UC Berkeley
UC Berkeley Previously Published Works

Title

Merging Responsibilities: Ethical Considerations for Securing Consent in Open-Source Investigations of Conflict-Related Sexual Violence

Permalink

https://escholarship.org/uc/item/3h73d4rk

Author

Koenig, Alexa

Publication Date

2024-07-01

Peer reviewed

eScholarship.org Powered by the California Digital Library
University of California

Merging Responsibilities

Ethical Considerations for Securing Consent in Open-Source Investigations of Conflict-Related Sexual Violence

Alexa Koenig,[*] Anthony Ghaly[**] and Simone Lieban Levine[***]

ABSTRACT

In emergent fields of practice, there is often an 'ethics lag' — a period of significant innovation during which the focus is on what can be accomplished more than on the safeguards that should be put in place to protect the public from the unanticipated consequences of that innovation. This is true of the emergent field of digital open-source investigations conducted for international criminal justice purposes, in which researchers and analysts comb the Internet for information relevant to their research. One sub-field where the ethics lag is particularly of concern is digital investigations of conflict-related sexual and gender-based violence ('CRSV'), especially with regards to whether and when investigators need consent from social media posters, survivors, bystanders and others to use information discovered in online spaces. This article explores options for centering and promoting victim safety and dignity by clarifying ethical issues that investigators should consider before using open-source information to support international investigations and prosecutions of CRSV. After identifying where the relevant law leaves gaps in guidance, the authors discuss a series of considerations that may help investigators ethically handle such sensitive data. Ultimately, the authors underscore the importance of securing consent from survivors when engaging in digital open-source investigations into sexual violence. What arguably varies is who should seek that consent, when, and how.

[*] Research Professor of Law, University of California, Berkeley (USA); Co-Faculty Director, Human Rights Center, UC Berkeley School of Law (USA) [kalexakm@berkeley.edu]
[**] PhD Student, Jurisprudence and Social Policy, University of California, Berkeley (USA); Graduate Student Researcher, Human Rights Center, UC Berkeley School of Law (USA) [anthonyghaly@berkeley.edu]
[***] Director of the Pro Bono Program, University of California College of the Law, San Francisco (USA); Research Manager (Pro Bono), Human Rights Center, UC Berkeley School of Law (USA) [levinesimone@uclawsf.edu]
All cited websites last visited 15 March 2024.

1. Introduction

In 2014, a video depicting the sexual assault of a woman in Cairo's Tahrir Square went viral.[1] After being uploaded to YouTube, the video was picked up by news outlets around the world. A global uproar ensued.

YouTube initially refused to remove the video from public view. As a result, millions of people around the world witnessed the woman's assault. Meanwhile, the survivor had little to no control over who accessed the video or the ways in which social media users deployed it.[2]

Seven men associated with assaults that took place that day, including the attack depicted in the video, were eventually sentenced to life in prison.[3] While on one hand these prosecutions can be considered a win for justice and an illustration of the powerful role that online images can play in motivating and supporting cases, on the other, they reflect how a deeply traumatizing moment in a person's life, captured by a smartphone and transmitted over social media, can become the focus of global attention without their consent.[4]

While the criminal case that followed the assault was domestic, not international, this example raises an important yet underexplored issue relevant to international criminal law and practice: the appropriate role of survivors' consent to the use of social media posts and other digital open-source information[5] in international investigations. It also illuminates critical tensions: while the survivor of CRSV may not want open source evidence of their assault used in investigations in ways that

[1] D.D. Kirkpatrick and M.E. Sheikh, 'Video of Mass Sexual Assault Taints Egypt Inauguration', *New York Times*, 9 June 2019, available online at www.nytimes.com/2014/06/10/woπrld/middleeast/video-of-mass-sexual-assault-taints-egypt-inauguration.html?_r=0 (all websites cited in the article were last accessed on 15 March 2024); J. Malsin, 'Egyptians Debate Gender Violence After Video Shows Woman Being Raped in Crowd', *Time*, 10 June 2014, available online at https://time.com/2852874/egypt-rape-video; L. Dearden, 'YouTube Refuses Egypt's Request to Remove Footage of Tahrir Square Sexual Assault', *The Independent*, 15 June 2014, available online at www.independent.co.uk/news/world/africa/youtube-refuses-egypt-s-request-to-remove-footage-of-tahrir-square-sexual-assault-9537086.html.

[2] For more on YouTube's deliberations with regards to whether to remove the video, see A. Koenig and A. Lampros, *Graphic: Trauma and Meaning in Our Online Lives* (Cambridge University Press, 2023).

[3] S. Li, 'Egyptian Court Condemns Tahrir Square Sexual Assaults with Seven Life Sentences', *The Atlantic*, 16 July 2014, available online at www.theatlantic.com/international/archive/2014/07/egyptian-court-condemns-tahrir-square-sexual-assaults-with-seven-life-sentences/374518.

[4] For more on the debate that took place within YouTube about how to handle the video (whether to remove, retain on the platform, etc.), see Koenig and Lampros, *supra* note 2.

[5] Digital open source information is that which is publicly-accessible online through observation, request or purchase. Digital open source information can include written materials, databases, videos, photographs, audio and other digital files: see University of California, Berkeley, Human Rights Center and UN Office of the High Commissioner for Human Rights (OHCHR), *Berkeley Protocol on Digital Open Source Investigations* (2022) available online at www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf (hereafter *Berkeley Protocol*).

may bring more attention to their suffering, that information may be critical to corroborate other victims' testimonies or provide lead or linkage evidence for courts.

Given how quickly international criminal investigators have come to rely on digital open source information,[6] the fields of law and ethics are struggling to catch up.[7] While there is an inherent risk of retaliation and other harms for any victim[8] who complies with a criminal investigation or prosecution,[9] stigmas surrounding sexual violence—whether arising from notions of sexual purity, gender norms or otherwise—threaten a unique and heightened risk of social, physical and psychological violence for the victims of such crimes.[10] These dangers complicate investigations into such offenses, which are already impeded by the longstanding difficulties of collecting evidence of CRSV that meets the necessary evidentiary standards for prosecution, especially in the context of conflict or political unrest.[11] Despite or even because of these heightened challenges, digital open sources can be a vital source of information, whether to corroborate survivor testimonies, to generate leads to other evidence (including testimonial and physical evidence), or to otherwise strengthen the evidentiary foundation of a case.

Survivor interviews, a primary form of evidence in traditional CRSV investigations, take place in a very different context than digital investigations. Yet this difference and the ethical issues it triggers have been underexplored. First, in face-to-face interviews, it is relatively obvious whose

---

[6] See, e.g., L. Freeman, 'Prosecuting Grave International Crimes Using Open-Source Evidence', in S. Dubberley, A. Koenig, and D. Murray (eds), *Digital Witness: Using Open Source Information for Human Rights investigation, Documentation and Accountability* (Oxford University Press, 2020); K. Hiatt, 'Open Source Evidence on Trial', 125 *Yale Law Journal* (2016) 323.

