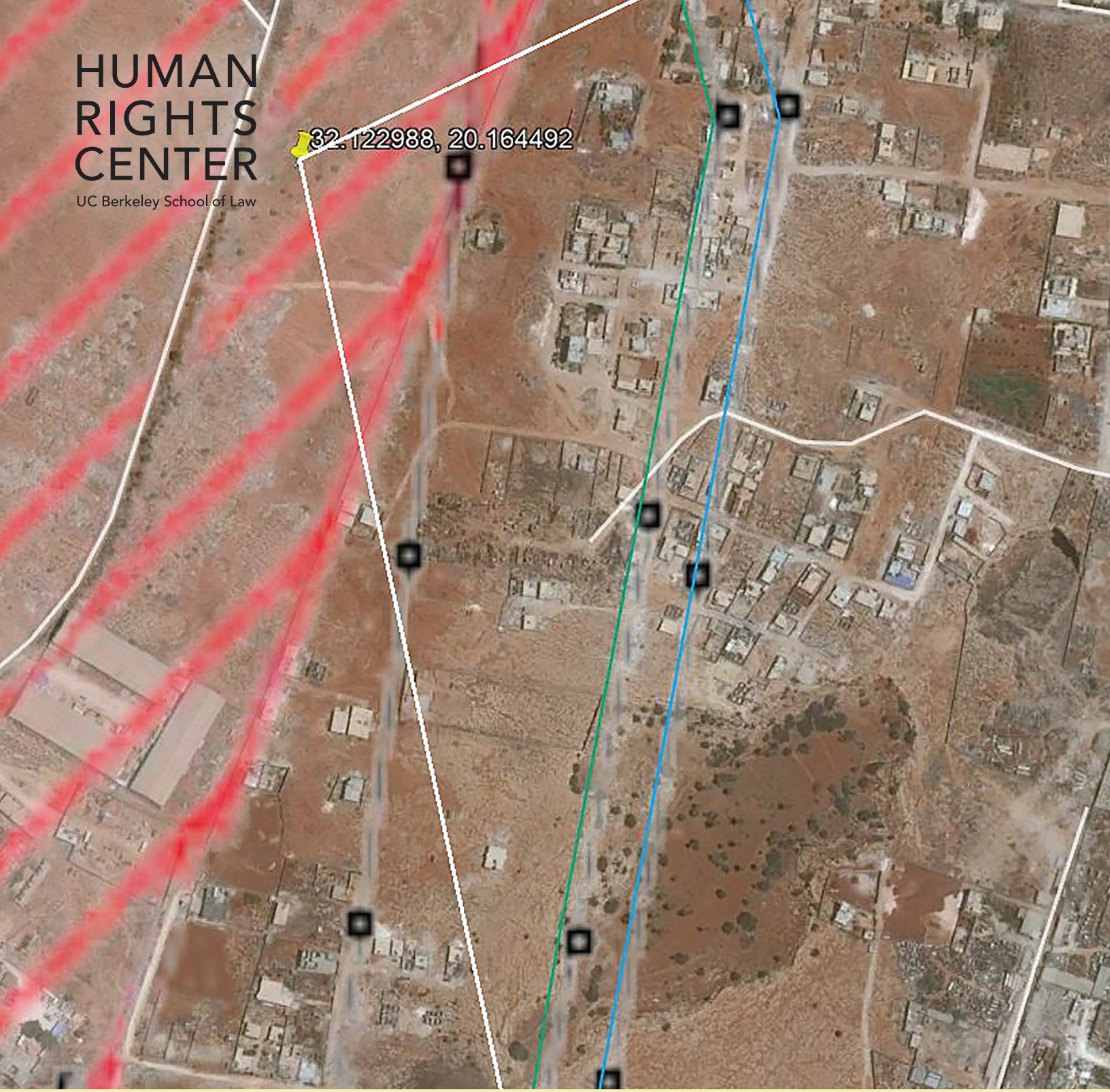

HUMAN RIGHTS CENTER

UC Berkeley School of Law

THE NEW FORENSICS

Using Open Source Information to Investigate Grave Crimes

HUMAN
RIGHTS
CENTER
UC Berkeley School of Law

THE NEW FORENSICS

Using Open Source Information to Investigate Grave Crimes

Human Rights Center
School of Law
University of California, Berkeley

Pursuing justice through science and law

The Human Rights Center at the University of California, Berkeley, School of Law conducts research on war crimes and other serious violations of international humanitarian law and human rights. Using evidence-based methods and innovative technologies, we support efforts to hold perpetrators accountable and to protect vulnerable populations. We also train students and advocates to document human rights violations and turn this information into effective action.

