MURAD CODE PROJECT

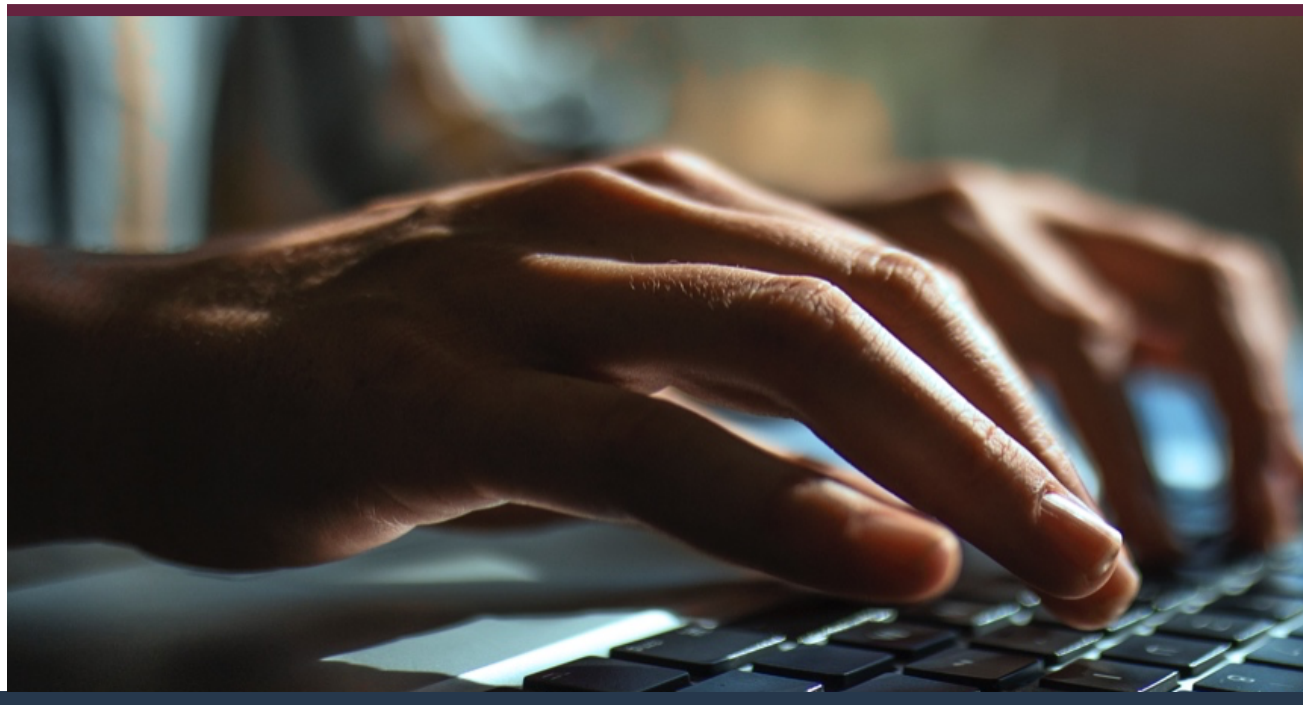
OPEN-SOURCE PRACTITIONER'S GUIDE TO THE MURAD CODE

NOVEMBER 2025

APPLYING MINIMUM STANDARDS FOR THE SAFE, ETHICAL AND EFFECTIVE GATHERING AND USE OF INFORMATION ABOUT SYSTEMATIC AND CONFLICT-RELATED SEXUAL VIOLENCE

Institute for International Criminal Investigations

HUMAN RIGHTS CENTER
UC Berkeley School of Law



MURAD CODE PROJECT

TABLE OF CONTENTS

MURAD CODE PROJECT

ACKNOWLEDGEMENTS

The development of this Guide forms part of the Murad Code project (muradcode.com).

The Guide was produced through a partnership between the Institute for International Criminal Investigations (IICI) and the Human Rights Center at the University of California, Berkeley School of Law (HRC), with critical input from this project's working group and other experts. Following several rounds of reviewing draft versions, a pilot version of the Guide was published for comment in April 2025; this final version integrates feedback received.

The following experts are the main drafters of the Guide: Dr. Alexa Koenig, Anthony Ghaly and Dr. Ingrid Elliott. Other experts contributed significantly to the development and review of the Guide. They include: Maggie Andresen, Hannah Bagdasar, Daniela Baro, Dr. Ulic Egan, Michael Elsanadi, Erin Gallagher, Olivia Head, Manon Louis, Libby McAvoy, Dr. Yvonne McDermott Rees, Nema Milaninia, Maria Mingo, Judy Mionki, Gabriël Oosthuizen, Lina Raslan, Andrea Richardson, Mara Steccazzini, Ben Strick, Gregory Townsend, Philip Trewhitt, Philomène Uwamaliya, Marion Volkmann-Brandau, Rachel Winny and Dr. Sarah Zarmsky. We are grateful for their invaluable assistance, as well as the assistance of those who cannot be mentioned or whose names are unknown to IICI and HRC, but who participated within collaborating organisations to review earlier versions of the Guide. None of these experts or the organisations they may be affiliated to necessarily agrees with all of the content of this version.

Importantly, the Guide was co-developed with survivor experts who have lived experience with systematic and conflict-related sexual violence. However, we realise that the provided guidance may be incomplete or not adequately reflect the full range of experiences and recommendations of survivors.

From 2023 to 2026, the Murad Code project, including this companion Guide, is supported by the government of Canada through Global Affairs Canada. Funding support for the development of the Guide was also provided by the Preventing Sexual Violence in Conflict Initiative of the UK government's Foreign, Commonwealth & Development Office (up to March 2023).

IICI Institute for International Criminal Investigations

HUMAN RIGHTS CENTER
UC Berkeley School of Law

In partnership with Canada

UK International Development
Partnership | Progress | Prosperity

MURAD CODE PROJECT

INTRODUCTION

This is a digital open-source practitioner's guide ("Guide") to conducting survivor-centred and effective research, documentation or investigations about systematic and conflict-related sexual violence (SCRSV). The Guide is framed by the Global Code of Conduct for Gathering and Using Information about Systematic and Conflict-Related Sexual Violence ("Murad Code" or "Code"). It is designed for human rights and criminal investigators, documenters and monitors, journalists, analysts, researchers, activists and others (whether paid or unpaid) who search for or use online digital open-source information and/or who may intentionally or unintentionally come across or handle information related to SCRSV during online inquiries, research, documentation or investigations ("practitioners").

More specifically, this Guide applies:

- to the remote gathering of information about SCRSV (defined broadly and inclusively) or about SCRSV survivors
- through digital open-source research methods (whether that content is text-based, audio-based, image-based or in another form) and
- the subsequent preservation, analysis, sharing, publishing and/or other use of that information
- for any purpose other than for the immediate care or support of survivors
- regardless of whether the discovery and handling of that content is intentional, incidental to other work, or accidental.

Despite the Guide's focus on SCRSV, much of its content may also be useful to practitioners who mainly or exclusively research non-SCRSV human rights violations and crimes.[1]

CONTEXT AND SCOPE

Although one of the main aspects of the Murad Code is interaction with survivors, the Code also captures minimum standards for indirect or remote gathering and use of information about SCRSV and its survivors. Open-source research about SCRSV can be harmful to survivors and others, even when open-source practitioners are not in contact with survivors. Open-source research of SCRSV should and can be survivor-centred, safe and effective.[2] The objective of this Guide is to provide insights and interpretation as to how the minimum standards distilled in the Murad Code can be upheld by open-source practitioners. The Guide has been developed in accordance with Murad Code Principle 8.3, which emphasises that the collection, receipt and use of indirectly sourced information – including online open-source information - implicates significant privacy, legal, security, mental well-being and other risks:

Principle 8.

Gather Information From Other Sources

8.3 ***Recognise rights and risks from indirectly sourced information:*** *We acknowledge that there are privacy, legal and security implications from the collection, receipt or use of indirectly sourced information from or about survivors, even if the information is in the public domain, in archives or retrievable from online (including public and non-public) sources. We recognise that the Code also applies to the gathering and use of such information.*

For open-source practitioners, the bottom-line of the Murad Code is that, while there are good reasons to gather and use online information about SCRSV, such practices should only be undertaken when practitioners can adhere to the minimum standards set out in the Murad Code. This is consistent with Murad Code Principle 4.4 (emphasis added):

Principle 4.

Add Value or Don't Do It

4.4 ***Are our intended outcomes realistic?:*** *We will only undertake this work where our objective can be realistically achieved in that setting with our resources, time and skills,* ***without causing harm.***

AUDIENCE AND TERMINOLOGY

The Murad Code applies to those who "gather" or "use" information in relation to SCRSV and includes those who "document, investigate, report on, research, monitor and otherwise collect ("gather") and use". For practical reasons, this Guide mostly uses the terms 'research' and 'investigate' and variations thereof, and does so interchangeably. However, the use of these terms is not intended to narrow or limit the scope and application of this Guide. The Guide addresses all practitioners who gather or use information about SCRSV, regardless of whether those practitioners describe what they do as documenting, researching, inquiring, fact-finding, investigating, reporting (news, human rights, etc.), monitoring or analysing.

Other definitions and clarifications on terminology are set out in Annex 1.

The standards and practices covered in the Guide are intended to apply to all open-source practitioners, including those who are not intentionally looking for or handling open-source material depicting or related to SCRSV but may nonetheless come across it. Practitioners include those paid to make online inquiries and those who choose to handle open-source information out of interest or opportunity without getting paid.

Outside of being part of a specialised SCRSV investigation team, there are numerous scenarios in which an open-source practitioner may come across evidence or other information of SCRSV even when they are not intentionally looking for it. Some examples include:

- A practitioner may discover a video containing evidence of crimes that do not qualify as SCRSV, such as the beating or killing of civilians by armed forces, only to find that the footage pans across imagery which may suggest the existence of SCRSV, such as unclothed persons being held captive.
- A practitioner looking for evidence of a militia's conscription of children may inadvertently find evidence of sexual enslavement of children when searching for online information using keywords that yield both sets of content.
- A practitioner may encounter videos or photos with one or more proxy indicators of SCRSV that merit further investigation by expert SCRSV investigators.[3] These can include the burning of buildings, the forced separation of genders, the presence of armed combatants, the conscription of children, and more.[4]
- A practitioner comes across marketplace listings (along with 'product' reviews) on social media for various services that suggest trafficking in people.[5]

Beyond addressing practitioners during the initial inquiry or discovery phase of human rights, criminal or other investigations, this Guide applies to all those who see, advise upon, collect, preserve, verify, analyse, otherwise use or share such information, including but not limited to: law enforcement officers; immigration and asylum officials; medico-legal experts; journalists; researchers; interpreters; community-based support organisations; survivor groups; and humanitarian workers who, for purposes other than immediate care and support, gather and share or publish such information.

Those who appoint personnel and manage and fund open-source inquiries should apply the principles shared in this Guide when setting standard operating procedures, developing systems, policies and protocols, and when budgeting and making resource decisions.

As with other forms of investigation, open-source research must take place in the framework of and pursuant to well-designed, pre-existing systems, policies, protocols and budgets. That minimises the risks of, for example: having to take important decisions under pressure and with no or too little time for reflection; breaking applicable laws; doing ineffective work; wasting limited resources; not having funding for important work; and harming survivors and colleagues.

The ability to implement this Guide may be affected by resource constraints, including of community-based and grassroots initiatives. Such barriers do not lower the minimum standards captured in the Murad Code, but this Guide tries to include practical solutions for low-resource contexts.

WHAT IS THIS GUIDE ABOUT?

The Guide is designed to translate applicable principles of the Murad Code to open-source investigations that include SCRSV-related issues. It will help practitioners recognise and consider critical ethical, human rights and other issues – and take thoughtful, pre-emptive preparatory actions – in order to avoid harming survivors and others and to support effective investigations.

> ***Murad Code Foreword**: Preparation is essential. We should actively avoid unplanned information-gathering and use, especially if we do not have the necessary systems, policies, procedures, risk assessments and plans in place.*

All open-source practitioners should prepare for the possibility that they may come across open-source information relating to or implying the existence of SCRSV during their online research, even when their objective does not directly or obviously implicate SCRSV. As with the Murad Code, this Guide underscores that those who gather or use digital information related to SCRSV can be both survivor-centred *and* effective. A survivor-centred approach is not only the most ethical one, but almost always the most effective one.

WHAT IS AT STAKE?

Harm may be caused to survivors not just through postings by perpetrators and others but also through the sharing, amplification or other use of such content by open-source practitioners.[6] Murad Code Principle 8.3 quoted above highlights various risks involved in the collection and use of open-source information, and the following list highlights a few examples of the harms that can be caused by the use of such information.

WHAT IS AT STAKE? NON-EXHAUSTIVE LIST OF EXAMPLES

- Someone posts photos, videos or other information which describe the people depicted as survivors of SCRSV. Even if they are SCSRV survivors, they may not be aware that the information is online and/or may not have consented to its posting or them being described as survivors or victims of SCRSV. The later amplification of that information by open-source investigators may expose the depicted people to major risks, including stigmatisation and violations of their human rights to privacy and dignity.
- A reporter finds a video on the internet which depicts the rape of a survivor and then posts stills from that video in their reporting in an effort to crowdsource identification of the perpetrator. Such crowdsourcing is a relatively common investigative practice that has been used by civil society and professional investigative agencies such as the FBI, Interpol and Europol.[7] Such crowdsourcing, if not handled carefully, may bring broader, unwanted attention to the survivor's rape, potentially magnifying their distress and violating the principle of survivor control (Murad Code Principle 2.3), or resulting in the false naming of possible perpetrators, endangering the named individuals' lives, livelihoods, families, and more.
- Practitioners share the video of a survivor's rape with members of their team who have no professional reason to view the video.[8] Such sensitive images should never be shared with anyone other than those who require professional access, out of respect for the survivor's dignity and other interests, and to protect the survivor, practitioners and others from potential psychosocial harm.
- A survivor posts material concerning the SCRSV that they experienced. Later, they come to regret that sharing (for privacy, family, security or other reasons) but are either unable to remove it or are not overly concerned about the information still being online because the content has not been viewed or spoken about by many people, including in the post-conflict community they live in, and it is buried deeply in their social media feed. But later, the content is found as part of an open-source investigation and included in a public-facing human rights report. The unwanted and unexpected increase in attention severely distresses the survivor and affects their health and security.
- An open-source investigation team comes across an online list of people named as survivors of SCRSV, which also contains email addresses and in some cases phone numbers; they suspect the document's owner did not realise that the document was publicly accessible. The investigators decide to use the roster to try to find out more information about the victims on social media. They start pulling together information about each survivor and decide to include that information in a report without the individuals' consent, violating the principle of survivor control and their right to privacy and dignity, among other harms.

Also at stake, however, is the importance of strengthening investigations, prosecutions and other forms of accountability for addressing SCRSV. For every reported instance of conflict-related sexual violence, as many as ten to twenty cases may go "undocumented and unaddressed."[9] This under-reporting is compounded by other factors that continue to hamstring work to prevent and address SCRSV, including stigma, assumptions, biases, resource constraints and deficient training. Increasing awareness of the ways in which digital open-sources can complement traditional forms of evidence or information – whether by providing critical contextual, linkage evidence or other information – can support the strengthening of efforts to prevent and address SCRSV, including through human rights reporting, legal accountability and reparations.

WARNINGS AND CAUTIONS

This Guide should be read in conjunction with the Murad Code, which is available in several languages at muradcode.com/murad-code. Many of its principles are referenced throughout this Guide but the Code has not been replicated fully here. All readers of this Guide are strongly encouraged to read the Code in full.

The Guide has also been drafted to be consistent with the *Berkeley Protocol on Digital Open-source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*[10] ("Berkeley Protocol" or "Protocol"), which establishes minimum standards for effective and ethical online investigations conducted for international criminal, humanitarian and human rights purposes. The Guide assumes that open-source practitioners and those who intend to incorporate open-source research into their investigations are familiar with the Berkeley Protocol.

Nothing in this Guide should be interpreted as modifying any substantive provision of the Murad Code or the Berkeley Protocol.

Further to the warning in the section above on "Audience and Terminology", regarding putting in place policies, protocols, systems and budgets before embarking on any investigation work, responsible investigation requires responsible preparation, to avoid reactive decisions that can harm survivors and their rights, practitioners, affiliated organisations, the investigation itself, and prospects of accountability, redress and care. Practitioners must be aware of serious issues of survivor safety, well-being and privacy, as well legal issues that may arise for survivors and/or investigators when sharing or handling sensitive material relating to sexual violence.

Nothing in this Guide should be interpreted as encouraging any form of open-source inquiry or investigation without responsible preparation, including risk assessments and mitigation measures, whether working as an individual or as part of an organisation.

Whenever practitioners encounter information that implicates or potentially implicates SCRSV, they should take the following steps:

1. Pause what they are doing.
2. Think: Should the practitioner forward, preserve or otherwise collect this information? Should they share it with appropriate authorities or stakeholders? Are they the right person to secure and hold the data? Do they know when and how they are required or recommended to collect consent from the potential victim and for what purposes? Do they know how to forensically preserve the data, if forensic collection is needed? Are they the correct person to procure or attempt to procure consent to later use the information, for example as evidence, or in a publication?
3. Secure expert guidance: Secure expert input, from other team members or externally, about the proper incorporation of survivors' rights and interests and how to effectively gather and use information if there is any doubt about the teams' necessary knowledge, demonstrated skills and attitudes, and make responsible decisions.
4. Act accordingly.