[7] A. Koenig and U. Egan, 'Power and Privilege: Investigating Sexual Violence with Digital Open Source Investigation', 19 *Journal of International Criminal Justice* (2021) 55, at 57-58; S. Dubberley, A. Koenig, and D. Murray (eds), *Digital Witness: Using Open Source Information for Human Rights investigation, Documentation and Accountability* (Oxford University Press 2020).

[8] For simplicity's and breadth's sake, this article's consent framework uses the word 'victim' instead of 'survivors', as the person who has suffered CRSV may not have survived their attack.

[9] See, e.g., Freeman, *supra* note 6; Hiatt, *supra* note 6.

[10] See P. Harter, 'Libya Rape Victims "Face Honour Killings"', *BBC News*, 14 June 2011, available at www.bbc.com/news/world-africa-13760895 (describing a UNHCR official as saying 'when a rape occurs, it seems to be a whole village or town which is seen to be dishonoured', as well as quoting a Libyan volunteer as saying, '[t]o be seen naked and violated is worse than death for' women and girls who have been raped publicly, and describing how parents will kill their children who have been raped and some victims will kill themselves to avoid being murdered or bringing perceived shame to themselves and their families); M. Sable et al., 'Barriers to Reporting Sexual Assault for Women and Men: Perspectives of College Students', 55 *Journal of American College Health* (2006) 157, at 159 (ranking shame, guilt, embarrassment, fear of retaliation, confidentiality concerns, fear of not being believed, financial dependence on perpetrator/perpetrator not allowing help, and not wanting a family member or friend to be prosecuted as the barriers with the highest perceived importance).

[11] See e.g. W.H. Wiley, 'The Difficulties Inherent in the Investigation of Allegations of Rape before International Courts and Tribunals', in M. Bergsmo, A.B. Skre, and E.J. Wood (eds), *Understanding and Proving International Sex Crimes* 1, 369 (Torkel Opsahl Academic EPublisher, 2012).

consent should be secured to use any resulting testimonial evidence—that of the person sitting for the interview. This contrasts with digital open source investigations, where (as explained in greater detail later in this article) there may be various stakeholders whose consent is relevant to using the digital data. Second, while interviewing is often a confidential process, information provided through open sources is by definition public; as a result, any privacy interests may be undervalued by both the general public and even some investigators. Third, while interactions with CRSV survivors should only be conducted by investigators with specialized training in trauma-informed and gender-sensitive interviewing, the collection of digital open source information is increasingly conducted by an array of civil society actors who may not have this specialized training, yet aspire to share their findings with legal teams. Indeed, given bare-bone budgets and the potential benefits of information sharing, such interactions and even cross-institutional collaborations are increasingly common. For example, reflecting the reality that 'the fight against impunity…is a collective obligation' and that 'civil society organizations are critical to this common work,' the International Criminal Court (ICC) and Eurojust have launched guidelines to increase the likelihood that civil society organizations' documentation will better meet the needs of legally-mandated investigators.[12]

Procuring consent to use digital open source information related to CRSV undeniably increases digital open source investigators' workloads, potentially pitting the efficacy of an investigation against survivors' interests. Especially in the context of war, it may be unsafe or even impossible for investigators to contact those who appear in a posted photo or video, or even the poster themself.[13] Consent is vital, but it is not immune to pragmatic difficulties. Obtaining consent will simply not be possible in some situations, as when the victim is deceased or otherwise unreachable.

Despite these challenges, consent considerations can be conceptualized as a safeguard to promote victim agency and safety, to curb overzealous investigators, and to increase the victim's power in a situation where victims have historically and systematically been denied control. As explained in greater detail below, from an ethics perspective the potential value of the information for investigation purposes cannot outweigh the need for victim consent; investigators should also

[12] *Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations* (2022).

[13] For a deeper examination of issues related to evidence, SGBV, and armed conflict, see, e.g., R. Maphosa, 'The Unreported War: Tackling Denialism and Social Stigma Towards Victims of Armed Conflict-Related Sexual and Gender-Based Violence', 32 *Stellenbosch Law Review* (2021) 155.

ensure victims' safety and willing participation. As it stands, however, there is little scholarship on when, how and by whom consent should be incorporated into digital open source investigations.[14] By proposing the following consent considerations, we hope to encourage both lay and professional investigators to limit practices that may result in re-traumatization and related harms, and to allow victims to determine what justice looks like for themselves.

While we hope that all categories of open source investigators will find this article helpful, we are primarily focused on the use of open-source evidence as it relates to international criminal legal investigations, such as those conducted by the Office of the Prosecutor (OTP) of the International Criminal Court (ICC), by the investigators of ad-hoc international criminal tribunals, and by domestic courts trying international crimes. We are also focused on the quickly-growing field of civil society investigators and lawyers who share the fruits of their investigations with national and international prosecution teams. While issues of consent are no less important in the context of non-legal investigations, such as journalism and human rights reporting, those use cases are secondary for purposes of this article.

With this background in mind, we offer suggestions below for how digital open-source investigations of sexual violence might more consistently and ethically incorporate consent for various uses of open source data. Obtaining consent *from* the proper person, *by* the proper person, in the proper time frame, and with the proper disclosures prioritizes the needs of survivors and ensures that investigations are consistent with the ethical principle to do no harm—or at least to minimize any harm.

Notably, sexual violence is a crime defined *by* a lack of consent. As a result, investigators using open source evidence of survivors' assault without their consent could be understood in the most extreme situations to be committing a second consent-related violation—one that should be avoided at all costs.

In the section following this introduction, we provide an overview of our methodology. In Part 3, we summarize relevant law and the various literatures that address the role of consent in international criminal cases. In Part 4, we offer ethical factors for digital open source investigators to consider when evaluating whether, how and when to secure consent in digital investigations of

[14] Koenig and Egan, *supra* note 7, at 60 (discussing resources for strengthening investigations of CRSV while acknowledging there is 'relatively limited guidance specific to digital open source information').

CRSV. We conclude by reiterating the importance of taking a victim-centered approach to digital open source investigations—one that necessarily foregrounds consent.

2. Methodology

This topic was first conceived several years ago when one of the authors noted that the rapid development and utilization of digital open-source investigations was outpacing the related ethical considerations, including survivors' interests. As with most emerging areas of practice, emphasis in the open source investigations field was initially placed on what *could* be done by deploying new tools and methods for fact-finding, analysis and data visualization, as opposed to what *should* be done.[15] Such an 'ethics lag' is well documented in other fields involving emerging technologies,[16] given the rapid pace of technological change. Although there is a growing body of ethics guidance related to digital investigations,[17] the dearth of discussion specific to sexual violence and consent considerations was concerning. With the research assistance of several law students at the University of California, Berkeley, School of Law, the authors dove into the legal and ethical considerations relevant to securing consent to use digital open source data.

