is equally important to assess the terms used by that community (including slang, which can be used to locate relevant online conversations), the sometimes-diverse spellings of key names, and variations in the location, gender, and age of users.

Any open source information used in court proceedings should be carefully verified. As mentioned earlier, verification should include a minimum of two steps: (1) verification of the source and (2) verification of the content. Primary objectives should include validating the source or the initial creator and the individual who uploaded or shared the content, the location and time the content was created, and the "reason" the content exists. Answering the who, what, where, when, why, and how underlying digital data helps maximize that information's potential use by prosecutors by helping place that information in context, and helps judges award information appropriate weight when entered into evidence.

A wide variety of information can be used to help verify the content of photographs and videos. Such information includes: (1) the identification of any metadata; (2) geolocation of any images (for example, using satellite imagery to identify the probable location of distinctive background markers, such as notable buildings or other surroundings); (3) chronolocation, like using sun calculation tools to corroborate probable time of day, or using weather records to help confirm the purported date or location; (4) background research into the uploader and/or original documenter to determine if it is likely that she was actually where she would have needed to be to capture the information (for example, scanning social media to see if the documenter regularly posts information from or about that country or apparently visited the country around that time); and (5) the use of newspaper articles and NGO reports to check external consistency and provide context.

A. Gathering Metadata

While the admissibility of digital evidence varies across jurisdictions, certain practices maximize the potential for acceptance. Metadata may help establish the time and date the file was created, any associated account, information about the device the file was created on, and any edits made to the file.[60] Ideally, metadata is available to help verify and authenticate potential evidence. Electronic documents, such as word documents, often contain metadata that may aid in the verification

[60] *See* The Engine Room, *supra* note 30, at 36.

of the content.[61] The data is automatically produced by the software or may be supplied by the item's creator.[62] Since metadata is typically generated automatically, often without the knowledge or aid of the user, it is less likely to be manipulated or deleted than other content.[63] In the case of video footage, investigators may be able to use metadata to determine the location of the place featured in the video and the creator of the video, which can then be extrapolated out to investigate featured events.

The interpretation of metadata, however, requires a set of fundamental assumptions. For instance, one must assume that the time zone on the device correctly reflects its surrounding environment at the time of the information's creation and that no one overrode or contaminated the metadata.[64] Thus, corroboration of metadata is often necessary.

B. Establishing Chain of Custody

Chain of custody[65] is a fundamental and critical issue for physical and offline documentary evidence, yet it is often overlooked by activists when securing potential evidence from open sources. The preservation of chain of custody can enhance transparency around how the investigator acquired the information and help ensure a lack of tampering with any collected information.[66]

Two of the biggest concerns with digital evidence are the risk of manipulation and the risk of take down, especially regarding graphic or controversial imagery. Archiving any photograph or video found online helps ensure that material will still be accessible for court purposes, even years in the future. It also ensures that legal actors can reference the video, photograph, post, or other content without solely relying on screenshots, which—like any digital image—can be manipulated. Tools such as Meedan's Keep,[67] Enrique Piracés' Video Vault,[68] and the

---

[61] STEPHEN MASON & DANIEL SENG, ELECTRONIC EVIDENCE 27 (4th ed., Inst. of Advanced Legal Stud., Sch. of Advanced Study, Univ. of London 2017).
[62] *Id.*
[63] Manipulation is still possible and several social media platforms automatically strip content of related metadata. *Id.*
[64] *Id.* at 28.
[65] Preserving chain of custody consists of documenting who had access to a unit of evidence and when, as an accountability mechanism to protect against anyone tampering with that evidence. BLACK'S LAW DICTIONARY (10th ed. 2014).
[66] *See* The Engine Room, *supra* note 30, at 36.
[67] MEEDAN, https://meedan.com/en/ (last visited Feb. 16, 2019).
[68] VIDEO VAULT, https://www.bravenewtech.org/ (last visited March 22, 2019).