Human Rights Center, UC Berkeley School of Law, 396 Simon Hall, Berkeley, CA 94720
Telephone: 510.642.0965 | Email: hrc@berkeley.edu
Web: hrc.berkeley.edu and Medium.com/humanrightscenter | @HRCBerkeley

Cover photo credit: Eliot Higgins, Bellingcat
Report design: Nicole Hayward

CONTENTS

INTRODUCTION

THIS REPORT *The New Forensics: Using Open Source Information to Investigate Grave Crimes* highlights the discussion, conclusions, and recommendations from an historic workshop on evidence collection and legal accountability that the Human Rights Center hosted in Bellagio, Italy, from 2–6 October 2017. Workshop participants explored how online open source investigations—internet-based investigations that rely on publicly accessible information—can be strengthened to improve investigations and prosecutions by uncovering critical evidence of serious international crimes, including genocide, crimes against humanity, and war crimes. This workshop is the first international effort to begin harnessing the probative power and potential of open source investigations for legal accountability.

Workshop participants included specialists in open source investigations, investigators and prosecutors from the International Criminal Court ("ICC" or "Court"), senior trial attorneys from other international tribunals, human rights investigators, and individuals with expertise developing human rights protocols and guidelines.

The workshop is the fourth in an ongoing series exploring how prosecutions of serious international crimes can be strengthened through the diversification of evidence, with an emphasis on adopting and adapting new and emerging technologies. The other three workshops and subsequent reports in the series include *Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the International Criminal Court* (2012), *Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court (2014)*, and *First Responders: Collecting and Analyzing Evidence of International Crimes* (2014). Special thanks to the Rockefeller Foundation for hosting the workshop and to Open Society Foundations, Humanity United, the Oak Foundation, and Sigrid Rausing Trust for their additional support.

The Bellagio Workshop on Open Source Investigations explored three key areas:

- *Historical Context and Need:* The workshop covered the historical and social origins of open source intelligence gathering and investigations, including why and how they have become critical for grave crimes investigations and prosecutions. This included the historical use of open source-derived information in international criminal investigations; contemporary examples of the use of open source information in international criminal investigations; an overview of processes used to develop and disseminate protocols and guidelines through the United Nations system; and the current use of—and challenges with—open source investigations at the ICC.

- *Challenges*: Participants identified and attempted to address disparate challenges related to open source investigations. These included the need for common definitions and principles that should underlie the development of international standards around open source investigations, as well as urgent issues related to crowdsourcing, discovery, preservation, presentation, and potential defence concerns.
- *Next steps*: Developing recommendations for potential deliverables as well as processes for fulfilling those recommendations and producing those deliverables.

BACKGROUND

THE INTERNATIONAL CRIMINAL COURT (ICC) issued an arrest warrant in August 2017 for Mahmoud Mustafa Busayf Al-Werfalli, a Libyan national, for alleged war crimes, including the execution of 33 prisoners in the vicinity of Benghazi between June 2016 and July 2017. What makes this warrant especially notable is that it is largely based on seven separate executions captured on video and obtained from social media.

The Al-Werfalli case is among the first in a new era of international criminal investigations and prosecutions that increasingly rely on open source information—which is publicly accessible on the internet, including photos, videos, and contextual information—to identify, document, and verify serious international crimes. The law has not caught up with technology. Even as this new era is upon us, no common international standards exist for gathering, handling, preserving, and presenting open-source evidence in international and national courts that can help maximize the weight accorded such information.

Global leaders in this field met in Bellagio, Italy, in October 2017 to discuss this gap and create a plan to draft standards to advance the use of open source information as evidence.

While journalists often collect and analyze open source information, its use by international and national prosecutors to investigate war crimes is relatively new. And as potential evidence of such crimes increasingly appears online, minimum standards need to be established to ensure that such information is captured and preserved in a manner that is admissible in criminal proceedings.