Importantly, digital open-source research does not include interviewing or interacting with survivors or their representatives, as information derived from those communications would be closed-source.

This Guide does not encourage or sanction in-person or remote engagement between open-source practitioners and survivors of SCRSV. Communication with survivors is strongly discouraged unless the practitioner has the necessary knowledge, demonstrated skills and attitude, given the risks to survivors and the reality that such communications fall outside the scope of a digital open-source investigation.

Any decision to approach SCRSV survivors must be made based on risk assessments and in full adherence to the Murad Code standards for approach and engagement.

The potential impact of contacting survivors must not be taken lightly; survivors' and others' lives may be put at risk.

Unless practitioners are trained in investigating SCRSV and otherwise have the necessary competence, practitioners should not intentionally investigate those crimes. If practitioners wish to proceed, they must ensure that they have the expertise on their team to manage and inform that process in conformance with the Murad Code, as well as other relevant standards.[11]

There are serious criminal and ethical implications of accessing sexually explicit or graphic material online, in particular content that may amount to child sexual abuse material (CSAM) or child sexual exploitation material (CSEM). Any search for SCRSV information online has the risk of producing such material, whether visual or descriptive. Careful preparation and protocols are required to mitigate such risks and take appropriate steps on discovery. Practitioners are strongly advised to read the section "Online Content Depicting Children" below.

STRUCTURE OF THE GUIDE

Given the significance and risks arising from online child sexual abuse or exploitation material, the first substantive section of the Guide addresses this issue. The rest of the Guide is organised to roughly mirror the three phases of digital open-source investigation set out in the Berkeley Protocol:

a) preparation[12]

b) investigation and verification

c) reporting, communicating and other use

Within this structure, the Guide explores the minimum standards distilled in the Murad Code (with the relevant principles from the Code reproduced verbatim), by discussing what each principle means for different phases and aspects of open-source investigations and by providing examples. When possible, the Guide provides recommendations for ways to meet the minimum standards. While this means that Murad Code principles appear out of order, it allows specific themes related to the various phases of open-source research to be grouped more helpfully.

This Guide is especially weighted towards the preparation stage, which mirrors the Murad Code's ethos that only with careful preparation can practitioners ensure that their work is safe, effective and survivor-centred.

ONLINE CONTENT DEPICTING CHILDREN

Searching online content involves the serious risk of surfacing depictions of child sexual abuse or exploitation:

1. A complex and evolving jigsaw puzzle of international, regional and national laws criminalise accessing, downloading and sharing such content. The mere accessing and viewing of such content may violate child 'pornography' laws which are in place for almost all nations. Preserving or downloading would be considered 'possession,' which is almost always illegal. There are serious prison sentences if found guilty, and potential registration as a sex offender.[13]
2. Each viewing is an additional violation of the privacy and integrity of the child who has been abused. That is so for each viewing by practitioners, their colleagues and others with whom they share that content.[14]
3. Exposure to such content can cause trauma and harm to the viewer.[15] Descriptions, online chat and texts can be just as disturbing as images. For example, the use of such materials in criminal trials may traumatise witnesses, jurors and judges, among others.[16]

Just because practitioners can find such content, it does not mean that they should use it. Just because content is online, it does not mean that viewing, using or sharing it is safe or cannot cause more harm

CRIMINALISATION PROVISIONS IN NATIONAL AND INTERNATIONAL LAW

- Depictions and nature of content: can extend beyond images or videos to live streaming or written text and can include self-generated content increasingly associated with grooming and 'sextortion', as well as 'shallow fakes' and artificial intelligence (AI)-generated 'deep fakes'.

---

*For example, the **South African Film and Productions Act 65 of 1996** (art.1 (e)): defines and criminalises "child pornography" to include "any image, however created, or any description of a person, real or simulated, who is or who is depicted, made to appear, look like, represented or described as being, under the age of 18 years -- (a) engaged in sexual conduct; (c) participating in, or assisting another person to participate in sexual conduct; or (c) showing or describing the body, or parts of the body, of such a person in a manner or in circumstances which, within context, amounts to sexual exploitation, or*

in such a manner that it is capable of being used for the purposes of sexual exploitation;...".

- Types of criminalised acts: these include "viewing" or "accessing",[17] "obtaining"[18] or "downloading",[19] "making",[20] "possessing",[21] "carrying" or "storing",[22] "distributing", "making available" or "transmitting",[23] "offering information to others where to find content" and attempted crimes.[24]

Failure to report the content to law enforcement or one of the many Child Sexual Abuse Material (CSAM)/Child Sexual Exploitation Material (CSEM) hotlines is an ethical, moral and potentially criminal failing. In many countries, there are mandatory reporting requirements on the discovery of CSAM/CSEM for service providers and others.25 Annex 2 contains a non-comprehensive list of international and regional legal instruments relating to CSAM/CSEM. It is the practitioner's obligation to know the relevant laws in the jurisdictions relevant to an investigation.

The imperative is for law enforcement to identify and safeguard the child and remove content from the internet. However, it is not for open-source practitioners to approach any child depicted online – trained law enforcement only do this after very careful risk assessments which have balanced the need for prevention of further abuse with the right to privacy and the risks of other harms which arise when victims are approached.

In many countries there are also criminal offences which relate to possession of indecent or extreme images of adults, or disclosure (including sharing or forwarding) of private sexual images without consent (also known as image-based sexual abuse),[26] as well as mandatory reporting in some countries for sexual offences or generally for serious crimes.[27]

HOW TO BE RESPONSIBLE

1. Put in place sound systems, policies, protocols and budgets before any investigation work starts.
2. Know the laws related to SCRSV and open-source research in relation to children in all relevant jurisdictions.
3. Assess and mitigate any risk. Recognise the gravity of any risks and build systems and critical partnerships to mitigate those risks including by creating external collaboration for reporting and safeguarding. Recognise that there are people who already have responsibility for some of what needs to happen next. Establish contacts with relevant law enforcement in advance, such as Interpol, and be aware of global or regional hotlines (see below).
4. Do not apply any scraping or mining techniques to data mine, dump and preserve material related to SCRSV *en masse*, as this exponentially increases the likelihood of "possessing" (and potentially sharing) CSAM or CSEM material.

A CSAM/CSEM RESPONSE AND REPORTING PROTOCOL

Practitioners (organisations and individual experts) should develop a response and reporting protocol. It should include:

- Safeguarding measures which include access to support and counselling, awareness of vicarious trauma and burnout, mechanisms for limiting exposure, and regular check-ins and debriefs with team members and/or supervisor.
- Ensuring practitioners can recognise what kind of content falls within CSAM or CSEM by providing clear advice, definitions and descriptions of examples.
- Ensuring practitioners err on the side of caution for age determination with clear advice and indicators.
- Instructing the team what to do and what not to do in the event of discovery of CSAM/CSEM. For example:

IF PRACTITIONERS COME ACROSS AN IMAGE OR OTHER DEPICTION OF CHILD ABUSE

1. **Do NOT save, screenshot, download, transfer, share or forward internally or externally, or otherwise further engage with the content.**

2. Record only 'non-content' relevant information such as the URL, date, time, size, type, duration, source, location, etc.[28]

3. Notify managers or other designated point person if working within or for an organisation.

4. **Based on prior legal, context and risk assessments, immediately contact (with the non-content information), as appropriate:**
   - Interpol
   - National law enforcement authorities in the country where practitioners accessed the content to explain what was accessed and to promote safeguarding of the child, and/or
   - A designated hotline, such as NCMEC, International Watch Foundation, etc..

5. Engage a counsellor or other appropriate person to debrief and for support.

Protocols should be expanded or replicated to cover indecent or extreme, sexually explicit images of adults, based on a review of relevant laws on cybercrime and online sexual abuse.

There is much to be learned from the safeguarding work done by online communication service providers to ensure the safety and well-being of content moderators who search for, identify, report and take down CSAM/CSEM content. Following litigation arising from harm to content moderators,[29] most companies have put in place systems of risk mitigation and support for those engaging with such content.

WHAT BEST PRACTICE CAN LOOK LIKE

The following list includes practice put in place by a well-resourced company which seeks to identify and remove CSAM/CSEM content from platforms. Open-source practitioners of other organisations can use such practice as a guide to tailor their own procedures.

1. Conduct organisational risk assessments, which include mitigatory policies, trainings, monitoring and audits to ensure compliance as set out below.
2. Mandate a 'no retention' policy for CSAM/CSEM content
   - immediately report and remove any discovered sexually explicit content rather than retaining it
   - explicitly prohibit downloading, storing, or internally sharing sensitive material unless absolutely necessary for legal accountability purposes.
3. Introduce standardised reporting and triage mechanisms
   - implement automated flagging and escalation procedures, ensuring that explicit materials are immediately reported to designated specialists rather than stored indefinitely
   - identify a reporting point (such as an independent oversight entity or a law enforcement liaison) to handle high-risk content.
4. Require mandatory training on digital ethics & legal risks: mandate digital ethics and compliance training for all personnel engaging in online investigations.
5. Ensure comprehensive psychosocial support for investigators & support staff: provide mandatory psychosocial support/referral pathways for all personnel engaged in these investigations, including:
   - access to trauma-informed mental health professionals before, during and after taskings
   - regular debriefing sessions and peer-support networks for those exposed to explicit content
   - mandatory training on recognising signs of trauma, burnout and psychological distress
   - anonymous and cost-free mental health support services for investigators, researchers, analysts and content moderators.
6. Adopt secure viewing and restricted access protocols
   - use temporary, secure viewing platforms, rather than allowing open downloads
   - use encrypted access restrictions to minimise exposure among personnel.

7. **Commit to best practices and organisational accountability:** adopt best practices in safeguarding sensitive materials and supporting staff well-being, including:
   - transparency in policies around handling explicit content
   - regular external audits to ensure compliance with ethical and legal standards
   - clear accountability measures for failing to protect staff from psychological harm.
8. **Establish a cross-sectoral collaboration model**
   - form partnerships with law enforcement, the National Center for Missing & Exploited Children (NCMEC) or similar organisations in other relevant countries, forensic analysts, survivor networks and legal experts to ensure ethical content handling.

FURTHER READING AND RESOURCES

- International Centre for Missing and Exploited Children (ICMEC), Child Sexual Abuse Material: Model Legislation and Global Review 10th Ed 2023, and database of international and national law
- ICMEC, Model Framework for Employers of Content Moderators (useful source of systems and support when staff may be exposed to traumatising material)
- INHOPE, Global CSAM Legislative Overview, 2024 (includes hotline information for each country included)
- Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (2016), "The Luxemburg Guidelines"
- WeProtect Global Alliance, Our publications - WeProtect Global Alliance

POTENTIAL CONTACTS AND PARTNERS TO RESPOND TO THIS CONTENT

- Interpol (and International Child Sexual Exploitation (ISCE) database)
- Europol, Stop Child Abuse – Trace an Object
- Law enforcement in country where material was accessed
- International Watch Foundation – 50 reporting portals around the world, IWF-ICMEC reporting portal (English) and international@iwf.org.uk if there is not one in country relevant to practitioner's work
- INHOPE global network of 55 member hotlines (INHOPE - Association of Internet Hotline Providers) and related resources
- USA: National Centre for Missing or Exploited Children (NCMEC) and the CyberTipline
- Canada: Cybertip.ca

A. FIRST PHASE: PREPARING FOR THE INVESTIGATION

The Berkeley Protocol includes three processes in the preparation phase: (a) assessing threats and risks and devising a plan for mitigating those threats and risks; (b) assessing the relevant information landscape (for example, where people are posting online, and who is posting in each location); and (c) developing an investigation plan. These processes may overlap and repeat throughout the investigation lifecycle. This preparation chapter also considers institutional and individual considerations such as the decision to do the work in the first place, and the setting-up of policies, instructions and responses if SCRSV information is discovered, and whether accessing the content is intended or unintentional. This is in line with the Murad Code approach.

1. RESPONSIBLE DECISION-MAKING

Decision-making takes place during all stages of an open-source investigation process. Such decision-making includes whether to embark upon an investigation to begin with; how to prepare for the investigation; how to scope the investigation; what systems and support are needed; and how the investigation should be conducted. As online inquiries start, decisions may be required minute-to-minute regarding what to look for next and what to do with relevant findings. The more decision-making is addressed during the planning stage of the investigation, the easier the decision-making should be throughout the investigation.

Principle 4.

Add Value or Don't Do It

4.1 *Make responsible decisions:* *We will assess the elements in this Principle to support responsible decisions about if, when and how to do this work. We recognise that our own self-assessments may benefit from consultation with others, such as community-based actors and external experts, to honestly assess whether our intended work and methods will be safe, effective and add value to survivors.*

A. Individuals vs Organisations

Unlike those who conduct their work using traditional interview techniques, open-source practitioners may work relatively independently, sometimes interfacing with a computer screen more than with other people. Regardless of whether this work is undertaken as an independent actor or as a member of an organisational team, the responsibility to make

careful, ethical decisions remains. These decisions must reflect the relevant minimum standards enumerated in this Guide.

Principle 7.

Build Systems, Competency and Support

7.1 *Institutional responsibilities and support:* *We recognise that we do not do this work alone. Most of us work in or for organisations. In organisations, we will implement this Code through leadership and commitment, policies, processes and resourcing, including in relation to consultants.*

7.2 *Work responsibly as independent actors:* *When we are working independently and cannot rely on institutional support, we will seek to ensure our work is backed by existing safe support systems and infrastructure, and individuals and partners who share our commitments under this Code.*

B. The Decision on If, When and How to Do This Work

Just because digital open-source information related to SCRSV is available does not necessarily mean practitioners should look for, collect, preserve, share, publish or otherwise use it. Practitioners should refrain from doing that when they do not have the necessary knowledge, demonstrated skills, attitudes, training, etc., to handle SCRSV-related content, or there are risks to the safety, dignity and/or other rights of SCRSV survivors that cannot be mitigated. "*First and fundamentally, with digital investigations, '[t]he fact that we are not prohibited from doing something does not mean that we should [do it].'*"[30]

Murad Code Principle 4 sets out some basic questions to aid decision-making about whether an investigation should be undertaken. For example:

Principle 4.

Add Value or Don't Do It

4.2 *What is our role and purpose?:* *We will be honest and clear about our purpose and role; the limitations and boundaries of our role; why we intend to collect information from survivors; what information we actually need from whom and in what form; how we intend to use the information and who we can share it with for that purpose.*

4.4 *Are our intended outcomes realistic?:* *We will only undertake this work where our objective can be realistically achieved in that setting with our resources, time and skills, without causing harm.*

4.5 ***Will we add value?:*** *We will reflect honestly on what added value or benefit our work or actions can bring to survivors. We will discuss these with survivors. We will only proceed if there is such an added value from our work. We recognise that some survivors are motivated by added value that our work might bring in terms of their families, communities or groups.*

4.6 ***Weigh added value against risks:*** *We will carefully weigh any potential added value against our understanding of the risks. We will design flexible methodologies which minimise risk and are fit for purpose.*

4.7 ***Challenge drivers of bad practice:*** *We will critically test any pressure or justifications of 'urgency', 'public interest', quantitative targets, 'prevention' or any other such motives to proceed where we cannot do so safely, effectively and ethically.*

Open-source practitioners should have a clear purpose articulated in an investigation plan. The plan should be explicit and detailed with regards to purpose and scope of pre-investigation, ongoing investigation, and post-investigation phases of work,[31] and reflect realistic expectations. The plan should be consistently communicated with team members, external collaborators and other stakeholders, enhancing the effectiveness of the research.

Murad Code Principle 4.6 requires that any value-add be weighed against potential risks to survivors and others. Therefore, practitioners must have realistically assessed risks and potential harms, as further discussed in the section on risk assessment below.

It can be difficult, if not impossible, to remotely ascertain the risks of digital open-source research to survivors, which is why this is ideally an assessment made in partnership with trusted local organisations, survivor groups and representatives, and/or others with specialised expertise about either the place where an event occurred or the specific violation[32] (Murad Code Principle 4.1). While practitioners can design flexible methodologies and approaches, when working remotely as in an open-source research environment, they may never know the full outcome and impact (or potential outcome or impact) of their research on survivors. Given this, practitioners must forego any action where they suspect a potential risk to survivors that cannot be assessed and mitigated. They also should be realistic about any potential added value they can contribute, or lack thereof.

In the context of digital open-source investigations, the commitment to "not ask if you do not need to" captured in Murad Code Principle 10.8 can be better understood in the open-source context as 'do not investigate, preserve and/or publish or otherwise share if you do not need to'. This foundational principle should not, however, discourage well-trained and well-prepared open-source practitioners from engaging in safe and sensitive investigations. By following the recommendations of this Guide and with proper training on gender- and trauma-informed investigations, practitioners can better understand the damaging effects of probing for explicit, sensitive or graphic details of sexual violence unnecessary for the identified scope and purpose of an investigation. When open-source practitioners do engage in investigations regarding SCRSV, this Guide can help them increase their sensitivity to the risk of harm that their work may pose to survivors, to the community, their investigation team and the public.

Principle 10.

Ensure Respectful and Safe Interactions

10.8 ***Do not ask if you do not need to:*** *We will not ask questions or probe for explicit, sensitive or graphic details of sexual violence where we do not specifically need this for our purpose. If we need this type of information, we will explain why to the survivor and will respect their decision whether to answer or not. We will also not fixate on or sensationalise such details when representing or reporting a survivor's experience.*

2. PRE-EMPTIVE PLANNING

Principle 5.