The team began by outlining the relatively unique harms and risks that conflict-related sexual violence victims face, such as cultural conceptualizations of sexual violence as not only a physical but also a dignitary assault, and existing protocols and guidelines for effectively and ethically investigating sexual violence in international contexts. Next, the team examined existing scholarship on digital open-source investigations, including minimum standards and best practices, and the developing consensus around the need to articulate ethical considerations related to open-source investigations more generally.

This research laid a foundation to begin addressing issues that are unique to the intersection of these two areas of expertise: in other words, the considerations that are not present in traditional

[15] See, e.g., G. Ivens, 'Responsible Open Source Investigations for Human Rights Research', Responsible Data, https://responsibledata.io/anniversary/responsible-open-source-investigations-for-human-rights-research (noting the emergence and importance of ethical questions regarding 'how to gain meaningful consent to publish findings and re-publish content, [and] what to do if consent is not possible').

[16] See, e.g., V. Wadhwa, 'Laws and Ethics Can't Keep Pace with Technology', Blog: MIT Technology Review, 15 April 2014, www.technologyreview.com/2014/04/15/172377/laws-and-ethics-cant-keep-pace-with-technology.

[17] See, e.g., *Berkeley Protocol*, *supra* note 5, at 14-15; L. Freeman, 'Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court', in Dubberley, Koenig, and Murray, *Digital Witness*, *supra* note 6; A. Koenig, F. McMahon, N. Mehandru and S.S. Batthachargee, 'Open Source Fact-Finding in Preliminary Examinations', in M. Bergsmo and C. Stahn (eds), *Quality Control in Preliminary Examination: Volume 2* (Torkel Opsahl Academic EPublisher, 2018).

investigations into sexual violence *or* in digital open-source investigations of other crimes. While investigators who interact directly with survivors have significant guidance with regards to the appropriate seeking of consent (for example, in using information shared during in-person interviews or documents that are physically handed over to investigators), there is relatively little for those who mine the Internet for potential evidence. Conversely, much of the guidance on open source investigations neglects the heightened sensitivity of handling digital information related to CRSV.

Testimonial, documentary and physical (or 'real') evidence may all be relevant to an investigation. Most guidance for CRSV investigations focuses on testimonial evidence, given a long-standing emphasis on talking with survivors, and thus largely assumes the investigator has direct access to the victim/survivor. However, digital open source investigations may be conducted thousands of miles from the affected parties and places. And while survivor testimonies are almost always considered closed-source information, digital open source information is by definition public. This has historically created some confusion around whether permission is needed to use online content or whether consent can be implied by the public nature of the content. Finally, with survivor testimony, it's relatively clear whose consent is needed—the survivor's. With digital content, there are often multiple interest bearers, ranging from the victim/survivor to bystanders who are visible in an image, to the person who captured an image, to the person who posted the material online. Some of these roles may be filled by the same person; often, they differ.

Next, the team considered how consent could or should be incorporated into digital open-source investigations of sexual violence. We asked several key questions starting with: why is consent necessary when it comes to using digital content posted publicly online? There seemed to be an obvious answer about victim re-traumatization versus opportunities for empowerment, as well as respect for victim autonomy and dignity in decision-making, but the question had multiple components and answers expanded over time. What benefits does consent provide to victims, primarily; secondarily, to affected communities; and thirdly, to investigations? What are the possible risks or even unintended consequences of seeking consent, especially with regards to online information? Should investigators seek consent from everyone depicted in the content, not just the victim(s) or the poster of the material (if not the same)? What should investigators do if they cannot ask for consent because the parties are anonymous or pseudonymous, have died or are otherwise unreachable? How should investigators consider the risk to victims, their families and

communities compared to the risk of missing out on digital information that could corroborate other forms of evidence?

After identifying these questions, the team examined various guidelines and other materials to assess how to incorporate an ethics-based consent framework into open-source investigations of CRSV and/or investigations that inadvertently surface evidence related to CRSV. A summary of our findings is below.

3. Social and Legal Context

Practitioners have estimated that for every reported instance of CRSV, approximately '10 to 20 cases go undocumented and unaddressed'.[18] For example, with regards to '3,293 UN-verified cases of conflict-related sexual violence in 2021, an increase of 800 from the previous year, an additional 32,930 to 65,860 went unreported'.[19] These rates reflect several challenges, ranging from an historic reluctance to recognize CRSV as a crime; a lack of training for investigators in identifying, documenting, and assessing CRSV; and an overall dearth of helpful evidence,[20] issues that can be further compounded by a lack of sensitivity to the needs of survivors throughout the investigation and prosecution process.

In response to these challenges, many organizations have put significant time, attention and resources towards improving the investigation and prosecution of CRSV and have provided much-needed guidance for investigators. While this literature often addresses the need to obtain informed consent to use testimonial information shared directly with investigators,[21] it largely glosses over digital open-source information as a source of evidence.[22] Below, we illuminate gaps in the legal and practical guidance that exists related to consent in CRSV investigations.

---

[18] A. Brown and A. Lavoie, 'Rising Rates of Rape and Sexual Violence in Conflict Should be an Alarm Bell', *UNDP Blog*, 25 June 2022, available online at www.undp.org/blog/rising-rates-rape-and-sexual-violence-conflict-should-be-alarm-bell.

[19] *Ibid*.

[20] See e.g., Wiley, *supra* note 11, at 369.

[21] S. Ferro Ribeiro and D. van der Straten Ponthoz, *International Protocol on the Documentation and Investigation of Sexual Violence in Conflict*, UK Foreign & Commonwealth Office, 2nd ed. March 2017, available online at www.un.org/sexualviolenceinconflict/wp-content/uploads/2019/06/report/international-protocol-on-the-documentation-and-investigation-of-sexual-violence-in-conflict/International_Protocol_2017_2nd_Edition.pdf (hereafter *CRSV Protocol*).