The meeting objectives included:

1. Providing guidance for potential legal standards for open source investigations intended for use in legal procedings: How do we make sure information derived from open sources is admissible and carries the maximum weight possible?
2. Identifying the principles that should underlie the development of legal standards: How do we create high-level principles that are useful for diverse legal jurisdictions, including the ICC and regional and national courts?
3. Determining how best to mature this field of practice: Do we need an international protocol, a set of guidelines, or other guidance?

Workshop participants included representatives from the ICC, the Commission for International Justice and Accountability, the Association for the Study of War Crimes, WITNESS, Amnesty International, the Syrian Archive, the University of Pretoria, and the Human Rights Center, among others.

Participants emphasized the need to:

- Preserve and manage information gleaned from open sources in a systematic way;
- Identify procedures for organizing video archives and other datasets so as to

facilitate their use by international criminal investigators; and
- Cultivate a community of practice and a system of peer review, as well as the development of ethical standards and the sharing of new investigatory methods and procedures.

The group recommended that the Human Rights Center spearhead the development of guidelines to increase the quality and consistency of the use of online open source information for evidence collection and verification. The primary audience for the guidelines should be NGO investigators, international and national tribunal investigators, prosecutors, judges, defence attorneys, journalists, and academics. The guidelines and a set of principles aimed at maximizing the potential value of open source information in courts should be disseminated to a wide circle of advisors for input and finalized at a workshop in 2018.

This process would build on earlier investigatory efforts to increase the diversity and quality of evidence of serious international crimes. Several decades ago, for example, DNA analysis was a cutting-edge practice that had to gain acceptance by the scientific and legal community as an appropriate form of forensic evidence. Other examples include the standardization of the forensic documentation of torture, which resulted in the Istanbul Protocol, and the investigation of suspected extrajudicial killings, which resulted in the Minnesota Protocol. These protocols helped set investigatory practices for these emerging fields.

Below, we discuss insights, conclusions, and recommendations from the meeting at Bellagio.

MAJOR ISSUES, TRENDS, AND CONTEXT

PARTICIPANTS SPENT THE FIRST DAY discussing the historical context and trends related to law and technology. They identified major issues and challenges to be delved into more deeply in the following days.

Alan Tieger drew on his experience as a prosecutor with the International Criminal Tribunal for the former Yugoslavia to provide an historical understanding of the use of open source materials in international criminal tribunals. Previously, war crimes tribunals relied on open sources that included books, documentary reports, and photographs. Digital open source resources, by contrast, played an "honorable but not pivotal role in investigations." He explained that despite these differences in content or delivery systems, all admission of evidence is and will be grounded in principles of reliability and probative value. While application and understanding of these principles may vary from chamber to chamber, judicial responses will be centered on whether the proposed material is sufficiently reliable to enter as evidence such that it becomes helpful to drawing conclusions. Several factors affect reliability, including—but not limited to—provenance, purpose, context, and internal/external markers of reliability. Importantly, reliability is not assessed in a vacuum, but within the context of a large repository of evidence. Open source materials become part of the totality of evidence. While every evidentiary item should be evaluated and afforded its proper weight, that weight depends in part on the other information around it. Thus, there is no mechanical or bright line test for the admission of any information, including open source material. The role for investigators using these methods is to help the court understand why this particular information should become part of the body of evidence. Therefore in creating standards, reliability should be the base consideration.

Lindsay Freeman, a Human Rights Center Researcher and graduate student at Leiden University, provided recent examples of the use of open source information in international and national cases.[1] She highlighted the similarities in complexity of scientific evidence and digital evidence and the responsibility of investigators to be careful in their use and analysis of that information. She recounted her experiences as a lawyer and investigator, citing the unreliability of certain metadata (such as time stamps on video footage), degradation of video with multiple transfers, subjectivity in interpreting visual imagery, ambiguity in low-resolution photographs and satellite imagery, lack of distinctiveness in city landscapes, and more. Freeman also discussed authenticity and the "best evidence rule" that would require the production

1 For more information, please see her working paper, *Using Open Source Methods to Gather Evidence of War Crimes and Human Rights Abuses*, which was provided as a resource for participants prior to the workshop and is available on the Human Rights Center website.

of an original "document"—a practice that is often impossible or hard to document when it comes to open source and digital material. She explored the duty of disclosure, and its relationship to the duty to properly preserve digital data. Freeman also discussed some pitfalls related to the proactive use of open source investigations, including "crowdsourcing" that can lead to a "crowd mentality"—for example, the misidentification of Sunil Tripathi as the Boston Marathon bomber and harassment of his family. Freeman also touched on the use of open source material in international cases, including the recent Al-Werfalli case in Libya.