Preparation is the Foundation

5.1 ***Prepare first:*** *We will undertake thorough planning and risk assessments, and ensure that the necessary knowledge, capacity, team, policies and procedures are in place before we start gathering information, especially before any engagement with survivors. This is a critical foundation for respecting survivors' rights, and for safe, accessible, ethical and effective outcomes.*

Open-source practitioners should be especially prudent to undertake digital investigation planning, as recommended by the Berkeley Protocol, *before* they start searching for and/or gathering relevant information. This includes steps such as conducting a digital landscape analysis and various risk assessments (physical, digital and psychosocial) applied to all who may be affected by the investigation, from their investigation team to investigative partners, the general public, survivors and others in their community.

In preparation for any open-source investigation, practitioners should be aware that they may come across evidence of sexual violence even when they are not expecting it, looking for it, and it is outside the designated purpose and scope of their investigation (**Murad Code Principle 5.8**). For instance, practitioners may be investigating the burning of a village and come across a video related to that event that depicts SCRSV.[33] Accordingly, practitioners should prepare for such unexpected discovery by having a policy or instructions in place for what to do with sexual violence material should they come across it unintentionally. This may include turning that information over to a designated person on the investigation team or to an external organisation that has expertise in the appropriate handling of such information and/or flagging the content as sensitive and limiting access. As noted in the preceding section, in some cases, such as those of child abuse, investigators may be legally obligated to report open-source information to law enforcement. This situation should be considered in the planning phase of all investigations.

3. BUDGET, POLICIES, PROTOCOLS AND SYSTEMS

As highlighted earlier, putting in place and adhering to the right policies, protocols and systems and having an appropriate budget are pre-requisites for doing survivor-centred and effective investigation work. Two examples of required systems, policies, protocols and resource-allocation follows.

The Berkeley Protocol requires that every practitioner and investigations team consider undertaking a data protection assessment and establishing a data and information sharing protocol that specifies the level of sensitivity of the digital data that will or may be collected.[34] This should also include safeguarding instructions for handling potential illegal content (e.g. child sexual abuse material or terrorism-related material).

All practitioners and their teams should also be aware of the security limitations of the digital tools they use. For example, previous investigators have sometimes placed sensitive data in cloud-based platforms (like Google or Dropbox) without realising that their folders, spreadsheets or other documents detailing sensitive data are publicly accessible. All practitioners should ensure that access to the digital data they have collected is restricted to the appropriate person(s). The process of decision-making around access and sharing should be explicitly documented. In order to ensure the privacy of survivors as outlined in Murad Code Principle 9.4, open-source practitioners should limit access and exposure to digital SCRSV materials both inside and outside their teams to those who must have access.

A. Psychosocial Wellbeing of Open-Source Practitioners

Principle 7.

Build Systems, Competency and Support

7.10 *Manage risks of vicarious trauma: We will ensure measures are in place to minimise the harmful effects of the work on ourselves, our team and others impacted. We will ensure basic training on signs and symptoms of trauma, vicarious trauma, compassion fatigue and burnout, and ensure institutional and team support protocols and safe working methods. We will include measures to manage these risks when people are working outside a team or office environment, including working remotely.*

Given the sensitive and potentially graphic nature of the content with which they may come in contact, practitioners and all those implicated in or by the research may be at especially heightened risk of vicarious and secondary trauma, re-traumatisation and other types of psychosocial harm.

Practitioners should ensure that measures are in place to minimise the harmful effects of their research on themselves, their team, survivors and others who may be impacted, as per Murad Code Principle 7.10 and the Berkeley Protocol.[35] Practitioners who work as part of an organisation should also incorporate regular training on the known risks of digital

investigation methods and known mitigation strategies, and should incorporate these strategies and insights in relevant policies and protocols.[36]

EXAMPLES OF PRACTICAL STEPS TO MINIMISE HARM TO PRACTITIONERS[37]

- Reducing exposure, such as ensuring short shifts or task times with exposure to graphic or traumatic material.

- Flagging graphic content so that project partners can determine whether, when and how they want to review that information.

- Electronically blurring or blocking graphic content when not needed for analytical purposes.

- Turning the sound down or off during content review.

- De-briefing with colleagues and/or other appropriate persons, such as counsellors.

- Raising awareness of the signs and symptoms of vicarious trauma and burnout.

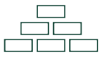
- Providing training on effective secondary trauma avoidance strategies and grounding and well-being exercises.

B. Language and Translation Functions

Practitioners should ensure that, either through human or – at a minimum – machine translation, they have the necessary expertise to conduct research in online spaces in relevant languages, including in survivors' languages. There are many strategies that exist for machine-based translation. Practitioners should be aware of these methods and, importantly, their limitations. Steps should be taken to, for example, minimise language bias and the incorrect identification or categorisation of relevant information. For example, machine learning-based tools are trained almost exclusively on an English language dataset; consequently, machine-based translation may not correctly translate

colloquial dialects or explain slang terms related to sexual activities used in local contexts. See also "Team Selection, Competencies and Briefings" section below.

4. RISK ASSESSMENT AND MITIGATION



Principle 5.

Preparation is the Foundation

5.3 *Assess and mitigate risks: Based on knowledge and understanding of the context, we will identify and assess any potential risks for all those involved, such as individual survivors, their family and communities, ourselves, and others involved in the process. We will assess general and specific risks for individuals and situations, such as confidentiality, safety, well-being, social repercussions and stigma, and legal rights. We recognise that this process should be informed by those competent in aspects such as gender, children and communications, and data, physical and other security. If we proceed to work with individual survivors, we will also seek a survivor's input on their risks. We will not proceed if the risks cannot be appropriately mitigated. This assessment and its mitigation measures will guide every aspect of our work. We will review the assessment as often as necessary.*

Before practitioners begin their research, they should evaluate how their actions in digital spaces may potentially impact people in other spaces (both online and offline) and take steps to minimise any potential harm. For example, this might include mapping who else is conducting a related investigation (so as not to unnecessarily interfere with or duplicate their work), ensuring the use of digital security best practices to minimise the risk of inadvertently signalling that an investigation is underway through their online activities, or avoiding communicating with survivors or others related to the investigation in public spaces online. Practitioners should also be sensitive to the risk of online surveillance of their team's and partners' activities.[38]

Survivor safety, well-being and dignity must always be prioritised over the practitioner's research, investigation and publication objectives. In the context of open-source research, risks to a survivor's safety and well-being include those physical, digital and psychosocial risks that can arise from conducting any online research into the survivors' identity, given the relative insecurity of any digital communication from storing, sharing or using such materials or, when this happens, from reaching out to survivors and/or their communities over digital means of communication (for example, due to surveillance, interception or hacking).

Principle 7.

Build Systems, Competency and Support

7.8 *Build confidentiality protections: We will put in place confidentiality protocols and measures to protect the survivor's information, privacy and safety, including taking special care to ensure the security of any digital communications, data management and storage.*

To identify and avoid such risks, open-source practitioners should include specific digital security concerns in their pre-investigation plans along with strategies for mitigation, as outlined in the Berkeley Protocol.[39] Risks to survivors also extend to their families and communities. In addition, practitioners should exercise due diligence in analysing all digital tools and devices that they may use during the course of an investigation so that they understand what security and other risks their use might entail.[40] Practical guidance on how to conduct risk assessments, both digital space risks and SCRSV risks, can be found in Annex II and Chapter V of the Berkeley Protocol, and Chapters 7 and 8 of the International Protocol on the Documentation and Investigation of Sexual Violence in Conflict (2nd ed.).

Principle 1.

Understand Survivors as Individuals

1.4 *Prioritise survivor safety: We will continuously prioritise a survivor's safety, well-being and dignity ahead of our objectives. We will work to understand the risks and repercussions to survivors and those around them which could arise from any contact with us. Such risks can include revictimisation, reprisals, stigmatisation, physical, online, information and communications safety risks, and legal risks.*

1.5 *Identify heightened risks: We will take additional, specific precautions when there are heightened risks of further harm. We recognise that any individual may face heightened risks which may change over time and context. Heightened risks may arise for child survivors including children born of war and unaccompanied children, persons from LGBTQI+ communities, persons with disabilities or with limited literacy, persons from indigenous or marginalised groups, and others.*

Murad Code Principle 1.5 requires the identification of heightened risks triggered by working with SCRSV-related information in an online environment. In the SCRSV context, showing survivors' faces (or other identifying features or locations) might have heightened ramifications, such as stigma, so-called 'honour killings', disownment by families/communities, loss of employment or property, etc. While digital open-source investigations include many of the risks present in physical world investigations, digital security and psychosocial security risks may be especially acute in the online context.

As outlined in Section IV of the Berkeley Protocol, practitioners should have training and/or other knowledge of those heightened digital and psychosocial risks and how to mitigate them, and put in place policies and/or practices to safeguard themselves, their teams, survivors and others.[41] For example, practitioners can take precautions to mask the identification of their computer when searching online, so as to protect their identities and

information about their investigation such as by using a virtual private network (VPN).[42] This can help obscure the investigator's location (for example, if they are working from The Hague), which may suggest their identity or otherwise compromise their anonymity or security.[43]

Whilst some deploy a sock puppet (a fake online identity), this should be used with extreme caution as it may imply deceptive or otherwise unethical practices. Depending on the role of the investigator and the context, using a fake identity may violate their professional code of ethics, violate a platform's terms of service or be illegal.[44] Every practitioner should have a policy for when and to what extent they will mask their identity online.

In addition, the internet is known for a prevalence of mis/disinformation; synthetic audio, video and other imagery; and other misleading or inaccurate data.

Whilst the creation and circulation of deep fakes can amount to systematic sexual violence in themselves, deep fakes also present a cautionary tale to practitioners to verify whether an image, video or other content truly depicts something that happened. Practitioners should be aware of these risks and deploy known verification strategies, including conducting technical, content and source analysis, as provided for in the Berkeley Protocol, in order to assess open-source information's authenticity and reliability.[45] For further discussion, see the "Verification and Investigative Analysis" section below.

***Case Study – Deep Fakes**: In South Korea, deep fakes have become a form of systematic sexual violence in their own right after teenage boys manipulated images and videos using AI depicting female relatives and classmates nude or engaging in acts of a sexual nature. The publication of these deepfakes through Telegram networks and other apps resulted in further sexual harassment and abuse directed towards the women and girls depicted.*[46]

5. BIAS AND NON-DISCRIMINATION

As outlined in the Berkeley Protocol, practitioners should do their best to conduct holistic open-source research that accounts for and actively works to reduce bias. This includes understanding and accounting for the risks of human, technical and access biases.[47]

Principle 8.

Gather Information From Other Sources

8.2 *Source representative information: We recognise that who we are, what we search for, and how and where we search can introduce harmful biases and blind spots in the information we find. We also recognise similar biases are introduced by limitations on the availability of information, such as through censorship, inequalities, social marginalisation, insecurity and technical factors. We will seek to minimise these risks.*

Open-source research can be negatively affected by blind spots and discrepancies in the kind of information that is available online due to access, technical and human biases that affect whose information is discoverable, the purposeful obfuscation of the underlying crimes by perpetrators who post the open-source content for other purposes (e.g., clandestine trafficking advertisement), or the surveillance of survivors' communities by perpetrators.[48] Consequently, the experiences and perspectives of marginalised groups, as well as the commission of stigmatised violence (e.g., same-sex sexual violence or violence against LGBTQI+ communities) might be missing from online spaces.

Case Study – Seeing Past the Label of Torture against Male Detainees and PoWs: *A common blind spot in SCRSV investigations has been the non-recognition of sexualised violence against men and boys. For example, sexual violence perpetrated against men in captivity is often described as torture instead of as sexual violence. This bias towards exclusively describing men's experiences as torture is fed by common misassumptions and stereotypes that only women are targets of sexual violence and that all forms of sexual violence are driven by lust rather than dominance. For example, in her review of the Peruvian Truth and Reconciliation Commission's final report and other materials, Michele Leiby found that the report indicated only 2% of reported SCRSV survivors were men, whereas her review of primary materials indicated 22% of reported SCRSV survivors were men. She identified several cases of sexual violence against men which had been only categorised as torture.*[49]

Because open-source investigations occur online, the recognition of a survivor's individuality begins with a consideration of whether, when and how relevant survivors communicate in online spaces so that practitioners do not inadvertently miss or ignore what individuals may be attempting to communicate. The answers to this inquiry can vary dramatically based on, for example, geography (including whether the survivors are in urban, rural or other environments), gender and age. For example, survivors in Myanmar might post information to Facebook, versus WeChat in China, or VKontakte in Russia. Youth in the United States might communicate over Snapchat or Instagram, whereas their parents might connect over Facebook, iMessage, BlueSky, Twitter (now X), LinkedIn or WhatsApp. Both may communicate over Venmo or another payment app. Moreover, it is important to recognise that what is communicated online does not represent the entirety of a survivor's experience.

Principle 1.

Understand Survivors as Individuals

1.2 ***Counter assumptions:*** *We will not make assumptions or generalisations about survivors or their experiences, such as how they 'should' behave or react, their vulnerability, trauma, resilience, gender, disabilities, capacity, maturity, reliability, needs or concerns.*

1.8 ***Be inclusive and do not discriminate:*** *We will not engage in or tolerate any form of discrimination including by those who support our work. We will seek to include and make reasonable accommodation for those who are often excluded or silenced due to persecution, marginalisation, presumed lack of agency or capacity, or being overlooked as victims.*

In recognition of the heightened risks outlined in **Murad Code Principle 1.5** and the principle on non-discrimination in **Murad Code Principle 1.8,** accounting for biases requires exercising due diligence to understand how distinct people and groups communicate issues of SCRSV online in the relevant communities, including any use of coded language, slang terms, visual cues or proxy indicators of SCRSV.[50] These discrepancies can be mitigated by establishing diverse teams of practitioners with cultural knowledge and who represent diverse perspectives to help identify and address collective blind spots. Other practices for offsetting biases include engaging in peer review, having multiple working hypotheses or theories of a case and including local knowledge and specialised knowledge of SCRSV in the affected community on the investigations team.

Murad Code Principles 10.2 and **10.7** also provide ways in which bias and prejudice about SCRSV can be reduced by making multiple searches, searching across a variety of social media sites (and other online spaces), using a variety of search terms in various languages, and recognising SCRSV as part of a pattern of violence in a conflict or other context.

Principle 10.

Ensure Respectful and Safe Interactions

10.7 ***Contextualise SCRSV:*** *We recognise that SCRSV does not happen in isolation from other violations and harms. We will also be attentive and respectful if a survivor chooses to communicate about other violations or harms that they may have experienced or witnessed.*

Recognising and proactively countering assumptions are critical to mitigating biases and prejudices. For example, practitioners should consider that online information, including that which reflects interviews with survivors, may not comprehensively reflect those survivors' experiences or details about a particular incident. It is critical, therefore, to understand that online information may be incomplete and/or misleading.

Practitioners should not assume that particular populations are or are not affected by sexual violence, including on the basis of gender, age, class, ethnicity or ability. Practitioners should adopt a gender-sensitive, age-sensitive and intersectional analysis as part of their digital investigation planning, considering how peoples' experiences and whether they report those experiences online may differ based on gender, age and other factors.[51] An intersectional analysis requires practitioners to recognise that distinct forms of harm, abuse, discrimination and other violence occur when multiple categories of social identity interact.[52] For example, a group of women may be the target of violence by combatant forces because of a combination of gender, age, class, religion and/or ethnicity.

Practitioners should always be open to the possibility that relevant information exists online, and as a result, make sure to integrate digital open-source fact-finding into any investigation into SCRSV. For example, some investigation teams have assumed that digital open-source information about a particular crime does not exist, like when the crime is known to have taken place inside highly secure facilities; this has frequently proven to be false. Individuals may smuggle footage out of those facilities and post that footage to the internet. Alternately, survivors and others may communicate about their experiences online once released.

The line between survivor and perpetrator is not always clear. For example, a perpetrator of SCRSV may also be a survivor, or may commit a rape under threat of their own death or torture or that of a loved one, such that they are not exercising independent will to proceed. While this information may be quickly discovered through traditional, on the ground investigation methods – such as testimonial evidence – that context may be missing in online videos or photographs. It is important that practitioners keep such possibilities in mind to question their own assumptions and to avoid labelling individuals who are implicated or depicted without additional information.

Principle 3.

Be Responsible and Have Integrity

3.3 ***Do not stigmatise:*** *We will examine and confront our own limitations in understanding perspectives and experiences beyond our own; our own biases, fears, trauma and triggers; and our own attitudes, prejudices and assumptions in relation to sexual violence and survivors. We will not convey any message to survivors (through our tone, words, body language or other actions) which blames, shames, further harms, judges, belittles, patronises, ridicules or disrespects them. We also will not present or publish any information about them which could do this.*

3.4 ***Ensure accuracy:*** *We will check that our understanding and representation of the information gathered are correct and free from misrepresentations or assumptions. Whenever possible, we will check the accuracy with the survivor and make any necessary corrections.*

Practitioners should take the time to understand their own potential biases, misconceptions or stereotypes about SCRSV, as well as their own relationship to the communities and crimes they are investigating, which may affect their perceptions in both helpful and unhelpful ways. Practitioners must seek to identify and minimise or eradicate any stigma or prejudice in how and what they communicate, how it influences and manifests in their inquiries – such as what they search for, where they search and how – as well as in their assessments and end use of material found. One practical example which can help is to work with community-based experts and interpreters to prepare and review over time a glossary of culturally acceptable, non-stigmatising terminology, as well as red flags for offensive or derogatory words or gestures in the relevant languages and culture.