[22] A notable exception is S. Dubberley and G. Ivens, *Outlining a Human-Rights Based Approach to Digital Open Source Investigations: A Guide for Human Rights Organizations and Open Source Researchers*, UKRI Economic and Social Research Council and University of Essex Human Rights Centre, March 2022, available online at https://repository.essex.ac.uk/32642/1/Outlining%20a%20Human-Rights%20Based%20Approach%20to%20Digital%20Open%20Source%20Investigations.pdf. This guide

A. Consent and CRSV Investigations

Many hard-won gains in the ethical investigation and prosecution of CRSV are reflected in the approach of the International Criminal Court (ICC), whose *Rules of Procedure and Evidence* aim to 'ensur[e] that sexual crimes are prosecuted in an effective and gender-sensitive manner'.[23]According to the Rome Statute, the legal treaty underlying the ICC, the prosecutor is obligated to 'respect the interests and personal circumstances of victims and witnesses' and to 'take into account the nature of the crime, in particular where it involves sexual violence [or] gender violence'.[24] In addition, the Court is required to 'take appropriate measures to protect the safety, physical and psychological well-being, dignity and privacy of victims and witnesses … particularly during the investigation and prosecution of such crimes.'[25] While these are important safeguards, it's unclear how they apply to people depicted in open source information, as opposed to people with whom the OTP has interacted and who are already participating in the proceeding. The Rules of Procedure and Evidence also require the Prosecutor to secure prior consent before introducing into evidence any information which the Prosecutor received on the condition of confidentiality as potential lead information under article 54(3)(e) of the Rome Statute.[26] Article 54(3)(e) specifically allows the Prosecutor to promise not to disclose information unless he receives the consent of the 'provider' of that information.[27] In a digital open source context, it's unclear who the provider is—is the provider the person who recorded and/or posted the information online? Critically, the person who recorded or uploaded the data may not be the person depicted in the open source content, whose consent is really at issue. In many cases, they are not. Importantly, neither the Rome Statute nor the Rules of Procedure and Evidence provide formal or

emphasizes the importance of maintaining international human rights standards at each stage of a digital open source investigation and provides examples of the various rights at risk during such an investigation and ways to mitigate the risks to these rights, including the right to privacy, right to life and freedom from torture, inhuman or degrading treatment, and right to liberty.

[23] T. Altunjan, 'The International Criminal Court and Sexual Violence: Between Aspirations and Reality', 22 *German Law Journal* (2021) 878; see also Institute for International Criminal Investigations, *Global Code of Conduct for Gathering and Using Information About Systematic and Conflict-Related Sexual Violence* (2020), available at www.muradcode.com/murad-code (hereafter *Murad Code*); Institute for International Criminal Investigations, *Guidelines for Investigating Conflict-Related Sexual and Gender-Based Violence Against Men and Boys* (2016), available online at https://iici.global/0.5.1/wp-content/uploads/2017/03/160229_IICI_InvestigationGuidelines_ConflictRelatedCRSVagainstMenBoys.pdf.

[24] Art. 54(1)(b) ICCSt.

[25] Art. 68(1) ICCSt.

[26] Rule 82 ICC RPE.

[27] Art. 54(3)(3) ICCSt.

mandatory evidentiary protection for those with whom the Prosecutor is *not* in direct communication and/or to whom the Prosecutor has not directly committed, under article 54(3)(e), to keep their information confidential. While there is a general obligation to protect the 'confidentiality of the proceedings and the security of victims,' that obligation relates to the publishing of documents.[28] Thus, depending on context—for example, when publishing information isn't at issue—the poster of open source content and depicted victims and bystanders may fall into unprotected categories.

At the end of 2023, the ICC released a new policy on gender-based violence. That policy, however, also makes few references to open source evidence.[29] The policy simply references digital open source information as a potential source of evidence that may be relevant to investigations and prosecutions of gendered violence. When discussing the harms that may befall survivors due to cooperation with the Court, the analysis is limited to witnesses, implying there has been some type of contact with those individuals and that they have agreed to participate in proceedings before the Court.

The second edition of the International Protocol on the Documentation and Investigation of Sexual Violence in Conflict (CRSV Protocol) underscores the importance of taking a victim-centered approach to investigating and prosecuting CRSV, yet also largely overlooks the digital domain. The CRSV Protocol does, however, outline three principles considered fundamental to securing adequate consent that may extend to open source contexts. Those principles are comprehension, voluntariness, and stated permission.[30]

'Comprehension' involves not just fully disclosing all relevant information about the documentation process to the survivor, but making sure the survivor truly understands the information.[31] The participant should understand the full range of risks and benefits of contributing to an investigation, as well as how the information is going to be used.[32] Multiple articles

[28] Rule 43 ICC RPE.
[29] See ICC Office of the Prosecutor, *Policy on Gender-Based Crimes: Crimes Involving Sexual, Reproductive and Other Gender-Based Violence*, December 2023, available online at www.icc-cpi.int/sites/default/files/2023-12/2023-policy-gender-en-web.pdf, at §§ 108-109.
[30] CRSV Protocol, *supra* note 21, at 89.
[31] *Ibid*.
[32] WITNESS, *Video for Change Guide: Conducting Safe, Effective and Ethical Interviews with Survivors of Sexual and Gender-Based Violence*, available online at https://library.witness.org/product/guide-to-interviewing-survivors-of-sexual-and-gender-based-violence (hereafter *Video for Change Guide*), at 10, 13; Dubberley and Ivens, *supra* note 22, at 10.

recommend asking participants and witnesses to repeat certain information back to investigators, using their own words, to guarantee a certain threshold of comprehension.[33] The World Health Organization has relatedly described the value of a 'consent statement,' in which interview participants are given specific information about exactly why they are being interviewed, the nature of the interview questions, and the precautions being taken by investigators to preserve participant confidentiality, among other things.[34] Yet another article suggests investigators ask participants what the worst-case scenario would be from them providing informed consent, so that the investigator can plan with the participant how to mitigate those risks.[35] Another challenges the practicality of the 'worst-case scenario' approach, especially in documentary contexts.[36] Regardless, if there are any limitations on confidentiality involved in the investigation process, the survivor must have an understanding of those limitations before their consent can be considered informed.[37]

'Voluntariness' requires securing *autonomous* consent, meaning consent free of coercion.[38] In international criminal law, the key question is whether the circumstances, including the environment in which consent is being sought, is coercive.[39] In conflict, there are numerous coercive circumstances that eliminate the ability of a survivor to provide autonomous consent, such as being held captive, the presence of soldiers or weapons, threats of retaliation, the presence of multiple perpetrators, the commission of other crimes, etc. Statements made in such contexts can almost always be considered coercive.[40] However, many of these have little bearing on an online context.

---

[33] See, e.g., CRSV Protocol, *supra* note 21, at 168.

[34] World Health Org., 'Informed Consent Form', available online at https://www.who.int/docs/default-source/documents/ethics/informed-decision-making.pdf; see also World Health Org., 'The Process of Obtaining Informed Consent', available online at https://www.who.int/docs/default-source/ethics/process-seeking-if-printing.pdf?sfvrsn=3fac5edb_4.

[35] *Video for Change Guide*, *supra* note 32, at 10.

[36] S. Gregory, 'Cameras Everywhere: Ubiquitous Video Documentation of Human Rights, New Forms of Video Advocacy, and Considerations of Safety, Security, Dignity and Consent', 2 *Journal of Human Rights Practice* (2010) 191.

[37] CRSV Protocol, *supra* note 21, at 91.

[38] *Ibid*. at 89.