Stuart Maslen discussed the process of developing and disseminating standards for forensic information, drawing from insights related to the Minnesota Protocol on the investigation of potentially unlawful death. He said that we may want to look to the domain of "soft law"—such as establishing guidelines—rather than the legally binding hard law that would lead to the creation of an international treaty, for example. Maslen highlighted similar efforts that have been processed through the United Nations, such as the Office of the High Commissioner for Human Rights, or the InterAmerican court, or via national jurisdictions.

Several members of the ICC's Office of the Prosecutor (OTP) also presented. They laid out the OTP's current and upcoming efforts to enhance the use of open source information in their investigations and prosecution processes. They explained how Facebook, YouTube, and Twitter had become a critical source of information for current investigations but how the lack of clarity around standards made it difficult to know how best to organize and present material. ICC representatives also covered the mechanics of how they capture and preserve information derived from open sources.

With this background, the group identified the need to start by developing definitions and relevant principles—a task that was undertaken on the second day of the workshop.

DRAFT DEFINITIONS AND PRINCIPLES

Definitions

On the second day, workshop participants focused on establishing key terminology related to open source investigations, developing definitions for that terminology, and identifying key principles that could provide a foundation for future guidelines. It was noted that several terms were being used interchangeably and, in many cases, inappropriately (for example, most open source information was being referred to by practitioners as open source intelligence or OSINT even when not used for intelligence purposes; information from social media was being described as evidence when not being used as evidence in a legal sense).

Participants reached consensus on the terms to be defined and the content of those definitions. It was agreed that definitions should be simple, with commentary added to provide insight as to how the definitions were derived and the choices that were made regarding phrasing. They especially focused on four terms: "open source information," "open source investigation," "digital investigation," and "online open source information," and distinguished those terms from what has been inappropriately used as a "catchall" term, namely "open source intelligence," also known as OSINT.

Participants reached consensus on the following draft definitions:

Open Source Information is *publicly available information*. Open source information is not defined by its specific source (whether digital or analog) or how that information is disseminated. Instead, it is information that can be accessed without the need to seek a warrant or employ other coercive or illegal measures. Participants agreed that open source information should be distinguished from open source intelligence, the latter of which is a *subcategory* of open source information, which is used for intelligence purposes. The ethics and legality of the use of open source information has no bearing on the term's definition.

Online open source information is *information that is publicly available on the internet*. Open source information may include (but is not limited to) that which is created, shared, or collated by journalists and news organizations; state agencies; political and military actors; commercial entities; international organizations; nongovernmental and civil society organizations; academics and academic institutions; private individuals; and groups of individuals with military, political, commercial, professional, and personal affiliations. Common types of online open source information include online news articles; expert and NGO reports; social media

content; image and sound recordings; geospatial imagery and mapping data; documents, including public administrative records and leaked confidential documents; library holdings, and more.

Online investigation is *the process of identifying, collecting, preserving, or analyzing information on or from the internet, whether via open or closed sources, as part of an investigative process*. The investigative process includes—but is not necessarily limited to—searching, reviewing, and deciding what to collect and what not to collect. This includes developing the initial query; defining search parameters; outlining security considerations; conducting the search (whether manual or automated), with an emphasis on locating and preserving the original or earliest posting (although "near duplicates" posted by later actors may provide critical information relevant to a case); recording the process, whether automated (as with Hunchly, WASP, the Internet Archive, Keep, or other tools), or manual (by keeping detailed notes), and preserving the materials. Information derived from an online investigation should be stored in two buckets, a "sandbox" for exploring what has been collected and its potential relevance to investigations and an "evidence vault," which triggers disclosure obligations.