Diversity within investigatory teams brings different perspectives on if, how and where to research open-source information; minimise technical or cognitive bias in investigations,[53] such as biases that reflect stigmas against SCRSV survivors or that distort the interpretation and analysis of digital data, and increase the efficacy of investigations. For example, as noted above, investigators have reported patterns of violence being interpreted as sexual and gender-based violence when perpetrated against women or girls, but interpreted as torture when perpetrated against men.[54] As a result, it is critical that digital investigation teams have training in the various types of SCRSV that may be present, and how SCRSV manifests similarly and/or differently across various demographic groups, including on the basis of age, gender, LGBTQI+ or intersectional status.

When conducting open-source research, practitioners should be guided by a series of research questions that help define the scope of their research. Practitioners should recognise the dangers and ease of 'cherry-picking' (selecting only the best or easiest to access information) online which feeds confirmation bias or a particular theory of a case. Practitioners should ensure that their digital search and verification processes are as unbiased as possible in order to increase the odds of accuracy, for example by using multiple working hypotheses as to what happened and who is responsible. When using digital information to conduct research, practitioners should track who, what, when, where and how something happened, and *how they know* the answer to each of these questions.

In tandem with their commitment to let open and unbiased questions guide their research, practitioners should also recognise that SCRSV does not happen in isolation from other violations and harms and should be attentive to signs of intersecting violence communicated online, as per Murad Code Principle 10.7 – for example, people who have been killed may also have been raped. Practitioners should also be attentive to and note harms conducted in or through digital spaces,[55] such as the magnification of harm and stigma through the online posting of sexually graphic imagery that may have the effect of humiliating or degrading the survivor or others, or the amplification of hate speech on social media.

***Case Study – Sextortion and other Online Harms**. One example is the phenomenon known as 'sextortion.' In Sri Lanka, perpetrators created a series of recordings depicting their rape of a number of people. The perpetrators then used the videos to blackmail the victims into submitting to further sexual acts on the threat that the videos would be released if they did not. In another situation in*

Yemen, legal investigators lost the ability to work with a survivor-witness because information about the survivor's rape was posted on social media. The witness had to then recant her story for her own safety.

Investigators should take special precautions to protect information about SCRSV to help prevent its communication across online spaces and ensure that their reference to such material in public communications, meetings, courts or other fora is designed to provide minimal risk of bringing additional unwanted attention to the experiences of specific survivors.

6. TEAM SELECTION, COMPETENCIES AND BRIEFING

Principle 7.

Build Systems, Competency and Support

7.3 ***Select the right team and partners:*** *We will build a team (including interpreters, intermediaries, guides, fixers) and select partners and others acting on our behalf who share our commitment to this Code. We will also consider the diversity, representation, confidentiality, safety and flexibility implications of these selections.*

7.4 ***Build the right competencies:*** *We will do this work only where we have the necessary knowledge, demonstrated skills and attitudes across our team. Those competencies include sexual violence and stigma sensitisation; understanding gender, diversity and context; working with people of different genders, disabilities and ages; informed consent and basic referral skills; risk recognition; safe communication and interviewing skills, including with children and in relation to remote interviews; trauma awareness and understanding; and information protection and preservation. We will keep the skills and knowledge which make this work safe and effective for our intended purpose up to date.*

7.5 ***Recognise our limitations:*** *We acknowledge that everyone has limits to their experience, expertise and perspective, as well as to their role or mandate. We will reflect honestly about, and will stay within, the boundaries of our knowledge, skills and understanding. Beyond our limitations, we will consult and work with others, such as trauma, security and child experts.*

Open-source investigations are often collaborative, engaging multiple individuals, organisations and disciplines. All collaborators should be aware of and commit to upholding the principles in the Code, the Berkeley Protocol and this Guide. Practitioners should also ensure they have the appropriate digital capabilities on their team or through their collaborations, both for conducting open-source research and for doing so with a sensitivity to gender, SCRSV, security, stigma, other ethical considerations, etc.[56] All practitioners should have regular training in holistic security, including best practices for

digital security and strategies for minimising the risk of secondary and vicarious trauma, which may be an especially acute risk in the open-source investigations context.

While practitioners who have little or no training working directly with SCRSV might opt to flag SCRSV material to specialists or to lawyers who can determine the material's potential investigatory or evidentiary value before moving on to other steps, including preserving the content (Murad Code Principle 7.5), doing so may not always be possible or practicable. For example, if the content in question is at imminent, short or medium-term risk of being removed from an online platform, it may need to be immediately preserved (the exception being content that is illegal to possess, such as information related to child sexual exploitation).[57] Therefore, even practitioners who do not commonly investigate SCRSV or consult experts should familiarise themselves with this Guide so that they can make responsible and informed decisions about how to handle such content.

In addition, the decision to flag the content to a specialist does not relieve the practitioner of the responsibility to ensure any handling of the sensitive content is done with the heightened level of care set forth by the Murad Code and this Guide. That care must be provided before, during and after deferring to specialists. The imperative should be to do no harm to the survivor, their community and others who are or may be impacted through the investigation or research process, and to protect their human rights, for example, by respecting their rights to privacy, dignity, life, health and justice.

Diversity for the purpose of team composition includes but is not limited to gender identity, language, nationality, country of origin, sexual orientation, religion and age. Country or cultural experts are especially valuable members of a team who can help put SCRSV into the context of the country or region affected. Having a team member as a reference who can decode cultural context and terminology is especially helpful when handling SCRSV considering culture-specific ways of referring to SCRSV, including for identifying and analysing relevant materials found online. As explained to researchers by one investigator, when someone from outside a culture learns a language, even if they become fluent, they are rarely taught technical terms related to sexual behaviour, let alone informal or slang terms.[58]

Specific to children, practitioners should consider Murad Code Principle 7.6 as permitting the use of digital open-source information depicting or otherwise indicating sexual violence against children *if and only if* practitioners are legally permitted to do so and have the necessary training and other competencies for appropriately handling data related to SCRSV and children (which is a very narrow subset of practitioners). Importantly, whatever the purpose or intention of handling SCRSV material depicting children, any accessing, possession or handling of such material can be a criminal offence, as explained above.

Practitioners should also be aware of and sensitive to the fact that although children are defined in international law as anyone under age 18, different communities have different ages of maturity and use different terms for children, which can confuse an age determination or assessment for persons under 18, and that there may be other indicators of juvenile status (visual, auditory, text-based or other) of which practitioners should be aware. For example, early or child marriage, child labour, or recruitment of child soldiers may all present children under 18 years old in adult roles, which may lead a team member not to recognise their status and rights as a child. Whenever possible, practitioners should consult with child rights experts who have deep knowledge of the laws and norms affecting children in the relevant community. When needed, practitioners should also consult with experts who know how and where information about children from that

community is communicated online, as well as how and where children from that community communicate online, before beginning their research.

Principle 5.

Preparation is the Foundation

5.10 *Brief your team and partners: We will brief and monitor our team and those acting on our behalf (including any partners) on our preparations and on safe, ethical and effective processes to adhere to this Code.*

In keeping with Murad Code Principle 5.10, practitioners should brief and monitor their team and those acting on their behalf (including any partners) on all of the aforementioned investigatory preparations and on safe, ethical and effective processes to adhere to the Murad Code, this Guide and relevant provisions of the Berkeley Protocol.

7. DIGITAL LANDSCAPE ASSESSMENT AND CONTEXTUAL KNOWLEDGE

Principle 6.

Know and Understand the Contexts

6.1 *Know the context: We will ensure that our team and those acting on our behalf base their work on a good understanding of the context in which the SCRSV took place and of the immediate environment around the survivor. We will identify positive and negative, direct and indirect impacts of the elements in this Principle on survivors, their families and communities, and our work, and will ensure this understanding informs our preparation and work.*

6.2 *Understand culture: We will identify relevant cultural and social norms, attitudes, traditions, rites and customs, as well attitudes about children, their decision-making and the age of adulthood.*

6.3 *Understand gender: We will assess gender dynamics, norms, violence and inequalities, and understand how they create risks of revictimisation and barriers to survivor support and other rights.*

6.4 *Understand stigma towards SCRSV and survivors: We will identify, risk assess and mitigate harmful misunderstandings, assumptions, attitudes and behaviour (known as 'stigma') within communities in relation to sexual violence and survivors.*

6.5 *Identify community dynamics: We will analyse group dynamics around survivors, such as power structures, competition for resources, politicisation of justice, intermediary motivations, gatekeepers (those who can control or influence access to survivors), empowering influences, and drivers which silence, pressurise or harm survivors and their families.*

6.6 *Recognise individual, compounded and collective harms: We will analyse different connected harms caused by SCRSV to individuals and collectively to groups such as families and communities, and how harms are compounded by multiple forms of discrimination.*

6.7 *Be familiar with laws and practices: We will familiarise ourselves with relevant formal and informal laws and practices (including ancestral systems). Such laws and practices may, for example, provide avenues to legal recourse for survivors, discriminate or perpetuate discrimination, criminalise a survivor for what has happened, fail to recognise a survivor as a victim of a crime, or legally require that we report information about crimes to authorities. We will discuss these with a survivor before they share their experience, so they can consider whether or not, and how, to proceed.*

6.8 *Understand appropriate communications and interactions: We will work to understand the significance and impact of all forms of our communication and interactions in the context, ensuring gender, age, disability, social, cultural and context sensitivity and respect. We will identify and use inclusive and non-harmful forms of communication which reflect survivors' identities, and respect non-harmful social norms and practices. We will also seek to understand cultural and other aspects of communication, including mannerisms, derogatory terms, common expressions and euphemisms, and gaps in language relating to SCRSV or the survivor.*

6.9 *Minimising negative repercussions: We will identify the risks of and minimise any negative repercussions from our work within a community.*

6.10 *Community-based sustained support: We recognise the important role of trusted community-based groups and support systems for the continuity of support for survivors, building trusted relationships, empowering survivors and for tackling negative attitudes in the community towards survivors. Such groups can include survivor networks, women's organisations, LGBTQI+ organisations, organisations for children, and organisations for persons with disabilities. Whenever appropriate, we will seek to work with such groups.*

Because open-source investigations may be conducted by practitioners working remotely with limited contextual understanding of the conflict location, any investigation planning, including risk assessment and management, must include sufficient research into the context of a region, culture and community before beginning the investigation, consistent with Murad Code Principle 6. This includes conducting a digital landscape assessment that details the extent of use of digital technologies in a region, how that use varies based on demographics, relevant platforms and websites, etc.[59]

When possible, practitioners should work with on-the-ground partners with lived experience in the region, ideally locals, to build a comprehensive perspective of sexual violence in that region, as well as to build any relevant contextual understandings. For

example, degrees of nudity and its social or legal impact can vary by culture; forced removal of a headscarf from a woman in Syria could be seen, felt and/or treated as forced nudity. In addition, women who do not wear a hijab where legally or socially required may become the targets of gender persecution and/or sexual violence, as can be seen in Iran and Afghanistan.[60]

> ***Case Study – Symbols and Signals***. *A non-Burmese digital open-source investigator discovered online images from Burma/Myanmar of sarongs tied together creating what looked like washing lines between buildings. While this phenomenon was identified as noteworthy, its significance and its connection to SGBV was lost on the investigator. However, to Burmese colleagues, it was immediately clear that this 'washing line' was meant to create a barrier discouraging security services from passing through. In traditional Burmese culture, men and women's laundry cannot be washed together, and touching or taking down women's clothes would be taboo and humiliating. The presence of these 'fences' composed of women's laundry became a symbol of sexual violence perpetrated by security forces against these women in those communities.*

In keeping with Murad Code Principle 6.2, practitioners seeking to identify cultural norms should recognise that such norms can differ based on whether communication happens online or offline and can even differ across internet sites (for example, the kind of information that is communicated on dating sites versus professional networking sites). Practitioners should therefore be sure to identify any investigation relevant cultural and social norms, attitudes, traditions, rites and customs that exist online. Assumptions about cultural rites and traditions can be complicated and often contradictory in online spaces, where historically marginalised people may have higher levels of agency than in offline spaces. Importantly, online narratives about some groups can themselves constitute a form of violence or incitement to violence, for example, where online platforms are used to dehumanise or spread stigmatising information about a particular population.

While important to know for online inquiries, practitioners also should be careful not to inadvertently adopt dehumanising or stigmatising terminology when communicating about such information. As noted above, open-source practitioners should pay particular attention to the ways in which sexual violence is talked about and/or depicted in the relevant community or communities (by survivors, perpetrators and others) in both online and offline contexts. This includes linguistic and/or non-verbal or visual information[61] exchanged and shared in a variety of social settings and communities. For example, slang terms for body parts or sexual behaviour, relevant memes or hashtags, emojis that may indicate sexual acts, and abbreviations and codes (such as "53X" for 'sex') that are used in digital communications. Careful attention should also be paid to whether such terminology is derogatory, insensitive or stigmatising so as not to perpetuate harms if they share or otherwise use those terms (for example, in a report or publication or in a courtroom).

Practitioners should especially note *where* people in the relevant community or communities are communicating and whether there are online fora where SCRSV-affected people may be particularly likely to share information, such as public chat groups (for example, on platforms like WhatsApp, Discord or Telegram). In addition, there may be fora where perpetrators are posting information or depictions of violence. Information shared online about offline locations where people may be communicating could also be important to note for any partners who are conducting research in situ.

Once fora are identified, practitioners should assess the appropriateness of collecting information from that space, including any privacy considerations. For example, it may be inappropriate to collect information from an online support group for SCRSV survivors, even if it is a public group with no restrictions on access, because there is a clear expectation of privacy and intent in terms of how information is shared or used, which does not include research, advocacy or legal accountability.

Practitioners should also assess whether survivors are in areas where they cannot share digital information easily, such as newly-formed refugee camps or areas that are geographically remote, as well as whether issues of access and literacy may impede digital reporting. Some women, nonbinary individuals, children, the elderly, LGBTQI+ populations, people from lower economic classes, those in rural areas and others might have lesser access to online spaces and lesser ability to communicate openly due to social or cultural contexts and the combination of identities they may hold.

There may also be issues as to *when* information was or was not shared online. For example, practitioners should pay attention to and document any internet blackouts in the relevant region during the time-period under consideration, understanding the impact that may have on what and when information is posted. Information about sexual violence may emerge later as survivors begin to feel safe enough to disclose (Murad Code Principle 9.7) or as occupied territory is liberated. This is important because it can skew when information potentially appears online; for example, once an internet blackout is lifted, or once people feel that there is sufficient community or international support, survivors or others may suddenly post about an event that took place weeks before. Such possible delays should feed into investigation planning, including the digital landscape analysis conducted at the onset of an investigation.

Open-source investigations often implicate legal and regulatory provisions that vary considerably between national, regional and international jurisdictions. Therefore, practitioners should consider working with partners and collaborators to assess the legality of conducting open-source research in that jurisdiction, consistent with Murad Code Principle 6.7 ("be familiar with laws and practices").[62] This includes, for example, noting where survivors may be criminalised in national laws, to avoid inadvertently creating legal risks for the survivor, for example where sexual acts outside marriage or sexual acts between members of the same sex are criminalised. Laws may also impact how online investigations are conducted, including when digital open-source investigation methods may cross over into illegal surveillance that requires a warrant or other legal process. Practitioners must also be aware of relevant local, national, regional and international laws that criminalise the possession and sharing of digital content (for example, privacy laws may restrict the downloading and/or transmission of certain kinds of data, such as nudity or sexual acts involving children).[63]

Another consideration is the impacts on survivors who are men and boys within the cultural and legal context of the event/nation/region. This includes accusations of a change

in sexual orientation due to the violence perpetrated against them, which may especially inhibit reporting, particularly in jurisdictions where homosexual behaviours are criminalised or can put survivors at acute physical risk. This type of assessment requires collaboration between team members with different types of expertise, such as contextual or cultural knowledge, as well as gender and linguistic expertise (often in several potentially relevant languages). Any assessment should include how sexual violence, sexual orientation, sexual identity and sexual relations are discussed and not discussed, in online and other social contexts by members of the relevant national, ethnic, religious, or other relevant groups.

Any applicable mandatory reporting laws must be carefully pre-assessed. Sharing information about SCRSV without a survivor's consent could breach their right to autonomy (control over their personal history, identity and image) and privacy (Murad Code Principle 2.3) as well as potentially creating grave security and other risks for survivors, practitioners and others. Such risks may be amplified where it is the military, police or other state authorities who are or appear to be the perpetrators of sexual violence depicted online, or where the necessary confidentiality of reporting channels and the proper management of that information by state authorities are lacking. Practitioners' policies and protocols should provide the framework for analysing the potential impact of any such laws on the investigation, the investigation team or organisation, survivors and others; identifying with whom the mandatory reporting obligations lie; decisions on whether or not and how to proceed with open-source research where such laws exist; and assessing all related risks and potential mitigation measures.

Practitioners should also be aware of and consider non-corroboration rules on sexual and gender-based violence in the relevant legal context(s),[64] as well as which jurisdictions still require corroborating evidence. Non-corroboration rules establish that a survivor's testimony need not be corroborated with other forms of information. However, even where corroboration is unnecessary, taking the time to consider alternative and additional sources of evidence from online open sources can help strengthen a case, show impacts and patterns of violence, and contextualise sexual violence.