[39] *Prosecutor v. Kunarac et al*., Case No. IT-96-23 & IT-96-23/1-A, Appeals Judgement, 12 June 2002, para. 130 (noting that 'the circumstances giving rise to the instant appeal and that prevail in most cases charged as either war crimes or crimes against humanity will be almost universally coercive. That is to say, true consent will not be possible').

[40] See *Prosecutor v. Bemba*, ICC-01/05-01/08-3343, Judgment pursuant to Article 74 of the Statute, 21 March 2016, paras 102-109; *Prosecutor v. Kunarac*, Case No. IT-96-23-T & IT-96-23/1-T, Trial Judgement, 22 February 2001, paras 645, 667, 711, 761; *Prosecutor v. Delalic et al*., Case No. IT-96-21-T, Trial Judgement, 16 November 16, 1998, paras 960-961; *Prosecution v. Furundzija*, Case No. IT-95-17/1-T, Trial Judgement, 10 December 1998, paras 89,

The World Health Organization has also provided recommendations for researching, documenting, and monitoring CRSV in emergencies and similarly notes that some victims might feel pressure to participate in investigations because they believe they need to do so in order to access services.[41] The World Health Organization emphasizes that investigators must never make unrealistic promises to earn survivors' participation.[42] The survivor must know they can withdraw consent at any point, and investigators must continue to obtain consent throughout the investigation process whenever possible—not merely at the beginning of a process.[43]

Launched by the Institute for International Criminal Investigations (IICI) and several other partners in April 2022, the Global Code of Conduct for Investigating and Documenting Conflict Related Sexual Violence (Murad Code) complements the WHO recommendations and CRSV Protocol by providing minimum standards for the 'safe, effective and ethical gathering and use of victim or survivor information' arising from CRSV.[44] For example, Principle 8.3 acknowledges the application of the Code to 'indirectly sourced information from or about survivors' including information 'in the public domain, in archives or retrievable from online' sources, while Principle 8.4 of the Code advises that practitioners ought to either (1) verify the survivor's consent or (2) mitigate risks and harms arising from sharing the content.[45] While the Code applies to the gathering of information in 'any form [including] digital, written, verbal, audio-visual, [and] photography,' most of its principles are predicated on the gathering of information directly from survivors, including via face-to-face interviews, and is therefore limited in its guidance on online open source content.[46] As a result, the IICI is now partnering with the Human Rights Center at UC Berkeley (including two of the authors of this article) and a circle of advisors to fill the gap by developing guidance that interprets the Murad Code for digital open source investigators. In both documents,

271. See also International Criminal Court, *Elements of Crimes*, Art. 7(1)(g)-1, ICC (2013), available at www.icc-cpi.int/sites/default/files/Publications/Elements-of-Crimes.pdf.

[41] See generally, World Health Org., *WHO ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies* (2007), available online at https://www.who.int/publications/i/item/9789241595681.

[42] *Ibid*. at 22.

[43] *Ibid*. at 24, 28; CRSV Protocol, *supra* note 21, at 183, Annex 7 xxxi; Murad Code, *supra* note 23, at 5; Dubberley and Ivens, *supra* note 22, at 10.

[44] Murad Code, *supra* note 23.

[45] *Ibid.* at 10.

[46] *Ibid*. As this article is going to publication, this gap is being filled by a team of researchers from the Human Rights Center at the University of California, Berkeley School of Law, the Institute for International Criminal Investigations, and a team of advisors and practitioners, who are together drafting a practitioners' guide to the Murad Code for online open source investigators.

survivor control over data is central, as Principle 2.3 of the Code requires the protection of survivors' data in any form (including digital) and that such information not be used or shared without 'express informed consent'.[47]

Like the Murad Code, WITNESS' *Video as Evidence Field Guide* discusses how to properly document human rights violations, but is specific to the use of video footage, whether open *or* closed source. The Field Guide notes that when capturing images related to sexual violence, documenters 'should be sure to obtain fully informed consent … mean[ing] that the survivor comes to wholly understand and agree to the use or sharing of the information they provide and are aware that they can place conditions on the consent or withdraw consent at any point in the process.'[48] However, the guide does not get into detail about when and how that consent should be secured when the content comes from digital open sources.[49]

Ultimately, none of these resources directly tackles the issue of consent to use digital open source information related to CRSV. Thus, the fairly clearcut guidelines that support traditional investigations into CRSV — those that rely on survivor interviews — leave guidance gaps when it comes to investigations conducted online.

B. Consent and Digital Open Source Investigations

The Berkeley Protocol on Digital Open Source Investigations provides minimum standards for ethical Internet-based investigations of international crimes, as well as violations of humanitarian and human rights law. While it offers a general set of principles that apply to all digital open source investigations, it does not provide guidance specific to CRSV. Thus, while guidelines for CRSV investigators leave gaps related to the digital investigations context, conversely, the Berkeley Protocol leaves gaps related to the heightened concerns and considerations that arise with CRSV investigations. However, there are still relevant points that can inform the appropriate handling of CRSV materials: for example, the Berkeley Protocol necessitates that, as part of the investigative process, the use of any personally identifiable information should only be included in 'analytical

[47] *Ibid.* at 4.
[48] Libby McAvoy, *Video as Evidence Field Guide: Using Video to Support Justice and Accountability for Sexual and Gender-Based Violence* (WITNESS 2021), at 26.
[49] Child-victims raise additional considerations that are outside the scope of this paper and deserve their own attention. For information on how to ethically acquire consent from minors, see, e.g., CRSV Protocol, *supra* note 21, at 245-263; WITNESS, *Obtaining Informed Consent*, available online at https://library.witness.org/product/obtaining-informed-consent; Dubberley and Ivens, *supra* note 22, at 22.

work product' with the 'consent of the persons involved.'[50] The Berkeley Protocol also underscores the importance of dignitary considerations of those affected by an investigation, as well as data minimization.[51] Taken together, these three requirements, and the Berkeley Protocol's overarching purpose of minimizing the risk of harm to all involved parties and stakeholders, can be inferred to require a careful handling of particularly sensitive content, such as CRSV-related data.[52] Our observations below are designed to expand upon those considerations with regards to investigations that may inadvertently or deliberately surface digital content relevant to CRSV.

4. Merging Worlds: Considerations for Seeking Consent

In this section, we propose an approach to securing consent to use digital open source information of CRSV that prioritizes survivors' interests while acknowledging the challenges with seeking consent in digital contexts. We identify multiple variables that should go into any calculation of whether consent is needed and from whom, who should seek that consent, how the consent should be secured, and when. Those variables are summarized in the table below.

individual who recorded the content	**individual who posted the content**	**individual(s) depicted in the content**	**intended use of the content**	**nature of the content**
victim	victim	victim	linkage evidence	explicit (depicts CRSV)
perpetrator	perpetrator	perpetrator	base crime evidence	implicit (suggests CRSV)
observer/ bystander	observer/ bystander	observer/ bystander	lead information	contextual (indicates *who* was present, *what* happened, or *where* it occurred, etc., but does not document the CRSV itself)

Typology of variables that may be relevant to consent considerations

Combining these fifteen variables results in an impressive array of scenarios, each of which may require a different approach to seeking consent. For example, the consent considerations may be very different for perpetrator footage used as lead information than for bystander footage that illuminates the base crime. Below we discuss the steps that investigators should take when

[50] *Berkeley Protocol*, *supra* note 5, at 65-66.
[51] *Ibid*. at 13-14.
[52] *Ibid*. at 11.

developing an ethical plan for seeking and securing consent. The steps are not provided in any particular order; an appropriate sequencing will vary depending on the information available and other contextual considerations.