Online open source investigation is *the process of identifying, collecting or analyzing information that is publicly available on or from the internet as part of an investigative process*. In addition to the points made about open source investigations, like all investigations, and online investigations above, ethical considerations include the scope of consent provided by the platform or poster, as well as how data is managed and stored.

Online open source investigations for international and national criminal investigations, like all investigations, can be conducted for diverse purposes, which may include (but are not limited to) crime pattern analysis, victimization, leads development, and establishing a conflict's background or context and the identity of witnesses and other persons or organizations of interest; linking individuals with events; analyzing organizational structures (such as military, political, or other networks); to corroborating other evidence; establishing a timeline of relevant facts and; providing linkage evidence that ties high-level suspects to frontline perpetrators; and to tracking fugitives or material objects. In addition to establishing the *actus reas* (the physical act underlying the crime) open source information can help establish the requisite *mens rea* (mental state of the alleged perpetrator), such as the intent or knowledge.

Workshop participants also recognized a need to define crowdsourcing and crowdtasking, two increasingly common means for gathering and analyzing information from large groups of people. While these terms were not discussed in detail, it was generally agreed that **crowdsourced information is *information obtained through solicitation of a large number of people, either paid or unpaid, typically via the internet*.** In the context of open source investigation, crowdsourcing would be used as a means of advancing an investigation, possibly to identify witnesses or solicit information specific to particular components of an investigation. **Crowdtasking is *the outsourcing of tasks to a large number of people typically via the internet,* in this context for the purposes of advancing an open source investigation.** It was concluded that research into existing definitions of these two terms would be conducted and adapted for purposes of the guidelines.

Principles

Participants also recognized the need to establish a set of principles around which guidelines for open source investigations could later be developed. The draft principles that the group identified and felt should be prioritized included preservation, transparency, legality, security, and objectivity.

Preservation

Social media sites frequently remove graphic content from their platforms, at which point critical

evidence may be lost; in addition, cases might develop years, if not decades, after a crime has occurred and after information has disappeared from the internet. The more information that can be preserved soon after the time of posting, the stronger potential cases will be in the future.

Participants discussed key components of the principle of preservation, including:

- Grabbing the "original" or "first posting" of an item of information and storing it in compliance with forensic standards. However, *preservation of any iteration of the information is better than none*.
- Conducting open source investigations as close in time to the underlying events as possible—ideally contemporaneously to the event. This is why first responders, such as activists and journalists, have become especially helpful to legal accountability processes. They often are collecting, preserving, or analyzing information much sooner than court investigators, who may not have jurisdiction over a particular incident until years or decades after the event.
- Preserving metadata, links, networks, content, and all comments from relevant social media and other sites. This can be done manually or via scraping (extracting data from online platforms). While the scraping of online platforms may violate terms of service, such violations will rarely destroy the data's value for legal purposes, at least in international tribunals. Of course, such automated processes may raise ethical considerations, including data minimization and data lifecycle considerations, etc.
- Preserving "chain of custody," ideally in compliance with forensic standards and procedures. This can be done manually (e.g., with careful notetaking about process and content) or automatically (e.g., using electronic tools like Hunchly). Ideally, the investigator will preserve the "original" and a copy to work on. The data should be archived, marked, and coded or otherwise organized so it can later be found and accessed, even if its use is years or decades later. This can be done via "hashing," the use of "blockchain," via Keep or the Internet Archive, or other means and methods.
- Ensuring the organization and searchability of archived information. The process can be automated (taking into consideration ethical issues, such as data minimization concerns or volume-related challenges). It should be noted that certain tagging and other categorization, particularly of videos or photographs, may require human involvement and judgment that cannot be automated—at least not yet. The overarching goal of preservation is to not lose track of the information, especially when it may not be needed for some time. Investigators should think through how the information can be safeguarded and managed for the long-term as opposed to merely short-term use.

In order to maximize the likelihood that the preserved information will be found admissible in an international or national court, investigators will need to (1) log their own IP address (to establish that they were connected to the internet at a particular date and time via a particular computer);[2] (2) connect to a time server to ensure the computer clock is accurate; and (3) screenshot the data they want to collect. Ideally, investigators will also capture the full source code underlying the target information. Of course, that work is not necessary if one can get data directly from an ISP host.