As part of their understanding of cultural and community-based norms, gendered dynamics and stigmas surrounding SCRSV, and laws and practices, practitioners should also, to the best of their ability, identify the risks of and minimise any negative repercussions from their work online, including risks to both online and offline communities, as required by Murad Code Principle 6.9. As articulated in Murad Code Principles 5.5, 5.6 and 5.7, identifying who else is gathering information and is working on similar issues on the ground can help practitioners build necessary collaborations to understand and minimise the risks associated with remote information-gathering.

Practitioners should take the time to understand who is trusted in a community by survivors and do at least basic due diligence on partners and community-based actors they plan to engage with ('partner mapping'). Much can be learned from engaging trusted community-based groups and support systems: ensuring the continuity of support for survivors; assisting practitioners in understanding the relevant digital and non-digital landscape, terminology and practices; empowering survivors; and tackling negative attitudes towards survivors. In addition to the groups mentioned in Murad Code Principle 6.10, this recognition may include non-governmental, governmental or intergovernmental

organisations that specialise in issues related to internet and communication technologies, issues of technology and human rights, sexuality and/or the use of digital technologies with regards to SCRSV.[65]

8. INVESTIGATION PLANNING

The Berkeley Protocol provides useful information on investigation planning in Chapter V and a template for a plan at Annex I. Investigation plans are not fixed in stone and should be updated during an investigation.

The very important topic of communicating with and securing the consent of survivors and others has important investigation planning components. See the next section "Preparing for Potential Communication with Survivors and Others for Consent" for the planning and other elements of the topic.

This section highlights the importance of several ingredients of investigation planning of particular importance to SCRSV including recognition of 'proxy indicators' (described below), having a response plan for sensitive data, identifying how and where to find alternative sources to posted information), and the importance of framing open research and investigative questions to counter bias and assumptions about SCRSV.

Practitioners should be aware that there are a number of proxy indicators of sexual violence in conflict,[66] including phenomena like the burning of villages; the separation of men and boys from women and girls; the transfer of gendered populations; youth forced to fight each other; recruitment of girls by armed groups and forces; the inspection of young women, girls and boys by armed forces or police; the sudden absence of a particular gendered group from public life; signs of aggressive 'morality policing'; the presence of new, conflict-related markets; checkpoints; the increased use of gendered hate speech by forces on patrol, etc.[67] Practitioners should be sensitive to those indicators so that they do not inadvertently overlook possibly-relevant SCRSV evidence and should identify the proxy indicators they are going to look for when planning their investigation.[68]

Open-source information may also provide important insight about the intent of individual SCRSV perpetrators, even if the acts of sexual violence are not available on social media. For example, a particular militia may use social media to spread propaganda about how they treat members of the LGBTQI+ community or their policies for dealing with women and children they consider 'spoils of war.' Advertisements posted to social media, or content posted to dating sites, may suggest trafficking in persons.[69] For example, ISIS published prices for 'slave' markets online as they traded girls that they had abducted from Yazidi communities.

Case Study – Digital Images Serve as Evidence of Base Crimes[70]*. In Sri Lanka, the OHCHR considered some gruesome photos and videos of dead detainees as outrages to personal dignity but also as "broader context of the humiliating and degrading sexual abuse to which detainees were treated when alive" including the "[t]reatment of female bodies, clothes having been removed or bras pulled up and trousers and underwear pulled down to fully expose their breasts*

and/or genital areas. The case of Isaipriya is a clear example of such desecration and outrage upon personal dignity. The OHCHR Investigation on Sri Lanka (OISL) reviewed numerous other photos and videos of unidentified dead women demonstrating a similar pattern, some obviously LTTE [Liberation Tigers of Tamil Eelam] fighters partially in uniform or wearing wide-legged trousers and checked men's shirts, and others in civilian clothing, all having breasts and genitalia exposed. In some cases, the legs had been spread wide. In videos, the cameras often linger over the genital areas, while the uniformed soldiers present can be seen and heard making sexual comments. The commentary which accompanies this video is particularly shocking. The soldiers are heard making very graphic, lewd and offensive sexual comments about the naked female corpses. In one of the videos, the semi-naked bodies of women are thrown onto a lorry without any kind of respect for the dignity of the deceased." In a similar video, the soldiers are seen to be celebrating their achievements, laughing and appearing to enjoy filming the genitals and breasts of deceased naked Tamil women.

Principle 4.

Add Value or Don't Do It

4.3 *Are there alternative sources?: We will look for alternative sources of SCRSV information and will ask ourselves whether our mandate or objective really requires us to interview survivors or use information sourced from them. We recognise that finding alternative sources removes the potential risks to survivors, those around them and to ourselves, of gathering such information directly from survivors, takes the pressure off survivors and provides more space for them to choose to participate or not.*

This principle suggests that open-source information – as an 'alternative source' of information – may have a valuable role to play in complementing interview-based information. In some instances, the open-source information may corroborate or be an alternative source to testimonial evidence, thus potentially reducing the risk to the survivor often associated with, for example, being interviewed.

Much of the time, valuable alternative source information does not include depiction of survivors or violations per se but provides contextual information, which can demonstrate who was in the area and what other things were happening. Such information can show movement, as well as events in the same location or timescale which can be critical to showing responsibility of perpetrators. Such information that does not depict survivors or violations often presents fewer risks to survivors but can be incredibly valuable for strengthening cases.

Practitioners should remember that both the survivor and individuals other than the survivor may have posted relevant content and should build that into their investigation planning and process, avoiding assumptions about what does and does not exist online. As part of investigation planning, practitioners should therefore consider where to find alternative sources of open-source information other than that posted by or about the survivor that might be sufficiently effective and impactful for their identified purposes, as required by Murad Code Principle 4.3. For example, have other people posted videos about an incident that include context and details about that incident? If seeking original content – such as the original video or photo from the person who created the video or photo, or the first uploader (when different people), as opposed to copies that others 're-post' to their accounts – practitioners should consider whether it may be better to first approach the documenter and/or uploader, with additional precautions when the documenter and/or uploader is a survivor.

Principle 8.

Gather Information From Other Sources

8.1 *Look for SCRSV information which is not from or about survivors: We recognise that useful information about SCRSV is not always from or about a survivor. We will seek to collect and use such information about SCRSV from wider sources (such as statistics, expert reports or analysis, and perpetrator information) as this information poses less risk for survivors, and can mitigate over-reliance on survivor information.*

8.5 *Do not undermine trust in humanitarian services: We will respect the importance of confidentiality and trust to the provision of support and care for survivors, and will not request or pressure support services to share information which a survivor has not consented to sharing.*

Relevant open-source information includes all publicly available information potentially relevant to an investigation that is accessible to open-source practitioners, including information and material that does not depict or concern any particular survivor. In addition to the resources mentioned in Murad Code Principle 8.1, wider digital sources include government or nongovernmental websites, online databases, posts about other affected parties, statistical information from service-providers assisting survivors, and observations from journalists and human rights researchers. Practitioners should not try to force confidential information about specific survivors into the public domain.

9. PREPARING FOR POTENTIAL COMMUNICATION WITH SURVIVORS AND OTHERS FOR CONSENT

Open-source practitioners do not ordinarily engage SCRSV survivors depicted in or otherwise associated with open-source content. Moreover, an advantage of open-source research is that it can be a very important component of efforts to avoid sourcing

information about SCRSV from survivors themselves, for reasons flagged in **Murad Code Principle 8.1**. However, practitioners may have to plan for the possibility of needing to engage survivors and others depicted in or associated with open-source content, particularly to secure consent or to check or confirm that consent was provided earlier, in order to store, share, publish or otherwise use that content

A. Overarching Considerations and Murad Code Principles

The use of public and online content still has privacy, legal and security consequences for survivors. Accessing it and using it can cause harm to survivors.

Principle 8.

Gather Information From Other Sources

8.3 *Look for SCRSV information which is not from or about survivors: We recognise that useful information about SCRSV is not always from or about a survivor. We will seek to collect and use such information about SCRSV from wider sources (such as statistics, expert reports or analysis, and perpetrator information) as this information poses less risk for survivors, and can mitigate over-reliance on survivor information.*

Just because content is readily available online, it does not mean that practitioners have consent to use that information.

Principle 2.

Respect Survivor Control and Autonomy

2.3 *Survivor control over their information: We will respect and support a survivor's right to privacy, which we understand to include control and autonomy over their personal history, identity and image. We will protect any personal survivor information or data (in whatever form) as confidential. We will not use or share that information without their express informed consent.*

Principle 3.

Be Responsible and Have Integrity

3.2 ***Dignity and respect:*** *We will support survivors with dignity, respect, humanity, courtesy, appreciation, and as decision-makers.*

Approaching survivors unexpectedly can heighten the risk of harm to them, as set out in Murad Code Principle 2.1.

This section of the Guide highlights why consent-focused engagement may be required, and from whom such consent may have to be sought. Given the Murad Code's focus on survivor rights, it highlights ethical considerations around survivor-related content in particular. It identifies the potential risks and harms and significant planning that must take place before practitioners contact anyone affiliated with the content they find, and explains why practitioners should be cautious even if their mandate permits communication with survivors and others. This section excludes considerations related to any engagement with alleged perpetrators, accomplices and others involved in the commission of SCRSV. It also does not provide detailed guidance on how open-source practitioners should conduct the necessary risks assessments and otherwise plan for and implement engagement with survivors and others. Should practitioners undertake such engagement, the minimum standards of the Murad Code concerning engagement with survivors, and other relevant best practices, guidance and laws, apply.

B. Key Questions and Considerations Around Consent and Potential Communication with Survivors and Others

When, from whom and how informed consent should be secured can be particularly confusing and challenging in an online investigation context as compared with other investigation contexts.[71] A major difficulty in digital open-source investigations is understanding *whether* consent may be needed, and if so, *whose* consent should be sought. The focus here is on survivor-related content. The following structure roughly follows the likely flow of key considerations and work in relation to this topic.

Is it 'survivor-related' content? Does it depict a survivor or specific incidents against them?

Any open-source content – whether it is text-based, audio-based, image-based or in another form – which depicts, describes or suggests that someone may be a survivor is necessarily 'survivor-related' content that, coupled with other considerations, may trigger

a need to plan for potential engagement with that survivor for their consent prior to its use.

Do not assume open-source survivor-related content comes with implied consent to use it.

Practitioners should never assume that survivor-related content is appropriate to use, even if the posts are public-facing (Murad Code Principles 2.3, 3.2 and 8.3). For example:

- Depicted survivors may not have known that they were being recorded and that the content was posted. Had they known, they may not have consented, and they may not have agreed to being publicly identified or described as victims or survivors of SCRSV.
- The person who has recorded survivors sharing their experiences of SCRSV may have violated an agreement with the survivors not to publish that content.
- Content posted by others may describe those depicted in the content as SCRSV survivors when they are not.
- Content posted by someone else may include an indication from survivors that they consented to its publication, but the survivors' circumstances may have changed and they may not want the content to be used any further.
- If posted by the survivor, their interest in sharing information publicly may have changed, or may not include the intended use.

> ***Case Study – Public Statements.*** *"A video on You Tube showed a gathering of victims and survivors of a dictatorial regime who met for the first time a few days after the fall of the said dictator who had been in power for decades. The amateur video showed a woman addressing the small crowd through a microphone, saying in a very emotional way that she had been raped while in detention. As she had made the statement herself in a public meeting, I assumed she was identifying herself as a survivor. She later became a public figure and when I met her a year later and spoke to her about what she had said, she denied ever having done so and refuted that she had been sexually assaulted. This was a stark reminder that even public statements in front of a crowd should never be taken as 'lasting consent' and that the survivor probably did not consent to being filmed and even less to the video being posted online."*[72]

Practitioners should especially not assume that because a survivor posted content about the SCRSV that they personally experienced, that they have provided ongoing, informed consent for practitioners to preserve and use that information during their investigation (Murad Code Principles 1.2 and 2.3). For example, it is possible that a survivor's personal, familial or community context may have changed after they posted the content online.

The sharing, publication or other use of such content can have severe consequences for persons depicted or described, their families, communities and others. Their lives may be

put at risk, they may be (re)traumatised, (further) stigmatised, (further) marginalised and have their privacy and dignity re-violated.

It is important to understand the risks of harm practitioners' intended use may cause, even if the information is already public-facing. For example, intended storage (preservation) or other use of the content involves a risk of disclosure to or access by third parties that could be harmful to or unwanted by the survivor (for example, for reasons related to stigma, psycho-social well-being, control over their information, privacy or security). Any intended sharing, publication or other use risks amplifying the visibility or accessibility of the content in ways that could be unexpected, unwanted by or otherwise harmful to the survivor (for example, for reasons related to stigma, psycho-social well-being, control over their information, privacy or security).

Thus, engaging survivors may be required to:

- secure consent seemingly not yet provided, or
- check, confirm or verify consent that was explicitly or implicitly provided earlier.

Verifying the extent of a survivor's existing consent

It may be possible to verify whether there is an existing consent granted for use of the survivor-related content without contacting the survivor. For example, if a human rights organisation has published survivor stories on their website or as part of a report, that organisation should have a set of informed consent records relating to the sharing and use of that information.

Among others, Murad Code Principles 2.3, 3.2 and 8.4 are relevant here.

Principle 8.

Gather Information From Other Sources

8.4 ***Verify survivor intention:*** *We will seek to verify indirectly sourced SCRSV information (including photos and videos of survivors), including where, when and how the information was obtained, and how and what consent was provided by the survivors for what use, and the initial intent or will for later use if shared by a survivor. If we cannot verify the survivor's consent or intent for their information to be used for our purpose, we will not use or share such information if we cannot properly mitigate the associated risks and harms.*

Regarding consent that has seemingly been provided earlier, there also may be questions about, for example, the content and scope of survivors' earlier consent (for example, survivors may have consented to the use of the content for advocacy but not for judicial accountability purposes, or survivors may have consented to the low-key use of the content but not to its use in a way which would amplify that content and draw more attention to the survivors), or about whether the earlier consent was properly secured and fully informed. As noted above, survivors' circumstances may have changed since they

provided the earlier consent. The more time has elapsed since the earlier consent has been provided, the likelier it is that survivors may want to withdraw or otherwise review that consent.

The open-source content and/or contextual information may show that the initial intention for the content's use still applies and covers the use to which the present practitioners want to put it. However, practitioners must carefully evaluate whether their conclusion that the survivor's original consent still applies and covers the (later) intended use is unbiased and well-founded, and practitioners should document or articulate the basis on which they made that determination.[73]

Should there be any doubt over the extent or continuation of existing consent, then a careful consideration process, including an added-value and risk assessment (described below), of whether and how to approach a survivor to renew or obtain consent is required.

Value-added assessment: does the intended use add value when weighed against the risk of approaching a survivor for their consent

As set out in the "Responsible Decision-Making" section above, Murad Code Principles 4.1-4.7 provide a useful framework to consider whether open-source practitioners should even consider approaching a survivor for consent, given the risks that could arise and the resources necessary to do this safely. Practitioners may decide that they will not gather or preserve, share, publish or otherwise use information about SCRSV if doing so would require procuring consent of survivors or others. Equally a practitioner may make this decision in relation to specific content because the information or their intended use is not as important as the well-being and safety of the individual depicted in that content, or because they were unable to verify or confirm consent to use that information without engaging the individual.

Risk assessments as a critical foundation to any decision to seek or confirm consent from a survivor

Practitioners should not assume that all survivors have similar risk profiles and interests. Accordingly, practitioners must evaluate risks on a person-by-person basis.

Principle 8.

Gather Information From Other Sources

8.3 ***Recognise rights and risks from indirectly sourced information:*** *We acknowledge that there are privacy, legal and security implications from the collection, receipt or use of indirectly sourced information from or about survivors, even if the information is in the public domain, in archives or retrievable from online (including public and non-public) sources. We recognise that the Code also applies to the gathering and use of such information.*

Risk assessments (**Murad Code Principles 5.3** (quoted on page 22)**, 5.4** and **8.3**) must be comprehensive, not only vis-à-vis survivors, but also others, including open-source practitioners, their colleagues and in case earlier consent was provided to a third party but that consent must be checked, that third party. The assessment must also include an evaluation of legal risks.

Principle 5.

Preparation is the Foundation

5.4 ***Remote interactions:*** *We will ensure that we understand the unique challenges and risks of online and other remote interactions with survivors. These include challenges regarding preparations; communications and data security; the survivor's access to technology; vetting those assisting us in the survivor's location, including intermediaries and interpreters; monitoring the survivor's well-being and comfort levels; and ensuring safe emergency response systems in the survivor's location. We acknowledge the serious risks that remote interviews with survivors who may face heightened risk of harm, including children, can entail. If we cannot appropriately address such challenges and risks, we will not proceed with remote interactions.*

Case Study – Legal Risks. *Legislation can make it very dangerous for international organisations to reach out to sources in some countries. For example, Russian law creates significant risks for sources present in the Russian Federation or in occupied territories of Ukraine who are contacted by international organisations to be perceived as critical of the Russian government. On April 28, 2023, the Russian Federation Federal Law No 157-FZ was passed, adding a new type of criminal offence described in s. 284.3 of the Criminal Code as "assisting in performance of decisions of international organizations in which Russia does not participate, of foreign state bodies' decisions, related to criminal prosecution of, in particular, Russian state officials". This offence is punishable by incarceration for up to 5 years. State treason (s. 275 Criminal Code) was in 2022 amended to include, among other actions, "providing financial assistance, technical assistance, consultations, or any other assistance to a foreign state, international of foreign organization, or their representatives, in activity aimed against security of the Russian Federation". This offence is now punishable by incarceration for up to 20 years. There is also a less grave offence (s. 275.1 Criminal Code) defined as "establishment of a confidential cooperation with a representative of a foreign state, international of foreign organization," provided that there are no elements of state treason. There is also an administrative offence for "public actions aimed at discreditation of the Russian Armed Forces" (s. 20.3.3 of the Russian Code*

of administrative offences), which is punishable by fine up to 50 000 RUB (circa 620 USD). A helpful collection of related resources are provided by OVD-Info.