A. Identify Whose *Consent Should be Sought*

As noted above, when interviewing survivors, the person whose consent should be sought is often relatively straightforward. In the digital context — for example when viewing a video that could serve as evidence — there may be multiple people whose consent is relevant. While victims' needs and interests should always be prioritized, there are several key actors involved in the creation, dissemination and collection of any piece of digital open-source information. Individuals whose interests should be acknowledged, in addition to the service provider who hosts the content and any relevant government agency that regulates online content, include the following:

(1) Victim(s): anybody depicted in the content as being harmed
(2) Perpetrator(s): anybody depicted in the content as harming others
(3) Observer(s): anybody depicted in the content who is not the victim or perpetrator (e.g., a bystander, first responder, documenter, etc.)
(4) Content recorder: whoever recorded the video, photograph or other content (can also be a victim, perpetrator, or observer)
(5) Content poster: whoever posted the video or photograph online (this person could also be a victim, perpetrator, content recorder or observer)

The consent required of any individual ultimately depends on their relationship to the content, the nature of the content, and how the information will be used. For example, how does the need to secure consent differ if it is the victim who shares the content, versus if it is a bystander or a perpetrator, given what is stated or might be inferred about the desire to share the information publicly? While it is inadvisable to infer consent to use videos and photos posted to social media, the risks may be lower when the poster is a victim who appears to be trying to bring attention to the crimes perpetrated against them than when the poster is an alleged perpetrator trying to boast about their exploits, or a bystander who may not have thought about the physical or psychological risks to a survivor, or may be prioritizing the needs of their community over the interests of the victim.

Observers share many of the privacy and safety concerns of victims, particularly if the observer is identifiable or is recorded engaging in behavior that is illegal or stigmatized, such as attending a protest, not wearing culturally or legally required clothing (such as not wearing a hijab in a region

that mandates the hijab), wearing coded articles of clothing (such as symbolic masks, patches or pins), being a non-married woman in the company of non-related men in a culture where that is frowned upon, and so on. This article's consent considerations are therefore largely the same for observers as for victims, with potential exceptions for observers who are law enforcement, public officials, or individuals who may be considered co-perpetrators.[53]

If a bystander posts a video showing a victim being sexually assaulted, and an investigator wants to use the video, then securing the victim's consent to use the video for those purposes is of paramount importance. Using the video as evidence in court, or posting the video without the victim's consent, could potentially be an additional assault to the victim's dignity. In addition, the violent nature of the video could carry a high risk of re-traumatization if the victim (or those close to them, or even other survivors of CRSV) were to watch it unexpectedly or to learn of its use or even existence secondhand (there is also, of course, the risk of secondary trauma to observers). Any cultural stigma attached to such an assault would further increase the risk to the victim's wellbeing.

On the other hand, if a perpetrator were to share a video of themself bragging about an assault with their friends, a criminal investigator seeking justice for the victim would not necessarily need to ask the perpetrator for their consent before saving the post for investigation and potential prosecution purposes. However, even in this hypothetical, there could be a risk of retaliation against the perpetrator or their family or community if they were identifiable in the video, and thus the video should not be shared with anyone who does not need access.[54]

The diversity of potentially affected parties further complicates the issue of whose consent should be sought. Victims, bystanders, and other stakeholders may have conflicting desires and/or interests, further complicating next steps. Social media platforms' interests reside at the intersection of privacy and intellectual property interests. For example, the person who created a social media post may have an ownership interest in that post; thus, companies require that when users post information to social media, they are consenting to its publication. Meanwhile,

[53] Dubberley and Ivens, *supra* note 22, discusses people who interact with open-source information on the host website, such as commenting on or 'liking' posts. Although an in-depth discussion of the consent implications of after-the-fact content-observers is beyond the scope of this article, these individuals' privacy should be respected wherever possible, including by censoring the names and identifying information (such as profile pictures) of commenters. See *ibid*. at 27 for a brief discussion on consent under this human-rights based approach.

[54] For examples where videos related to alleged international crimes were freely shared within investigative teams see Koenig and Egan, *supra* note 7.

investigators are primarily concerned with consent as it relates to the dignity interests of those depicted. The content recorder's or poster's status as a victim, perpetrator, or observer is therefore more important for determining whose consent is needed than their ownership over the content. For example, it is critically important for investigators and others to secure the victim's informed consent before publicly posting information related to their sexual assault (for example, if trying to build momentum for future accountability)[55] while it may be antithetical to the interests of justice for an investigator to seek the perpetrator's consent before using such a video as evidence in a criminal prosecution. Such examples are fairly common sense. More complicated, however, is the issue of consent as it relates to the other possible combinations of the identity of the content recorder or poster, the individuals depicted in the content, the intended use of the content, the investigator's role in the case, and the nature of the information depicted.

B. Identify Whether the Context *Requires Consent*

Context could ultimately be broken down into a series of factors: the desired use of the data, the risks faced by those who could potentially be affected by that use, and whether that use would be external or internal facing, public or private.

Consent is especially needed whenever an individual could be placed at risk of harm due to public-facing or quasi-public uses. Investigators should evaluate the physical, digital, psychosocial, economic, reputational and other risks that could result from requesting consent to use content in furtherance of the investigation.[56]

Generally, a depicted party includes all those whose identities are discernible in a piece of open-source media. In the context of sexual violence, a piece of content might include the victim before, during or following an act of violence. Because victims of sexual violence always have a privacy

[55] See e.g. the backlash that arose when a reporter reprinted the video of a rape. The journalist's intent had been to crowdsource information that may lead to the arrest of the perpetrator(s), but the re-posting of the video was heatedly criticized for potentially magnifying the victim's trauma. See e.g. K. Hill, 'This Week in Horrible Journalism: Jezebel's Rape Photos', *Forbes*, 10 February 2012, available online at www.forbes.com/sites/kashmirhill/2012/02/10/this-week-in-horrible-journalism-jezebels-rape-photos/?sh=69d674c42597 (criticizing A. North, 'Did Libyan Video of a Journalist's Rape Get Posted on YouTube?', *Jezebel*, 8 February 2012, formerly available online at https://jezebel.com/did-libyan-video-of-a-journalists-rape-get-posted-on-yo-5883491).