2 Logging the IP address of the investigator's computer is complicated by the relatively common use of TOR, which masks the IP address, by NGOs to conduct open source investigations. NGOs should take into account that the higher the standard used in information retrieval and preservation, the less likely the investigator will have to testify to have that information be useful, as careful documentation may provide some degree of self-authentication.

Transparency of Methods (Accountability)

All steps in the online open source investigation process—from identification of relevant material through preservation, analysis, and reporting—should be transparent and therefore accountable and reliable. Transparency is particularly important for potential replicability, the standard underlying scientific information. Can investigators who did not conduct the original investigation and analysis attest that the methods used were appropriate to the investigation and that they could or would reach the same or similar conclusions using the underlying materials? To the extent possible and reasonable, investigators should maintain clear records regarding their processes, including preservation of chain of custody of all collected information, and engage in record keeping around how the investigation was conducted.

Legality

Investigators should understand the exclusionary and other rules of evidence of any relevant jurisdiction before designing and conducting an online open source investigation. When conducting such an investigation, it is important to think through whether there are laws that might preclude the use of the information collected as evidence, especially in national proceedings. In international courts, this may not be as important: a wide range of information is admissible in international tribunals, but the weight accorded that information might vary.

In the case of the ICC, open source investigation activities are required to comply with the legal framework of the Rome Statute and the Office of the Prosecutor's operational standards and procedures. Specifically, investigators must honor the rights of persons pursuant to Article 55. Evidence will not be admissible if collected by means of a violation of the Rome Statute or of an internationally recognized human right that casts (1) serious doubt on the information's reliability, or (2) serious damage on the integrity of the proceedings, per Article 69. In addition, the protection of victims and witnesses, per Article 68, is paramount. The need for investigations should be balanced with the right to privacy and the duty to protect staff, witnesses, and members of the public.

Ultimately, international courts are required to comply with human rights laws. Violations of such laws may result in exclusion of the relevant information.

Objectivity (Equality of Arms)

Open source investigations should include both incriminating and exonerating materials without favor. In the case of the ICC, this is required by Rome Statute art. 54(1)(a). Objectivity should be integrated into the development of search parameters, including the selection of search terms and the design of algorithms for automated searching, as well as in the review of collected materials. To counteract bias, workshop participants discussed the value of approaching investigations from the perspective of employing multiple working hypotheses or proving a null hypothesis. They also emphasized the importance and value of peer review, as well as employing two factor authentication, which means analyzing both the *content* and the *source* of the relevant information.

Security

"Do no harm" should be the first consideration of any investigation.[3] An open source investigator should think through the digital, physical, and psychosocial security of those with whom they're interacting and anyone identified in the collected information, as well as herself and any affiliated staff. The investigator should also consider and plan for data security.

---

3 See Maria Nystedt, Christian Axboe Nielsen, and Jann K Kleffner, *A Handbook on Assisting International Criminal Investigations*, Folke Bernadotte Academy and Swedish National Defence College, 2011, pp. 46–48, available at: https://fba.se/en/how-we-work/research-policy-analysis-and-development/publications/a-handbook-on-assisting-international-criminal-investigations/.

Integrity

All materials that are collected should be preserved with the same characteristics as the original (or as close to that as possible). Some form of chain of custody should be maintained in order to support the integrity of the materials. This process may include taking notes or using automated tools for preservation (see preservation, above). It may also require that investigators and analysts provide on-the-record testimony about how the materials were collected, preserved, and analyzed or expert testimony on professionally accepted standards and procedures. All investigative steps need to be recorded, whether manually or automatically. Investigators who testify in proceedings will be expected to review and answer questions about all investigative decisions and any action taken as part of the investigative process.

Ethics

The need for ethical practice is not a principle per se, but something that runs through all of the principles. This includes thinking through data ethics, such as appropriate management of the data lifecycle and data minimization principles (which require collecting no more information than needed); the increased vulnerabilities that data collection may create for witnesses and others; and the need for informed consent of use of the underlying materials for legal accountability purposes. Investigators should also be mindful of their "footprint"—for example, too many people accessing the same website might raise flags that are problematic for others. Investigators reaching out to the same people may also be burdensome for those sources.