Confirming earlier consent with a survivor

An important question concerning any checking of earlier consent is who should engage the survivor. Should it be those to whom the earlier consent was provided? In general, that may be the best option. A relevant consideration may be Murad Code Principle 7.9, which underscores the importance of continuity and consistency in communicating with survivors. However, risk, value-added and other assessments may show that the earlier content-taker no longer exists or for other reasons will not be able to or may not be suitable to reengage the survivors (e.g., Murad Code Principles 4.1-4.7, 5.3 and 8.3).

Principle 7.

Build Systems, Competency and Support

7.9 ***Continuity and consistency:*** *We will seek to ensure that the same person is communicating with survivors, to maintain trust and comfort levels, and to minimise risks that may flow from a change in personnel. We will discuss with the survivor any request from them to change personnel or the contact person, and we will respect their request.*

The final step before any determination to proceed with engaging with survivors (or others) is undertaking a holistic assessment of safety and well-being ramifications of proceeding to engagement, in consultation with (among others) an expert on the protection of survivors and witnesses. This assessment should include physical, psychosocial and digital security risks[74] to any individual who might be affected, including the survivor, the survivor's family, the survivor's community, the practitioner and their team. The assessment should be informed by SCRSV minimum standards and best practices, including those concerning competencies of everyone involved and those advanced by trauma experts, and supported by holistic, trusted support services accessible to the survivor.

Were survivors to be engaged by or at the request of open-source practitioners, the minimum standards distilled in the Murad Code pertaining to such engagements apply and should be carefully followed. What follows are a few examples of some key considerations for open-source practitioners about engaging survivors.

First, practitioners should assess which experts are or will be supporting open-source practitioners with the engagement. Everyone, including security specialists and any interpreters and intermediaries, must have appropriate knowledge, skills, attitudes and training. These are important planning decisions and steps to take in advance of establishing any contact with survivors, whether directly or indirectly (through

intermediaries). Practitioners should work through those with expertise in communicating with SCRSV survivors in a trauma-informed manner.

Practitioners must seek tailored advice from communications and security experts on private, discreet and safe means of digital or other communications, prior to attempting to contact any survivor and should steer away from inquiries made over public-facing posts or by sending direct messages to survivors over social media platforms. Appropriate, safe means of communication should be determined as part of the risk assessment process (see **Murad Code Principle 5.3** and the "Risk Assessment and Mitigation" section above). As with in-person contact, remote contact can involve considerable risks.[75]

Practitioners should consider the possibility that some survivors may not have exclusive control over their digital lives, exclusive access to or control over landline phones, mobile phones or other digital devices, and that their accounts may be under the control of or be accessible to others, including family members. The personal circumstances of some survivors may also be such that they rarely have private time away from family members, colleagues or others. Such circumstances present important privacy, confidentiality, security and psychosocial risks.

Regarding interpretation and translation, appropriate means of communication should also include ensuring the ability to communicate in a language accessible to the survivor, in order to support their control and informed decision-making consistent with **Murad Code Principles 2.3** and **2.4**. AI-facilitated interpretation and translation tools are inadequate for such sensitive communications.

Consistent with **Murad Code Principle 2.1**, which cautions against 'unexpected approach', practitioners should also consider whether a phone or internet-based call, if being considered as the means of initial contact, is appropriate. For example, an unexpected call which brings up distressing information may shock survivors, regardless of whether they are with other people at the time.

Once communication has been established, **Murad Code Principles 2.2, 2.3** and **2.4** require practitioners to respect and support a survivor's choices concerning the survivor's control over their information. Practitioners should discuss with survivors how the proposed use may magnify public exposure to the survivor's experiences, negatively affect their online or offline identity or impose other risks.[76] To ensure respect for survivors and their autonomy, practitioners should not explicitly or implicitly condition or promise access to any aid, assistance, protection or other benefit in exchange for a survivor's agreement to provide information or consent to its use. Any consent must be specific, express and fully informed.[77]

Practitioners should be prepared to provide information about services for survivors (**Murad Code Principles 5.6** and **7.7**), including medical and psychosocial support, protection, advocacy, legal and other services, should they reach out to them about using open-source content. This may include helping survivors to understand their data privacy rights and interests, and options for protecting or preserving those rights, including over where that data is sent, who has access, and how it is used.

Practitioners should implement a clear plan for the survivor's emergency access to support so that support can be available before, during, or after any interaction they may have and when the practitioners or others publicly release or amplify content which has the potential to negatively impact the survivor.

Before initiating communication with survivors, practitioners should establish a protocol for survivors to safely follow-up with them after the conclusion of the investigation, as per Murad Code Principle 5.9. While contact or follow-up may be impossible for open-source practitioners for a number of reasons – including the anonymity or pseudonymity of information shared online, the deletion or removal of accounts, digital risks or threats that might be triggered by remote contact, organisational policies that prohibit direct contact with individuals and other reasons – when practitioners do successfully initiate contact with survivors, they need to be prepared in case later contact is needed at various stages of their research to update survivors on the progress of the investigation, if appropriate and safe to do so.

Who else's consent might be needed?

Open-source information may depict or concern survivors who are impossible to contact. For example, they may be unidentifiable, detained, unsafe to contact (e.g., because they are under constant surveillance) or deceased. In such cases, practitioners should still enquire whether they may need the consent of others such as family members, bystanders and content uploaders for the intended use. They need to conduct all necessary risk, value added and other assessments to weigh the potential value versus the potential risks of proceeding with using that content, in accordance with, for example Murad Code Principles 4.1-4.7 and 8.3.

Regarding *whose* consent may have to be sought, apart from survivors, other rights-holders may have an interest in the content. These individuals include:

- others depicted in the open-source content, including bystanders
- the creator and/or uploader of the content and
- family or other community members (even if not depicted or otherwise included in the content).[78]

Review throughout all phases

Practitioners' initial assessment that they may or may not need to plan for such engagement may have to be revisited during the investigation phase. For example, practitioners may have originally determined not to publish any information about SCRSV but, during their research, revised their original decision because of the unanticipated quality and volume of that content; that change in planned use will necessitate a revision of the investigation plan. Practitioners should consider the possible need to communicate with survivors and others during the preparation phase (this section), investigation phase (Section B), and reporting, communicating and other use phase (Section C).

C. Consent Considerations Related to Material Depicting or Describing Children

Upholding a child's right to participate in the decision-making process, as per Murad Code Principle 2.5, requires open-source practitioners to handle the identification, collection, analysis and use of such digital open-source information with particular caution.

Children may be survivors, witnesses, perpetrators or otherwise affected by or involved in violations and crimes (for example, children who may have been abducted and then used in fighting).

Age determination can be hard in practice - relevant contextual information may be missing from a piece of digital open-source content, and it can be especially difficult to ascertain who is a child in online spaces where they may be anonymous or pseudonymous. A practitioner cannot assume an individual is over a certain age just because they are present on a social media platform that has age restrictions, as such restrictions are rarely enforced.

Practitioners should add the additional protections afforded to children,[79] such as using personnel with demonstrated competency, skills and experience in working with children (Murad Code Principles 5.3, 7.4 and 7.6) and conducting best interests of the child (BIC) assessments, when weighing whether to use digital open-source information that may depict minors. This underscores the importance of deploying child experts on digital investigation teams.[80]

In the case of CSAM, contact with a child is only done by trained law enforcement after very careful risk assessments and planning. The purpose is primarily to prevent further abuse and provide support and, if possible, pursue legal accountability. For open-source practitioners who are not mandated justice or protection officers, reaching out to children for consent to use CSAM should be strictly avoided.

For other types of content, practitioners should be advised by child experts and follow the UN Convention on the Rights of the Child and best interest of the child (BIC) assessments when including children in decision-making. It is important to know the age of consent in the country where the child is, to consider best practice guidance on when and how informed assent should be obtained from a child, and when the informed consent of their parent, legal guardian or other appropriate adult is required.[81]

B. SECOND PHASE: CONDUCTING THE INVESTIGATION

The Berkeley Protocol identifies six main phases to the investigation process: (a) online inquiry (search or discovery); (b) preliminary assessment; (c) collection; (d) preservation; (e) verification; and (f) investigative analysis. These processes may overlap and repeat throughout the investigation lifecycle. In this section, some of these phases are combined, while state of mind and monitoring considerations are added.

1. STATE OF MIND

In addition to the guidance above on the importance of open-mindedness and non-bias during preparation, practitioners should be careful to conduct their investigations with an appropriate state of mind. Given the remote nature of most online open-source investigations, there is a risk that practitioners may feel disconnected from the people and incidents they are investigating, and that given the volume of materials and duration of online searches, practitioners may become desensitised to the humanity of the situation. Practitioners should take steps, at the onset of and throughout investigations, to remain sensitive to the fact that real human beings, their experiences and concerns are at the centre of their work. Practitioners should not gamify their investigations in ways that dehumanise or desensitise themselves or others to those who have been impacted by SCRSV.

2. IDENTIFICATION (SEARCH/DISCOVERY)

Practitioners are reminded of the advice in the Guide's "Introduction", that upon discovery of indicators of SCRSV, they should PAUSE, THINK and GET ADVICE (and consult relevant protocols) before acting.

Principle 9.

Take the Time, Create the Space

9.2 ***Reduce time pressures:*** *We will seek to remove time pressures to promote voluntary and informed decision-making, enabling survivors to share their information in the way and at the pace they wish. We recognise that like rushed interactions, lengthy interactions can also be a form of pressure and a cause of discomfort to survivors, particularly for children. If there are any fixed time-limits which a survivor needs to understand in order to exercise their rights, we will discuss these with the survivor.*

Although digital open-source practitioners often experience a sense of urgency, especially when open-source information is being rapidly shared and removed from online spaces, practitioners should still seek to remove time pressures, in accordance with Murad Code Principle 9.2. The goal of that is to promote voluntary and informed decision-making, both for survivors (where applicable) and for themselves and their team, and to take time to be thoughtful about whether, when and how to handle SCRSV-related materials. In the context of digital open-source investigations, removing time pressures is relevant for safeguarding appropriate time for digital investigation planning, building protocols and processes for handling sensitive digital information and securing informed consent from survivors to use the material when needed.[82]

If a practitioner comes across an image or other depiction of child abuse or exploitation (CSAM/CSEM), they should follow the steps set out in the "CSAM/CSEM Response and Reporting Protocol" portion of the "Online Content Depicting Children" section above.

3. PRELIMINARY ASSESSMENT AND COLLECTION

Principle 4.

Add Value or Don't Do It

4.10 ***Data minimisation:*** *We will only collect, store and use a survivor's personal information, including digital information, if justified for a clear purpose, necessary for achieving that purpose and proportional to the ability to fulfil that purpose, and if we can protect that information.*

There is a tension – which must be acknowledged and carefully resolved by practitioners – between the recognised risk of removal of online material which drives calls for collection and preservation so as not to lose information, and the recognised risks of data collection to those whose data you have collected. Following the risk assessments conducted during the preparation phase, practitioners should be aware of the risks that collection and preservation raise for survivors and others. For example, collected material may be hacked or may otherwise become vulnerable to being shared beyond the investigation team; material collected for legal investigation purposes may be potentially disclosable to the defence; material held by a government actor may be subject to public disclosure requests; or materials on servers may not be secure or may be subject to regulatory or state access.

Critically, collection may amount to criminal 'possession' of child sexual abuse or exploitation material, as emphasised at the start of this Guide.

The concerns above underscore the importance of adhering to data minimisation principles throughout an investigation, including limiting the sharing of and exposure to digital open-source information to those who have a legitimate, professional need to have access to be consistent with Murad Code Principle 4.10.[83]

Compliance with data minimisation principles may require practitioners to think carefully before scraping large quantities of data from social media and other online sites and further assess what doing so may mean for their ability to responsibly manage that data. For example, what does possession of such a large volume of information mean for the quality of their investigation and their legal liabilities?

4. PRESERVATION

Principle 3.

Be Responsible and Have Integrity

3.7 *Do not damage potential evidence: We will not take or remove original documents, physical items or other potential evidence from a survivor or location, even when asked to do so, unless we have the mandate, it is necessary to do so, we can do so safely, there is no one in a better position and role to do this, and we have the capacity to manage and safeguard the integrity of such evidence.*

Practitioners must refrain from damaging any potential evidence and should consider whether they are the right person to safeguard such evidence; this is a nuanced consideration, particularly in relation to SCRSV materials. Given the risk of removal of online information, especially that which is graphic and/or related to SCRSV, preservation is often flagged as a key consideration in open-source investigations. However, there are legal considerations and considerable risks if the open-source practitioner cannot preserve the material properly and safely, and where the possession of this material by persons who are not law enforcement professionals may be criminalised.

A notable exception to the preservation principle is information that depicts sexualised violence against children, including nudity, which is almost always illegal to possess, transmit, etc. Non-content information about such material should be immediately reported to the appropriate authorities and potentially to the platform on which it sits.

For SCRSV content that is legal to possess, has been risk assessed, for which there is added value in preservation, and which the practitioner can safely handle and safeguard, practitioners should preserve a copy, following the guidance provided by the Berkeley

Protocol,[84] including by collecting contextual information and metadata, and ideally hashing all downloaded content if that content may be useful as legal evidence. Any modifications or analytical work should be done on a copy of the saved content, in order to maintain the integrity of the original. In keeping with Murad Code Principle 3.7, practitioners should also be sure not to manipulate or otherwise damage the preserved, original, digital file. When that is impossible, practitioners should note any modifications.

The commitment to confidentiality and de-identification found in Murad Code Principles 2.3 and 7.8 requires that practitioners evaluate any options for anonymising or pseudonymising the survivor or other information which may identify the survivor in the data collected, such as by blurring faces on images (copies, not the original images that may be evidence), or other protections; any legal or other implications and requirements should be considered when deciding if and how to implement such protections.

At later stages, respecting and supporting a survivor's choices necessitates transparency with any authorities, partner organisations, affected individuals and communities and others about the limitations inherent in concealing the survivor's identity when using digital open-source information. Murad Code Principle 2.3 specifies that practitioners should protect the confidentiality of survivors' information and data, for example when preserving digital open-source information for later potential use. Adhering to these obligations in the context of open-source investigations includes consideration of what it means to 'share' information, and when information is shared, ascertaining the most secure means of doing so.[85]

5. MONITORING

Monitoring processes – regularly reviewing pre-specified sites, hashtags, key terms or accounts for new content, sometimes in real time – raise significant risks of secondary and vicarious trauma, given that the practitioner will often have little to no warning about what they might come across. In addition to preparing for the possibility of discovering SCRSV content prior to the onset of an investigation, teams should have detailed protocols for monitoring processes that reduce the risk of harm, including secondary or vicarious trauma, at any point in which new SCRSV material may be discovered over the course of an investigation.

6. VERIFICATION AND INVESTIGATIVE ANALYSIS

Note: *In this Guide and in this particular context, 'verification' refers to using digital means of assessing the reliability and authenticity of digital content — it does not refer to verification through 'triangulation' of evidence by way of direct contact with survivors.*

Given the risks of encountering mis/disinformation online, practitioners should take particular care with the verification of digital content, following guidance in the Berkeley Protocol to engage in source, technical and content analysis.[86] This is especially important given the sensitivity of content depicting or implicating SCRSV, and the potential legal and ethical consequences of using, and thereby legitimating, SCRSV content that is fake, misleading or otherwise unreliable. The methodology for verification should be planned as part of the investigation plan.

When conducting their investigative analysis (the reviewing and interpretation of verified content to develop substantive findings), practitioners should pay attention to when particular open-source research methods or gender-related considerations require expertise that is not present in the investigatory team – for example, image/video comparison analysis (which is a professionalised field of practice with certification processes), or how sexualised violence may be described differently when it is perpetrated against men or women, or against adults and children. Practitioners should engage the appropriate experts if needed or refrain from continuing the research until they acquire the appropriate expertise.

Furthermore, practitioners should be aware that methods and tools related to digital investigations emerge and change quickly and should be sure that their team updates its training as necessary. Practitioners should also be careful to make clear and, if possible, address the limitations of any verification process.

7. COMMUNICATING WITH SURVIVORS AND OTHERS DURING AN INVESTIGATION

See the section “Preparing for Potential Communication with Survivors and Others for Consent” in Section A.

C. THIRD PHASE: REPORTING, COMMUNICATING AND OTHER USE

This section applies to any practitioner who shares digital open-source information privately or publicly, including within investigation teams, with the public (including through media) and in court or other accountability processes.

1. COMMUNICATING WITH SURVIVORS AND OTHERS PRIOR TO PUBLISHING AND OTHER USE

Practitioners' respect for survivors and their personal space should extend to their digital spaces, as per Murad Code Principle 10.3. As part of this, practitioners should take care to not bring additional and/or unnecessary attention to survivors', uploaders' or their own social media feeds or other online communications. That is to avoid negatively impacting their use of those spaces, such as by triggering trolling (when someone posts a comment or other information online that is intended to upset the survivor, the uploader or others) or by doxing (revealing private information about the survivor, the uploader or others).