[56] While beyond the scope of this paper, using sensitive content in investigation may also create risks for the content recorder or uploader. For more on the safety considerations when conducting open-source investigations, see *Berkeley Protocol*, *supra* note 5, at 31-41.

interest at stake in the use or publicization of media depicting their traumatic experiences, the interests of the victim in sexual violence cases are always non-zero.

Investigators must consider whether the proposed/desired use of open-source material could have a negative impact on the content poster, the victim, or any implicated non-aggressor third parties, including observers and the victim's family members.[57] Harm may include not only threats to life or physical safety but also threats to social standing, familial relationships, psychological wellbeing, or economic prospects. These risks may be relatively minimal for the collection and preservation of the data, or if the data is used as a lead to other categories of evidence, but more acute if introduced in court, or in a public-facing document that summarizes the case or context. Considerations for evaluating the risks may include but are not limited to the probable or possible reaction from the community, the scale and severity of that reaction, potential threats of further physical violence against the party, potential negative consequences for the party's family and loved ones, potential intrusions from the media or the public in the course of investigatory or judicial processes and, finally, the dignity of the party. Assessing the risk to the dignity of the party necessarily requires an examination of the nature of the content in question. We have differentiated the nature of that content as *explicit* (depicting sexual violence), *implicit* (suggesting the occurrence of sexual violence), or *contextual* (indicating the 'who,' 'what,' and 'where,' but not depicting or suggesting the violence itself).

In considering these factors, investigators ought to also determine, to the extent possible, both the most likely and the worst possible outcomes of using the explicit or contextual material with or without acquiring the party's consent, as contextualized by the cultural and religious norms of the depicted party and their community. Because evaluating risk may be difficult, practitioners should err on the side of overestimating the safety interest when considering the worst possible outcomes for the subject.

Oftentimes, open-source investigators use indirect identifiers such as abbreviations or pseudonyms to protect victims' identities. However, this approach can be insufficient to protect those whose experiences, characteristics, or attributes are relatively unique, such as when they are

[57] Title I, Art. 1 EU Charter of Fundamental Rights ('Human dignity is inviolable. It must be respected and protected'); Universal Declaration of Human Rights, G.A. Res. 217A (10 December 1948); G. Le Moli, *Human Dignity in International Law* (Cambridge University Press, 2021).

the only remaining member of a specifically targeted ethnic or religious group in a region or when their physical identity is captured in a video or photograph.

To account for this, investigators ought to minimize, to the extent possible, the further sharing of sensitive information, and should notify individuals about the safeguards they intend to deploy, when initially requesting consent. In accordance with the University of Michigan's Inter-university Consortium for Political and Social Research's (ICPSR) recommendations, such notifications should be descriptive and explicitly state which information will not be shared.[58] The ICPSR suggests that investigators and other researchers expressly inform individuals that 'any personal information that could identify [them] will be removed or changed before files are shared with other researchers or results are made public,' and that '[their] answers to the questions . . . will be anonymous'.[59] While the law may require that an individual's name be attached to sensitive information for use in criminal trials, investigators pursuing other, non-legal accountability efforts should make clear to the individual that their answers will remain anonymous to the extent possible, while acknowledging that it is increasingly possible to de-anonymize even anonymized parties given the 'mosaic effect' — the ability to piece together clues from online (and sometimes offline) sources to uncover protected information.[60] Ultimately, what is most important is honesty and transparency around the data's use, and continuing notification about what is happening with a case, as security permits.

Specific consent is also needed when content is acquired from social media platforms even though the poster has theoretically affirmed that anyone featured in their content has consented to the act of posting. Terms of service for the social media platforms where open-source material is often discovered, such as Facebook, X/Twitter, Telegram and TikTok, put the onus on the user to ensure that all individuals featured in the content have consented to have the content posted. Although most social media companies prohibit posting content of someone without their consent, there are few accountability measures to ensure that these guidelines are followed[61] and norms

[58] Inter-University Consortium for Political and Social Research, 'Recommended Informed Consent Language for Data Sharing', University of Michigan, available online at www.icpsr.umich.edu/web/pages/datamanagement/confidentiality/conf-language.html (hereafter *ICPSR Recommendations*).
[59] *Ibid*.
[60] See *Berkeley Protocol*, *supra* note 5, at 12 n. 26.
[61] Facebook, YouTube, and X all include provisions in their Terms of Service either prohibiting users from posting content of others without their consent or asking them not to. See 'Terms of Service, Part (3)(2)', Facebook, available online at www.facebook.com/legal/terms ('You may not use our Products to do or share anything … [t]hat you do not own or have the necessary rights to share'); 'Terms of Service', YouTube, available online at

vary widely between individuals and communities. In addition, such provisions are predominately designed to protect the companies from liability, as opposed to ensuring individual control over what is and is not posted, and what is removed.

The majority of social media accountability mechanisms rely on a non-consenting individual to report the offending content to the company, and then go through a process to have that content removed—something that may be difficult if not impossible for those embroiled in a war, incapacitated due to injury, or without access to the internet, among other scenarios. Therefore, even when consent may be implied, investigators should be aware of the flawed nature of this implied consent, particularly for vulnerable individuals and groups. Even where consent to post was *expressly* indicated, the poster may not be the victim, and thus the victim's interests haven't been expressed; in addition, consent for the initial posting is not necessarily continuous, nor does it automatically extend to the use of the content in an investigation. Therefore, investigators must not rely on these initial, potentially faulty indicators of consent, whether explicit or implied.

The considerations also differ if the content is used or intended to be used merely as lead information, versus as linkage or base (primary) evidence. Will an investigator use the video or photograph to identify who might be available to serve as a witness, or indicate what physical evidence might exit? Does an image potentially lead to additional documentary or digital evidence, for example by showing the remnants of a munition, or because others who are visible appear to be recording the event? Although most investigators would not seek consent before using a social media post to secure leads to other types of evidence (such as physical evidence depicted in a video, or documents that may be visible), given the minimal risks to the victims, this may not be best practice if the video is used, for example, to reach out to potential witnesses present in the image. Reaching out may raise new risks for various stakeholders, including the victim.

What the investigator can do is scan the post and relevant contextual information for evidence of heightened risks in order to help them identify appropriate ways to minimize risks, should they reach out. For instance, the poster may have used a specialized code in the caption of the post to mask the location of the video (e.g., of an LGBTQ-friendly space in a country that prohibits such

www.youtube.com/static?template=terms ('Permissions and Restrictions: the Content you submit must not include third-party intellectual property (such as copyrighted material) unless you have permission from that party or otherwise legally entitled to do so'); 'Terms of Service', Twitter, available online at https://x.com/en/tos ('We reserve the right to remove Content that violates the User Agreement, including for example, copyright or trademark violations or other intellectual property misappropriation, impersonation, unlawful conduct, or harassment'). Users can use privacy settings to control how people can find them or can report offending content to the platforms.

gatherings) to protect the identity of depicted bystanders. Careful consideration of the visual, textual or auditory strategies employed by the poster can ultimately reveal whether any attempt to procure consent from any depicted party, bystander or otherwise, would create some heightened risk of harm.