Additional considerations for open source investigators

Disclosure considerations

NGOs and other organizations and individuals must be aware that when information is turned over to prosecutors everything—with very rare exceptions—must be disclosed to the defence. Disclosure obligations may vary by judge/chambers. Potential problems with disclosure start with how information is collected and indexed (there must be clarity so that the investigator or prosecutor knows what information is in the collection and can share that with the defence). The investigator or researchers should properly describe, index, make searchable, and avoid duplication of information. Typically, international prosecutors will write a disclosure memorandum. The goal should be to make the information as accessible and easy as possible for disclosure purposes.

Verification and authentication procedures

NGOs should also think critically about verification and authentication procedures. Ideally, they will use a minimum two-step verification process that includes (1) *source* verification and evaluation, and (2) *content* verification and evaluation. At a minimum, the coding of any archives should include the following: who (names of individuals, unit, command, etc. with consistent descriptions that may include a coding scheme); what (document? photo? video?); where (coordinates? city?); and when (date, made as narrow as possible).

If working to support a particular case, the investigator may want to develop a coding scheme based on the charges. If the investigator is not working on a particular case, coding based on the charges should probably be avoided, although a generic coding system should still be used so that relevant information can be discovered.

Crowdsourcing

While crowdsourcing offers tremendous potential to supplement the investigatory and verification work of court investigators, it also offers particular challenges. Once ICC investigators possess information, they must be prepared to disclose it. For example, investigators must be able to disclose any information that has been emailed to and opened or downloaded by them. The nuances of disclosure

are particularly important when court investigators work with crowdsourced information as they alert any participants to disclosure obligations before soliciting information. There is also a need to provide knowledge of the potential use of the information for legal purposes and to secure the consent of the creator. Importantly, anyone who decides to share information with ICC investigators for legal accountability purposes (e.g. a journalist or NGO investigator) cannot decide later that they want to retract that information.

Importantly, whoever conducts an open source investigation and shares that information with a court lawyer must be prepared to testify at trial. Ideally, an investigation will be structured so the minimum number of people will need to testify and that same procedure is followed each time. If numerous people are working as a team, the person with enough frontline knowledge to testify about the investigation process should be the point person to be prepared to go to the court.

Finally, secondary or peer review should become standard practice. For example, it can be helpful to court investigators if different NGOs have reached similar conclusions using open source materials. This secondary or review can be used to support replicability (bringing such investigations closer to a scientific standard), strengthening confidence around validity and general quality control, and minimizing the risk of bias.

RECOMMENDATIONS

Workshop participants recommended that the Human Rights Center, in partnership with others, do the following:

1. **Produce a glossary of relevant definitions based on the definitions outlined during the workshop.** This glossary should be widely disseminated to bring consistency to terminology used in the field.

2. **Refine a set of underlying principles relevant to open source investigations upon which any future guidelines or other standards could be based.** These principles should include the principles identified during the workshop, although others may be identified and included based on further research.

3. **Produce a substantive document that captures the history and legal context of open source investigations.** This could be included in the draft guidelines or published separately.

4. **Produce guidelines to support the improved quality of open source investigations for legal accountability.** The Human Rights Center will take lead on drafting guidelines with input from worshop participants and other open source investigations experts. The guidelines should then be disseminated to a broad and geographically diverse circle of advisors for commentary before finalization. Once finalized, the guidelines should be translated into multiple languages for broadest possible application. The audience should include NGO investigators, tribunal investigators, prosecutors, judges, and defence attorneys, as well as journalists and others who are not operating under a specific set of standard operating procedures.

5. **Develop a community of practice that can provide peer review or credentialing of open source investigations,** including an ongoing roster of experts. The aim is to (1) improve open source methods and procedures, and (2) identify people who can serve as peer reviewers. As part of this, participants should and will explore the possibility of starting a chapter at the American Association for the Advancement of Science or another forensically oriented institution.

6. **Develop a website for open source legal investigators.** This site would serve as a shared repository of helpful materials, including the resources identified above and emerging jurisprudence. The site could be housed at the Human Rights Center, University of California, Berkeley, School of Law and operated in partnership with other universities.