Even when practitioners do not speak with the survivor directly, they should respect the importance of a survivor's control over how their experience is shared, amplified or otherwise used. If known, practitioners should be sensitive to survivors' desire over how to conduct any interaction with investigators and any use of or reference to their experiences.[87] If not known, practitioners should seek to discover the survivor's wishes over how to conduct any interaction and any use of or reference to their experiences. See the section "Preparing for Potential Communication with Survivors and Others for Consent" in Section A.

Practitioners should take an inclusive, intersectional approach[88] to their research that recognises that each survivor is a unique individual who may have been previously marginalised or silenced.

A. Internal Sharing

Given the sensitive and often explicit nature of SCRSV information, internal sharing should be limited to as small of a group as possible and based on a needs and risk assessment. Sharing material unnecessarily may compound the effects of the initial violation against the survivor, can risk harming colleagues and can increase the risk of the information being shared outside the team and organisation. Internal data protection systems and protocols should be deployed responsibly and effectively to maximise the confidentiality and security of this information.

B. Criminal Justice and Other Legal and Quasi-Legal Proceedings

The harm to survivors of unconsented sharing and use in criminal justice or other legal or quasi-legal proceedings (such as human rights inquiry bodies or truth commissions) can include retraumatisation and revictimisation. Investigators, prosecutors and others should think carefully about what content/material to use as evidence, given the risk of retraumatisation to survivors, and also to court personnel, juries, judges, commissioners, etc. For example, explicit images of CSAM can be traumatising and there may be alternatives to its use. Viewing by prosecutors, judges and the defence are usually limited to exceptional circumstance and only when strictly necessary.[89]

C. Reporting Violative Content to Hosting Platforms, Law Enforcement or CSAM Hotlines

As noted in the "Online Content Depicting Children" section above, it is important to have a policy, process and instructions for reporting potentially criminal content, including CSAM, CSEM and other explicit imagery, to law enforcement and to CSAM hotlines. For each platform being searched, it is also important to be familiar with its community standards and terms of service and to know how and when to appropriately report such content to those platforms.

D. Other Non-Public Sharing

Any form of sharing, including non-public sharing, creates risks to the privacy and well-being of SCRSV survivors and may otherwise compound the violation or crime that they have experienced. Sharing with UN bodies, such as special procedures, investigative mechanisms, fact-finding commissions or commissions of inquiry, requires an assessment of the protection and potential uses and sharing of that information by that body, as well as their consent processes.

Principle 2.

Respect Survivor Control and Autonomy

2.3 *Survivor control over their information: We will respect and support a survivor's right to privacy, which we understand to include control and autonomy over their personal history, identity and image. We will protect any personal survivor information or data (in whatever form) as confidential. We will not use or share that information without their express informed consent*

As detailed above and required by Murad Code Principle 2.3, any survivor-related content should only be used or shared with the express, specific consent of the survivor for use, type of use and sharing.

Equally for each individual or organisation with which practitioners intend to share, the practitioner should carry out due diligence and risk assessments, as well as ensure confidentiality, upholding of principles of informed consent for all further use and sharing, and the protections of the Murad Code to the shared material. This would include putting in place documents such as memorandums of understanding, non-disclosure agreements, partnership agreements, etc.

E. Publication

Practitioners must safeguard pre-publication privacy and conduct legal, ethics and security reviews of any information to be published. This could include redaction, pseudonyms, checks for mosaic/cumulative identification, removing personally identifiable information, checking that geolocation coordinates or other information do not inadvertently reveal the location or identification of sources, removing original source links, etc. Careful consideration of both transparency on sources and methodologies and protection of individuals is required, but with the rights of individuals trumping other considerations. Safeguarding also requires identification of risk to the reader or viewer; trigger warnings, blurring of graphic visuals and other content modifications may help minimise any risks.

If there might be a backlash – either online or offline – practitioners should prepare a mitigation or other response strategy in advance of sharing or publishing the results of their open-source research.

Principle 3.

Be Responsible and Have Integrity

3.4 ***Ensure accuracy:*** *We will check that our understanding and representation of the information gathered are correct and free from misrepresentations or assumptions.*

Practitioners should conduct a content review, which assess all outputs for accuracy, stigmatising language or misconceptions around SCRSV, its survivors, perpetrators and others (community, family, etc). Content should also not fixate on or sensationalise graphic or explicit details of a survivor's experience.[90]

Principle 10.

Ensure Respectful and Safe Interactions

10.8 ***Do not ask if you do not need to:*** *We will also not fixate on or sensationalise [explicit, sensitive or graphic details of sexual violence] when representing or reporting a survivor's experience.*

F. Sharing Back to Affected Communities

An important ethical component of research is to share the results with those affected and/or who contributed to research or publication. Considerations of consent, confidentiality and deidentification, what is appropriate to share, with whom, when and how should be assessed by the practitioner and their team. Practitioners should recognise and mitigate the risks of collective trauma and other impacts from SCRSV when sharing back to affected communities.

2. LEARNING LESSONS, REVIEW AND IMPROVEMENT

While monitoring, adjusting and improving processes should be carried out during all phases of the investigative process, the sharing and use phases are particularly valuable timepoints for reviewing the entire process and gathering and incorporating lessons learned with regards to policies, procedures and practice. This can include whether risks were effectively mitigated, processes were efficient and safe, and whether there is any feedback or remedial steps required to improve future processes, including whether the decisions made during **Murad Code Principle 4: Add Value or Don't Do it** were the right ones for this process.

CONCLUSION

In 2021, the UN documented 3,293 cases of conflict-related sexual violence, which constituted an increase of 800 cases from the year before. Although only a tiny fraction of survivors secured legal accountability for these crimes in either international or national courts, the UN estimates an additional 32,930 to 65,860 cases went unreported – strongly suggesting the need to strengthen the documentation and analysis of such crimes and violations.[91]

The scale of under-documentation and under-prosecution of SCRSV is massive. Given the extraordinary increase in the use of smartphones and social media by communities around the world during the first quarter of the 21st century, digital open-source information may provide critical contextual, base and linkage evidence that practitioners can use to strengthen the evidentiary foundations of human rights and criminal cases, fact-finding reports, advocacy reports, news reports, etc. However, the goals of reporting, advocacy, justice, reparations and the like are only truly served when investigations and associated activities centre the interests and rights of survivors.

The hope is that this Guide – and future refinements and improvements – will be practically useful and strengthen the likelihood that digital open-source investigation work is both effective and survivor-centred.

MURAD CODE PROJECT

ANNEXES

ANNEX 1 - DEFINITIONS AND TERMINOLOGY

This Guide defines all terms as they are defined in the Murad Code or as they are defined in the Berkeley Protocol. Some key terms are reproduced or introduced below:

a. *Open-source information/digital open-source information:* Open-source information is that which any member of the public can observe, purchase or request without requiring special legal status or unauthorised access.[92] Digital open-source information is open-source information that can be accessed from the internet.

b. *Open-source practitioner:* Anyone (paid or unpaid) who gathers or uses publicly-accessible information as defined above, including from the internet. Such practitioners may intentionally or unintentionally discover information related to SCRSV during any stage of their research.

c. *Child:* Any person under 18 years old, as defined in the UN Convention on the Rights of the Child of 1989.

d. Child Sexual Abuse Material (CSAM) and Child Sexual Exploitation Material (CSEM): These terms have different legal definitions in different countries. In general, they commonly define CSAM as imagery or videos which show a person who is a child and engaged in or is depicted as being engaged in explicit sexual activity or exposing a sexual organ for the purpose of exploitation or abuse.

e. *Child marriage:* According to the United Nations International Children's Emergency Fund (UNICEF), child marriage "refers to refers to any formal marriage or informal union between a child under the age of 18 and an adult or another child."[93]

f. *Survivor:* In this context, a person depicted in digital content as being subjected to sexual violence that may be systematic or conflict-related. The terms 'victims' and 'survivors' can have different meanings in different settings and languages, and those who have experienced violence may prefer one term over the other, or neither. Like the Murad Code, this Guide uses the word 'survivor' instead of 'victim' as the former is most often considered empowering. However, survivors' choices of identity should be respected and reflected by those around them. It is also important to acknowledge that some victims do not survive the violence. While the Murad Code focuses on working with survivors, aspects of the Code also apply to the protection of privacy and rights of victims who experienced and survived SCRSV but may since have died.

g. *Systematic or Conflict-related Sexual Violence*: The Murad Code defines this term broadly: "SCRSV includes rape, sexual slavery, forced prostitution, forced pregnancy, forced abortion, enforced sterilization, forced marriage, trafficking in persons for the purpose of sexual violence and/or exploitation, and any other form of sexual violence of comparable gravity perpetrated against any person where that conduct is directly or indirectly linked to an armed conflict. It also includes such acts during peacetime or transitional phases when they are part of systematic, repressive, structured, or political violence, and when such violence is used to terrorise or destroy communities. SCRSV

includes but is not limited to sexual violence which amounts to the international crimes of genocide, crimes against humanity or war crimes."

h. *Lead evidence:* Lead evidence suggests that a crime may have taken place, even if it does not explicitly depict the crime itself, and may lead or point to other evidence. It functions as 'evidence' insofar as it may propel an investigation forward, even if the material itself is not subsequently presented in a court of law.[94]

i. *Primary evidence:* Also referred to as 'crime-based evidence', primary evidence is "evidence of the crimes upon which the charges are based, including information about who, what, where and when. For example, if the alleged perpetrator is charged with murder as a crime against humanity, any information proving that there was a murder is considered crime-based evidence."[95]

j. *Linkage evidence:* Linkage evidence is "evidence of the responsibility of the alleged perpetrator for the crimes committed, which is particularly important if the perpetrator did not directly commit the crime. In other words, it is the evidence that connects the responsible party with the crime. For example, in cases in which the allegation is that a superior failed to prevent or punish alleged violations of which they were aware or should have been aware, linkage evidence is that which proves this awareness or tends to show that the superior was in 'effective control' of the direct perpetrator."[96]

ANNEX 2 – EXAMPLES OF INTERNATIONAL AND REGIONAL INSTRUMENTS ON CHILD SEXUAL ABUSE MATERIAL (CSAM) AND CHILD SEXUAL EXPLOITATION MATERIAL (CSEM)

- UN Convention on the Rights of the Child, 1990
- Optional Protocol to the (U.N.) Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2002
- UN Convention on Cybercrime, 2024
- ILO Convention on Worst Forms of Child Labour, 1999
- African Charter on the Rights and Welfare of the Child, 1990
- African Union Convention on Cyber Security and Personal Data Protection, 2014
- CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) "Lanzarote Convention", 2010
- CoE Convention on Cybercrime, 2004 (Budapest Convention)
- EU Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography (under revision draft Directive 2024)

- Regulation (EU) 2021/1232 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (interim one in place extended to 2026 with NCMEC reporting by electronic communication service providers) and new proposed regulation on preventing and combatting sexual abuse and sexual exploitation of children under consideration EUR-Lex - 52022PC0209 - EN - EUR-Lex
- League of Arab States, Arab Convention on Combating Information Technology Offences (Arab Convention), 2010
- ASEAN Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse, 2019 (non-binding) and Regional Plan of Action 2021

ENDNOTES

[1] For more general guidance on investigating SCRSV, see UK Foreign and Commonwealth Office, *International Protocol on the Documentation and Investigation of Sexual Violence in Conflict: Best Practice on the Documentation of Sexual Violence as a Crime or Violation of International Law* (2nd ed), 2017, https://www.gov.uk/government/publications/international-protocol-on-the-documentation-and-investigation-of-sexual-violence-in-conflict; International Criminal Court (ICC), *Policy on Gender-Based Crimes,* 2023, https://www.icc-cpi.int/sites/default/files/2023-12/2023-policy-gender-en-web.pdf; *Hague Principles on Sexual Violence,* 2019, https://thehagueprinciples.org/; WITNESS, *Video as Evidence Field Guide: Using Video to Support Justice and Accountability for Sexual and Gender-Based Violence,* https://library.witness.org/product/sgbv-guide/; Institute for International Criminal Investigations (IICI), *Guidelines for Investigating Conflict-Related SGBV Against Men and Boys,* 2016, https://iici.global/wpd/wp-content/uploads/2023/08/160229_IICI_InvestigationGuidelines_ConflictRelatedSGBVagainstMenBoys.pdf; UN Women, *Identifying Gender Persecution in Conflict and Atrocities: A Toolkit for Documenters, Investigators, Prosecutors and Adjudicators of Crimes Against Humanity,* UN Women, 2023, https://www.unwomen.org/en/digital-library/publications/2022/01/identifying-gender-persecution-in-conflict-and-atrocities.

[2] Make no investigation-related contact with survivors of SCRSV unless the person making the contact is an expert in engaging with survivors. Related aspects are addressed later in the Guide.

[3] See *International Protocol*, pp.24. For practical purposes, when designing investigation methodologies, investigators may consider creating their own list of potential SCRSV proxy indicators that is appropriate for their context.

[4] See e.g. *International Protocol*; Koenig and Egan, "Power and Privilege: Investigating Sexual Violence with Digital Open-source Information," *Journal of International Criminal Justice*, vol. 19, no. 1, 17 May 2021, pp.55-84; Koenig and Egan, "Hiding in Plain Sight: Using Online Open-source Information to Investigate Sexual Violence and Gender-Based Crimes," in *Technologies of Human Rights Representation*, edited by Dawes and Moore, SUNY Press, 2022; Bagdasar, "Recognising Sexual and Gender-Based Violence as an Open-source Researcher," *Bellingcat*, 3 Mar. 2023, www.bellingcat.com/resources/2023/03/03/sexual-and-gender-based-violence-open-source-researche-osint-digital/.

[5] See e.g. OSCE, "Mapping the Online Landscapes of Risks of Trafficking in Human Beings on Sexual Services Websites Across the OSCE Region," 2023, https://www.osce.org/cthb/555441.
[6] See e.g. Zarmsky, "Is International Criminal Law Ready to Accommodate Online Harm?" *Journal of International Criminal Justice*, 9 May 2024, https://doi.org/10.1093/jicj/mqae013; Dubberley and Ivens, "Outlining a Human-Rights Based Approach to Digital Open-source Investigations: A Guide for Human Rights Organisations and Open-source Researchers," University of Essex, 2022, https://repository.essex.ac.uk/32642/1/Outlining%20a%20Human-Rights%20Based%20Approach%20to%20Digital%20Open%20Source%20Investigations.pdf.
[7] See Hill, "This Week in Horrible Journalism: Jezebel's Rape Photos," *Forbes*, 10 Feb. 2012.
[8] Koenig and Egan, "Hiding in Plain Sight".
[9] Brown and Lavoie, "Rising Rates of Rape and Sexual Violence in Conflict Should Be an Alarm Bell," *UNDP Blog,* 25 June 2022, as quoted in Koenig, Ghaly and Levine, "Merging Responsibilities: Ethical Considerations for Securing Consent in Open-Source Investigations of Conflict-Related Sexual Violence," *Journal of International Criminal Justice*, vol. 22, no. 2, 2024, pp.263-280, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4895271.
[10] OHCHR & HRC, 2022.
[11] See e.g. *International Protocol*; ICC, *Policy on Gender-Based Crimes*; *Hague Principles*; WITNESS *Video as Evidence SGBV Field Guide*; IICI *Guidelines for Investigating Conflict-Related SGBV of Men and Boys*; UN Women, "Identifying Gender Persecution".
[12] Berkeley Protocol, chapters IV and V.
[13] See e.g. South Africa Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007, Chapter 6 – National Register for Sex Offenders, § 42, *Government of South Africa*, 2007.
[14] Canadian Centre for Child Protection, *Survivors' Survey Full Report*, 2017, Canadian Centre for Child Protection, www.protectchildren.ca/en/resources/survivor-survey-report/. See fig. 83 pp.147-155.
[15] Newton, "The Secret Lives of Facebook Moderators in America," *The Verge*, 2019, https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona.
[16] See e.g. Crown Prosecution Service (CPS), Guidance on Indecent and Prohibited Images of Children, latest update 2024, https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children.
[17] See e.g. Philippines Law 11648 Section 4(s). See also S.4(p) "to join a website that hosts such material"; Belgian Criminal Code Art.417/47; Italy Law 238/ 2021 (even if not stored or downloaded); Netherlands Criminal Code Sections 240b, 252.
[18] See e.g. Australian Criminal Code.
[19] See e.g. South Korean Act on the Protection of Children and Youth Against Sexual Offenses.
[20] E.g. in the UK courts have interpreted 'making' to include opening an attachment to an email containing an image; downloading an image from a website onto a computer screen; storing an image in a directory on a computer; accessing a pornographic website in which indecent images appeared by way of automatic "pop-up" mechanism; and receiving an image via social media, even if unsolicited and even if part of a group. See CPS, Guidance on Indecent and Prohibited Images of Children.
[21] See e.g. Argentina Penal Code Art.128 (knowing possession, distribute or disseminate).
[22] See e.g. Colombian Criminal Code Art.213-219C.
[23] See e.g. Colombian Criminal Code Art.213-219C; Philippines Law 11648 Section 4(d); South Korean Act on the Protection of Children and Youth Against Sexual Offenses; Belgian Criminal Code Art.417/44.