Internet Archive's Wayback Machine[69] can be used to safely store digital files in a virtual space to mitigate the risk of an uploader or an adversary deleting the original. Tools like Hunch.ly[70] take chain of custody to the next level so that the path can later be forensically analyzed by not only making it possible to access the acquired information, but also creating a record of how the digital search was conducted. Increasingly, legal investigators are "hashing"[71] content so that they can later confirm the integrity of the evidence by checking that it hasn't been modified since the original capture.[72]

However, investigators rarely start the chain of custody. Frequently, electronic evidence, especially in the form of video, is shared via private networks. This makes it impossible for investigators to verify the original time of the content's creation and the initial individuals through whom the content passed. The mere act of examining digital data—reading or opening an electronic file—risks contamination. Furthermore, videos shot by non-professionals are often of relatively poor quality, making verification more difficult. While technology companies, such as Facebook, Twitter, and YouTube, do store metadata affiliated with videos and photographs internally, they are reluctant to release that information for international criminal justice purposes without going through a mutual legal assistance treaty (MLAT) or other formal court process, in part to avoid endangering users or infringing on user privacy. The higher standard for open source materials to be used for trial, versus the standard for journalistic and/or human rights advocacy purposes, makes documenting all discovery, verification and preservation practices a necessity. Ensuring evidence is admitted and accorded significant weight by judges may largely depend on the amount of metadata collected, the preservation of chain of custody, and the quality of verification and authentication.

---

[69] INTERNET ARCHIVE'S WAYBACK MACHINE, https://archive.org/web/ (last visited Feb. 16, 2019).

[70] HUNCH.LY, http://hunch.ly (last visited Feb. 16, 2019).

[71] Hashing is using a mathematical function to generate a value or values that can be used to protect the security of a digital item from tampering. Comparing a digital unit's hash values at different time points can establish whether that unit has been modified in the intervening time period. (If the numbers match, the unit hasn't changed.) *Hash Functions*, NAT'L INSTITUTE OF STANDARDS & TECH. (Jan. 31, 2018), https://csrc.nist.gov/projects/hash-functions/sha-3-project.

[72] *See, e.g.*, Jeff Deutch & Hadi Habal, *The Syrian Archive: A Methodological Case Study of Open-Source Investigation of State Crime Using Video Evidence from Social Media Platforms*, 7 STATE CRIME J. 46, 58 (2018) (discussing the hashing of videos derived from open source content).

There are both internal and external markers of reliability that increase the likelihood that digital data can be authenticated. The following chart specifies metrics for both categories:

Category	**Internal Markers**	**External Markers**[73]
Metadata	Date stamps, timestamps, digital signatures, GPS data and triangulation, watermarking	Source
Location	Street signs, prominent landmarks	Storage/ Chain of Custody
Integrity	Whether tampered with, via editing or manipulation	Testimony
Continuity	Capturing event in its entirety, people arriving/leaving, surroundings	Replicable process for gathering and storing the evidence
Identity	Hash values that serve as a unique identifier and can be assigned to a single file or group of files.	Consent of use in legal proceeding

Taking into consideration these internal and external markers can help investigators and prosecutors maximize the legal value of the information they collect and help judges and other fact finders assess both its veracity and its reliability.

CONCLUSION

As mentioned above, guidelines, including an international protocol, are currently being developed to clarify the basic practices and minimum standards that should be employed when conducting online open source investigations and verifying that content for courts. Such guidelines will help international criminal investigators obtain appropriate information for prosecution and provide support for how information should properly be acquired, preserved, and presented. While the amount of digital data accessible to legal investigators will continue to grow exponentially, digital evidence must be properly stored,

[73] New Perimeter: Our Global Bono Initiative, *Using Photos and Videos as Evidence*, DLA PIPER 13–14 (June 18, 2012) (on file with authors).

catalogued, and mined in order to avoid a digital backlog.[74] Ultimately, international criminal investigators should adhere to forthcoming standards to ensure that the paramount images—those images that frontline activists and survivors may risk their lives to acquire—can realize their full potential in court.

[74] *See* Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, 41 FORDHAM INT'L L.J. 283, 333–35 (2018) (discussing the importance of lawyers using new technologies to manage digital evidence.