APPENDIX A

WORKSHOP PARTICIPANTS

Chairpersons

ALEXA KOENIG, Executive Director of the Human Rights Center and Lecturer, University of California, Berkeley.

ERIC STOVER, Faculty Director of the Human Rights Center and Adjunct Professor, Schools of Law and Public Health, University of California, Berkeley.

Participants

HADI AL KHATIB, Investigator, Bellingcat and Syrian Archive

YVAN CUYPERS, Cyberinvestigator, Office of the Prosecutor, International Criminal Court

SCOTT EDWARDS, Senior Advisor, Amnesty International

LINDSAY FREEMAN, Researcher, Human Rights Center and LLM student, Leiden University

STEVE KOSTAS, Senior Legal Officer, Open Society Foundations

ANDREA LAMPROS, Communications Director of the Human Rights Center and Manager of the Human Rights Investigations Lab, University of California, Berkeley

STUART MASLEN, Honorary Professor, Faculty of Law, University of Pretoria

KELLY MATHESON, Senior Attorney and Program Manager, WITNESS

FELIM MCMAHON, Investigator, Office of the Prosecutor, International Criminal Court

JULIAN NICHOLS, Senior Trial Lawyer, Office of the Prosecutor, International Criminal Court

THOMAS PROBERT, Research Associate, Center for Governance and Human Rights, University of Cambridge

CRISTINA RIBEIRO, Investigations Coordinator, Office of the Prosecutor, International Criminal Court

GAVIN SHERIDAN, CEO, VizLegal

ALAN TIEGER, Senior Trial Attorney, International Criminal Tribunal for the former Yugoslavia

MARK WATSON, Head of Cyber Exploitation and Digital Forensics, Commission for International Justice and Accountability

GUY WILLOUGHBY

This report was authored by Alexa Koenig and edited by Andrea Lampros and Eric Stover. Lindsay Freeman, Kelly Matheson, Stuart Maslen, Thomas Probert, and Alan Tieger also reviewed and provided edits to the report. The Human Rights Center wishes to thank the Rockefeller Foundation for hosting the workshop, and Open Society Foundations, Humanity United, the Oak Foundation, and Sigrid Rausing Trust for their additional support.

APPENDIX B

WORKSHOP AGENDA

OPEN SOURCE INVESTIGATIONS: STANDARDS AND PRINCIPLES

October 2–October 6, 2017,
Bellagio, Italy

DAY ONE: Context and Big Picture

Tuesday, October 3

9:30 AM: Welcome and meeting objectives
Eric Stover and Alexa Koenig

9:45 AM: Introductions

10:15 AM: History of OSINT in international criminal investigations
Alan Tieger

10:45 AM: Contemporary examples of the use of OSINT in international criminal investigations
Lindsay Freeman

11:25 AM: Guideline and protocol processes
Stuart Maslen

12:00 PM: Open source investigations at the International Criminal Court

- Overview *Cristina Ribeiro*
- FSS technical approaches *Yvan Cuypers*

2:00 PM: Open source investigations at the International Criminal Court, continued

- Past case study Al Mahdi *Felim McMahon*
- Current case study: Al-Werfalli *Julian Nichols*

3:00–4:30 PM: Identification of challenges that will be addressed for Day Two (integrating case study) and possible discussion of one or more of those challenges

DAY TWO: Challenges

Wednesday, October 4

9:30 AM: Challenges

- Crowdsourcing
  - active v. passive collection
  - outreach
- Discovery
  - searching
  - monitoring
- Preservation
- Presentation
- Defence concerns
- Other

2:30 PM: Review of Draft Standard Operating Procedures

7:00 PM: Cocktails and dinner at the Villa Serbelloni with the Scholars in Residency

DAY THREE: Next Steps

Thursday, October 5

9:30 AM: Review of major issues from day two

10:00: Guidelines: Draft outline

2:30 PM: Identification of next steps

- Drafting
- Vetting
- Dissemination
- Training
- Working Group

HUMAN RIGHTS CENTER
UC BERKELEY SCHOOL OF LAW
396 SIMON HALL
BERKELEY, CA 94720
510.642.0965

HRC@BERKELEY.EDU
HRC.BERKELEY.EDU
MEDIUM.COM/HUMANRIGHTSCENTER
@HRCBERKELEY