[24] See e.g. Ireland Criminal Law (Sexual Offences Act 2017) s.14(2).
[25] See e.g. South Africa Criminal Law (Sexual Offences and Related Matters) Amendment Act 32, 2007 §54 (1)(a).
[26] UN Convention on Cybercrime, Art.16 (non-consensual dissemination of intimate images); UK Online Safety Act (2023) Section 187 (sending images of genitals), 188 (sharing image or film of person in intimate state without consent); German Criminal Code Section 184k (without approval, create or transmit a photograph/image of genitals, breasts, underwear), 201a (without approval, creates or transmits photograph/image of person in private premises/protected from view); Italian Criminal Code, Article 612-t34 ICC (sends, … disseminates sexually explicit images without consent); Brazil Penal Code Article 218C (make available, transmit, …. Disseminate … photography, video or other audio-visual records that contains a scene of rape or rape of a vulnerable person or that makes incitement or induces its practice, or, without the consent of the victim, sex scene, nudity or pornography.)
[27] See e.g. Netherlands Criminal Procedure Code Art.160 (most serious crimes including rape); Ireland s.9(1)(b) of the Offences Against the State (Amendment) Act 1998 (serious offences); Australia New South Wales Crimes Act s.316 (serious indictable offences which includes assaults).
[28] Note that data can be classified as non-content data (i.e., traffic data like IP address, date, time, size, type, duration, and source of communication; location data, which is data that helps identify the subscriber).
[29] "In 2017, content moderators sued Microsoft after viewing CSAM over the course of their employment and developing PTSD, claiming employer negligence, and not receiving the necessary counselling. In February 2020, Facebook reached a settlement with 11,250 current and former moderators resulting in a combined compensation of $52 million for mental health issues resulting from the job. In September 2020, former content moderators filed a lawsuit against YouTube, alleging that YouTube did not support the mental health of moderators, leading to "severe psychological trauma for the employees. … The suit was finalized in late 2022, with an approximate $4.3 million settlement. As part of the settlement, YouTube agreed to provide content moderators with onsite and virtual counselling services by licensed clinicians for individual biweekly sessions, as well as access to telephonic counselling and peer support groups that meet monthly." International Centre for Missing and Exploited Children, *The First Line of Defense in Online Child Protection: A Model Framework for Employers of Content Moderators,* 2024.
[30] Rahman and Ivens, "Ethics in Open-source Investigations," in *Digital Witness,* edited by Dubberley et al., Oxford Academic, 2019. Researchers Rahman and Ivens recommend adopting a human rights, rather than a utilitarian, approach to decision-making, including with regards to using digital materials in investigation processes. They argue that human rights — and thus a sensitivity to the inherent dignity of all involved — should be 'respected and protected' at all stages, including data collection, verification and presentation. See also Koenig and Egan, "Power and Privilege," citing to Hu, "Responsible Data Concerns with Open-source Intelligence", *Responsible Data*, 14 Nov. 2016, https://responsibledata.io/2016/11/14/responsible-dataopen-source-intelligence/. See also Wood, "Social Media Intelligence, the Wayward Child of Open-source Intelligence", *Responsible Data*, 12 Dec. 2016, https://responsibledata.io/2016/12/12/social-media-intelligence-thewayward-child-of-open-source-intelligence/.
[31] For templates that can aid with digital investigations planning, see the annexes in the Berkeley Protocol.

[32] See e.g. McAvoy, "Centering the 'Source' in Open-source Investigation," *Open Global Rights*, 21 Jan. 2021. This article explains the importance of centring the needs and interests of the individuals who share information online, and/or about whom that information is shared.
[33] Importantly, such discovery of sexual violence material differs from the "unexpected disclosure" described in Murad Code Principle 5.8, in that the survivor has not necessarily consented to such information or material being captured, recorded, or published online.
[34] Berkeley Protocol, chapter V, subsection E(1)(d).
[35] Berkeley Protocol, section IV(B)2(e). For additional resources, see DART Center for Journalism and Trauma, *Working with Traumatic Imagery,* 2014, https://dartcenter.org/content/working-with-traumatic-imagery, *Advice for Dealing with Vicarious Trauma,* 2015, https://dartcenter.org/media/advice-dealing-vicarious-trauma; Antares Foundation, *Managing Stress in Humanitarian Workers;* Human Rights Resilience Project, *Tools and Programmes for Resilience*.
[36] See e.g. Koenig and Lampros, *Graphic: Trauma and Meaning in Our Online Lives*, Cambridge University Press, 2023; Winny, "Let's Talk About Mental Health," *Centre for Information Resilience*, 16 Nov. 2023; WITNESS, *Video as Evidence SGBV Field Guide*; Dubberley et al, "Digital Human Rights Investigations: Vicarious Trauma, PTSD and Tactics for Resilience," in *Digital Witness: Using Open-source Information for Human Rights Investigation, Documentation, and Accountability*, edited by Dubberley et al., Oxford University Press, 2020.
[37] *International Protocol*, pp.108-110, 139.
[38] See e.g. "Holistic Security: A Strategy Manual for Human Rights Defenders," *Tactical Technology Collective*, 2016. See generally, Citizen Lab Website at https://holistic-security.tacticaltech.org/downloads.html. See also Myanmar Witness, "Pro-SAC Digital Offensive," 17 Oct. 2023, https://www.myanmarwitness.org/reports/pro-sac-digital-offensive (pro-democracy individuals through their social media footprints); Amnesty International, "Thailand: State-backed digital violence used to silence women and LGBTI activists," 16 May 2024, https://securitylab.amnesty.org/latest/2024/05/thailand-state-backed-digital-violence-used-to-silence-women-and-lgbti-activists/ (women activists targeted by digital surveillance); Human Rights Watch, "Spyware Targets Human Rights Watch Staff in Jordan," 1 Feb. 2024, https://www.hrw.org/news/2024/02/01/spyware-targets-human-rights-watch-staff-jordan. Other examples include telephone contacts and laptops searched at check points or house searches in occupied territory in Ukraine, Sudan and many other places. With regards to stigma and its effect on reporting on SCRSV, see Lanthier et al, "Coming out of the closet about sexual assault: Intersectional sexual assault stigma and (non) disclosure to form support providers among survivors using Reddit," *328 Social Science and Medicine*, 2023; United Nations Security Council Meetings Coverage, "Shame, Stigma Integral to Logic of Sexual Violence as War Tactic, Special Adviser Tells Security Council, as Speakers Demand Recognition for Survivors," 15 May 2017; Mellen et al, "The Psychosocial Consequences of Sexual Violence Stigma: A Scoping Review," *Sage Journals*, 2024.
[39] See Berkeley Protocol, annexes.
[40] For an overview of potentially relevant considerations see Annex V of the Berkeley Protocol, "Considerations for validating new tools." See also the Guidance of the United Nations Secretary-General on Human Rights Due Diligence for Digital Technology Use.
[41] See e.g. Berkeley Protocol, chapter IV; Smith et al., "Holistic Security: A Strategy Manual for Human Rights Defenders," *Tactical Technology Collective*, 2016.
[42] A virtual private network (VPN) is a means to create a secure connection and relative anonymity for someone accessing the Internet. Note that there are protection limits to the use of VPNs: see,

e.g. Matthews-El and Bottorff, "Is Using a VPN Safe? What You Need to Know About VPN Security," *Forbes*, 1 Jun. 2024, https://www.forbes.com/advisor/business/software/are-vpns-safe/.

[43] As a side benefit, masking a device's location and/or setting its signal to an alternate location can also help with searching for and identifying information relevant to the investigation.

[44] A sock puppet is a term for using a fake identity online. False identities are often assumed online to protect the investigator's identity, investigation, those impacted, and affiliated devises. The legality and ethics of assuming a false identity varies across jurisdictions relevant to an investigation, the purpose for which the investigation is being conducted, and the professional identity of the investigator.

[45] Berkeley Protocol, chapter VI, subsection E.

[46] See e.g. Matsuo, "Deepfakes and Korean Society: Navigating Risks and Dilemmas," Korea Economic Institute of America, 3 Oct. 2024; Kim, "In South Korea, Rise of Explicit Deepfakes Wrecks Women's Lives and Deepens Gender Divide," PBS News, 3 Oct. 2024; Martin, "'Anyone Can Be a Victim': Sprawling AI Fake Nudes Crisis Hits South Korea," Wall Street Journal, 28 Aug. 2024.

[47] See e.g. Berkeley Protocol, section VI(E); McDermott, Koenig and Murray, "Open-source Information's Blind Spots: Human and Machine Bias in International Criminal Investigations," *Journal of International Criminal Justice*, vol. 11, no. 1, 2021, pp. 85.

[48] See e.g. Berkeley Protocol, chapter II(A)3; McDermott, Koenig and Murray, "Open-source Information's Blind Spots, pp. 85-105; Zarmsky and Mionki, "Symposium on Fairness, Equality and Diversity in Open-source Investigations: Out in the Open: Fair Trial Rights and Open-source Evidence at the ICC," *OpinioJuris*, 2023.

[49] Leiby, "Digging in the Archives: The Promise and Perils of Primary Documents," *Politics & Society,* vol. 37(1), pp 75-99, 2009. For further discussion and examples, see Elliott et al., "Bridging the Gap Between the Reality of Male Sexual Violence and Access to Justice and Accountability," *Journal of International Criminal Justice*, Vol.18, pp.469-498, 2020, https://ideas.repec.org/a/sae/polsoc/v37y2009i1p75-99.html.

[50] See e.g. Koenig and Egan, "Power and Privilege"; Koenig and Egan. "Hiding in Plain Sight"; Bagdasar, "Recognising Sexual and Gender-Based Violence as an Open-source Researcher".

[51] See e.g. Koenig and Egan, "Power and Privilege"; Koenig and Egan, "Hiding in Plain Sight"; UN Office of the High Commissioner for Human Right, *Integrating a Gender Perspective into Human Rights*, 2018, https://www.ohchr.org/sites/default/files/Documents/Publications/IntegratingGenderPerspective_EN.pdf; ICC, *Policy on the Crime of Gender Persecution*, 2022, https://www.icc-cpi.int/sites/default/files/2022-12/2022-12-07-Policy-on-the-Crime-of-Gender-Persecution.pdf.

[52] See e.g. Emergent Justice Collective, "Intersectional Approaches to Investigations Webinar," January 2022, https://www.youtube.com/watch?v=5aczrTj_wHg; Gopalan, "Breaking Binaries and Honing-in on Harms: Inclusive Approaches Towards Sexual and Gender-Based Crimes," *Contemporary International Criminal Law Issues*, pp. 265-303, 2023; UN Office of the High Commissioner for Human Rights, *Guidance Note on Intersectionality*, 2022, https://www.ohchr.org/sites/default/files/documents/issues/minorities/30th-anniversary/2022-09-22/GuidanceNoteonIntersectionality.pdf; ICC, *Policy on Gender-Based Crimes*, pp. 10; Egan, "Digital Accountability Symposium: Intersectionality and International Criminal Investigations in a Digital Age," *Just Security*, 19 Dec. 2019.

[53] See e.g. McDermott, Koenig and Murray, "Open-source Information's Blind Spots", pp.85.

[54] Koenig and Egan, "Hiding in Plain Sight".

[55] WITNESS, "Supporting Survivors of Gender-Based Violence: Documenting Evidence," 2022, https://blog.witness.org/2022/03/supporting-survivors-of-sgbv-documenting-evidence/.

[56] Berkeley Protocol, section II(A).
[57] Various jurisdictions have created legal mandates for the reporting of child sexual abuse material that is encountered online. See section "Online Content Depicting Children" in this Guide. See also 18 U.S. Code §§ 2258 and 2258A, which mandates the reporting of such material to the CyberTipline or the National Center for Missing and Exploited Children.
[58] Koenig and Egan, "Hiding in Plain Sight".
[59] Berkeley Protocol, Annex III.
[60] See e.g. Afghan Witness, "Violence behind a screen: rising online abuse silences Afghan women," 17 Nov. 2023, https://www.info-res.org/afghan-witness/reports/violence-behind-a-screen-rising-online-abuse-silences-afghan-women/; Amnesty International, "Iran: Security forces used rape and other sexual violence to crush 'Woman Life Freedom' uprising with impunity," 6 Dec. 2023, https://www.amnesty.org/en/latest/news/2023/12/iran-security-forces-used-rape-and-other-sexual-violence-to-crush-woman-life-freedom-uprising-with-impunity/.
[61] Examples of non-verbal/visual information include phenomena like looking away when asked about sexual violence, or objects like broom handles, glass bottles, or weapons next to individuals who are deceased.
[62] Berkeley Protocol, Annex III.
[63] See e.g. in the United States it is illegal to possess or distribute child pornography, more formally known as child sexual abuse material. This law could be triggered by digital open-source practitioners that download, use or share such material, even when their intent is human rights or law enforcement oriented, if they don't have legal authorisation to possess or distribute such material. Social media companies that identify such material on their platforms report that content to the National Center for Missing and Exploited Children, which then works with law enforcement to encourage the investigation and prosecution of child sexual exploitation. See also section "Online Content Depicting Children" in this Guide.
[64] See e.g. ICC, Rules of Evidence and Procedure, Article 63(4); *International Protocol,* pp. 61 (a conviction can be based only on the evidence of a victim). See International Commission of Jurists, "Sexual Violence Against Women: Eradicating Harmful Gender Stereotypes and Assumptions in Laws and Practice", 2015, https://www.icj.org/wp-content/uploads/2015/04/Universal-GenderStereotypes-Publications-Thematic-report-2015-ENG.pdf, pp.13-16, for a discussion of the troubling history of old cautionary rules which required corroboration for victims' testimony.
[65] See e.g. OSCE, "Mapping the Online Landscapes".
[66] See e.g. *International Protocol*, pp.24; Koenig and Egan, "Power and Privilege"; Koenig and Egan, "Hiding in Plain Sight"; Bagdasar, "Recognising Sexual and Gender-Based Violence as an Open-source Researcher".
[67] UN Women, "Identifying Gender Persecution".
[68] Some useful resources include: The Hague Principles on Sexual Violence (addressing what might amount to an act of a sexual nature); *International Protocol*, pp.24; and UN Early Warning Indicators Matrix (which sets out scenarios and fact patterns in which sexual violence has occurred previously or commonly in relation to conflict).
[69] See e.g. OSCE and Asian Partnership for Co-Operation, "Combating Technology-Facilitated Trafficking in Human Beings in Central Asia and Across the OSCE Asian Partners for Co-operation," 2021, https://www.osce.org/cthb/497032; OSCE, "Mapping the Online Landscape of Risks of Trafficking in Human Beings on Sexual Services Websites Across the OSCE Region," 2023, https://www.osce.org/cthb/555441.
[70] Report of the OHCHR Investigation on Sri Lanka, ¶ 571, UN Doc. A/HRC/30/CP.2 (Sept. 16, 2015), pars. 323–325.

[71] Koenig, Ghaly and Levine, "Merging Responsibilities", pp.263.
[72] Quotation of a practitioner who wants to remain anonymous.
[73] Berkeley Protocol, pp.11-12.
[74] See Berkeley Protocol, section IV; Smith et al., "Holistic Security".
[75] See e.g. IICI, *IICI guidelines on remote interviewing*, Aug 2021, https://iici.global/wpd/wp-content/uploads/2023/07/IICI-Remote-Interview-Guidelines.pdf. IICI urges great caution before undertaking any remote interviews and related contact with survivors, and unreservedly discourages remote interviews and related contact with children.
[76] Koenig, Ghaly and Levine, "Merging Responsibilities".
[77] Ibid.
[78] For more on whether, when and how consent should be secured to use digital open-source information in an investigation, see Koenig, Ghaly and Levine, "Merging Responsibilities", pp. 263.
[79] See e.g. ICC, *Policy on Children*, 2023, pp.30, https://www.icc-cpi.int/sites/default/files/2023-12/2023-policy-children-en-web.pdf.
[80] See also IICI, *IICI guidelines on remote interviewing*.
[81] See e.g. UNICEF and International Rescue Committee, *Caring for Child Survivors of Sexual Abuse Guidelines (Second Edition)*, 2023.
[82] See section A(9) of this Guide. For more on the role of informed consent in digital open-source investigations also see e.g. Koenig, Ghaly and Levine, "Merging Responsibilities".
[83] Berkeley Protocol, chapter II, subsection B(2).
[84] Berkeley Protocol, section VI(D).
[85] Berkeley Protocol, chapter IV, subsection B(3) and subsection C(1)(a).
[86] Berkeley Protocol, section VI(E).
[87] See e.g. interview by Charlotte Maher with Leyla Hussein, "Speaking of Violence," Bellingcat, 15 August 2025, https://rss.com/podcasts/bellingcatstagetalk/2167911/.
[88] See e.g. Emergent Justice Collective, "Intersectional Approaches"; Gopalan, "Breaking Binaries"; Stahn and de Silva (eds.), *The International Criminal Court in its Third Decade*, 2023; UN Office of the High Commissioner for Human Rights, *Guidance Note on Intersectionality*, 2022; ICC, *Policy on Gender-Based Crimes*, pp.10.
[89] See e.g. CPS, Guidance on Indecent and Prohibited Images of Children, sections on Viewing the Images, Providing Images to the Defence.
[90] See e.g. interview by Charlotte Maher with Leyla Hussein, "Speaking of Violence".
[91] Brown and Lavoie, "Rising Rates".
[92] Berkeley Protocol, pp.6.
[93] https://www.unicef.org/protection/child-marriage.
[94] See e.g. WITNESS *Video as Evidence Field Guide on Sexual Violence*, pp.8.
[95] Berkeley Protocol, pp.27.
[96] Ibid.