Finally, the nature of the content itself may inform whether, when, by whom, and in what way consent should be sought. As noted above, the media may be *explicit*, such as when a sexual assault is recorded on video, *implicit*, such as when the content suggests the occurrence of a rape by capturing the sound of a victim's screaming or other indicators of sexual violence,[62] and finally, *contextual*, such as when the content depicts children or pregnant women held in captivity, suggesting the possibility of sexual slavery or a related crime, but not depicting the sexual violence itself. An inquiry into the nature of the content can, and often should, go further than is linguistically encompassed by these categories, and may consider the type of digital media involved (photo, video, or audio recording) to determine the nature of the content, or the time elapsed since its creation.

Given these variables, we recommend that the person who is weighing whether to reach out to a possible victim to secure consent assess whether the victim can be reached; the possible risks to the victim, their families and communities that could result from reaching out; whether additional risks would be created through that attempt; and whether those risks can be mitigated.

C. Identify Who *Should Seek the Consent*

Another significant issue is *who* should seek that consent—and when. It's important to assess where along the workflow the investigator sits, and whether given their position or expertise they are the best person to reach out. For example, if the digital open source investigator is working for an independent organization and is voluntarily providing information to an external legal team, they may not be the appropriate interface; perhaps the lawyer in charge of case building is better positioned to know what digital open source information may be especially critical to their case and to explain how that content might be used. The lawyer may also be in a better position to determine whether the item is potentially useful as evidence and thus whether the victim should

[62] See e.g. H. Bagdasar, 'Recognising Sexual and Gender-Based Violence as an Open Source Researcher', *Bellingcat*, 3 March 2023, available online at www.bellingcat.com/resources/2023/03/03/sexual-and-gender-based-violence-open-source-researche-osint-digital (discussing indicators of violence).

be approached. They may also have additional training and experience in working with sexual violence survivors, further ensuring that any contact is as victim-centered as possible.

If the investigator *is* the most appropriate person to reach out, they should make sure they have the appropriate expertise to communicate in a trauma-informed manner (that is, that they are an expert in working with sexual violence survivors). Investigators should conduct any consent discussions in the individual's preferred language, avoiding legal terminology whenever possible and following best practices for interacting with CRSV survivors. If legal terms are necessary, the investigator should provide the individual with a full explanation of what those terms mean, as consistent with existing protocols.

D. Identify How *to Seek the Consent*

Once consent will be sought, *how* should that consent be sought and what form should it take? As explained above, best practices suggest that consent should be explicit,[63] voluntary,[64] specific,[65] informed, and continuous[66] and all procedures should be designed to further those requirements. Each element should be considered as necessary but not sufficient. In addition, a greater presence of one should not excuse the absence of another.

Thus, whoever seeks the consent should place special consideration to what information survivors need to determine the consequences or the potential consequences of their possible involvement. Ideally, investigators should convey:

a. How the information will be used, both in the short and long terms;
b. The potential positive and negative implications of using this information in an investigation (without setting unrealistic expectations);
c. Potential legal obligations to be imposed if the case goes to trial;
d. The procedures in place for safeguarding the underlying data;
e. Who will have access to the information; and
f. Any perceived safety risks to the individual, their family, or their community, both short and long term.[67]

[63] Silence is not consent; a grant of consent must be clear and unambiguous.
[64] Freely given as opposed to coerced. This includes ensuring that the individual has the legal ability to grant consent given to their age and mental acuity (including capacity and sobriety).
[65] Limited to the particular source of information (e.g., video, picture, tweet, etc.), incident of CRSV, and investigation or prosecution.
[66] Consent can be withdrawn at any time, particularly as new information comes to light about repercussions or the use of the information. However, practical complications with obtaining consent in a wartime context, for example, make it difficult if not impossible for investigators to check in with victims to confirm continued consent. For this reason, investigators should attempt to make their initial conversation about consent as comprehensive as possible.
[67] CRSV Protocol, *supra* note 21, at 90 (noting that informed consent involves consenting to all aspects of documentation).

The person seeking consent (whether an investigator, lawyer, or otherwise) should aim to obtain consent in the safest manner possible.[68] For example, investigators should avoid asking for consent to use digital open source information over social media, and should never solicit consent through a public social media post (for example, in a reply to posted content).[69] Although a direct message is considerably safer than a public comment, it is possible that perpetrators (particularly of intimate-partner violence), family members, or others may have access to the victim's social media and other electronic accounts.

Although there is, of course, a distinction between investigators on the ground and investigators conducting their searches online, open-source investigators must still adhere to the general principles of investigators. These include considering how well an investigator is known in the community, not asking members of the community for help being put in contact with victims, credibly identifying oneself as an investigator so a victim can verify their identity and legitimacy, establishing trust, ensuring all translators establish trust, and so on.[70] At a minimum, consent should be documented in written or audio format to protect both investigators and survivors from downstream social or legal issues.

E. Scope of Consent

Even if consent can be obtained in accordance with the recommendations discussed above, safety and privacy concerns may arise during the later parts of an investigation, particularly when sensitive information is shared with other investigators, or the results of the investigation are introduced in court or ever published publicly. So what, ultimately, is the temporal and substantive scope of consent?

---

[68] See Koenig and Egan, *supra* note 7 at 55, 78 ('Discussions of privacy also invoked multiple references to the need for data greater anonymization, controlled and secure storage, and team management').

[69] Many journalists, for example, will seek consent to use a video, photo or other item posted to social media by commenting on the post.

[70] See, e.g., UN OHCHR, *Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice* (2015), at 33-35 (establishing '[p]rinciples of human rights and international humanitarian law fact-finding and investigations'); *ibid*. at 49-52 (describing information-gathering methods, including best practices for interviewing); *ibid*. at 74-82 (emphasizing and providing guidance for the '[p]rotection of victims, witnesses, sources, and other cooperating persons', including guiding principles, security risk assessment, preventive measures, protection of information, and responding to allegations of threats or reprisals).

The ICPSR suggests that researchers provide clear information about how they will protect personally identifying information.[71] Of course, victims may rescind consent while an investigation is ongoing. In addition, if the material is needed for another use than that for which consent was originally sought, then further consent should be obtained.

Some practitioners may argue that consent is no longer relevant after a case concludes. However, responsible data management requires that investigators account for the data's lifecycle, including when legally or ethically such data must or should be destroyed.

Finally, if there has been a significant intended change to the initial scope of use, the victim should be contacted as soon as possible and informed of the intended change and should be asked whether they consent to that expanded use. If consent is later restricted or rescinded, investigators should adhere to the survivor's direction.

5. Conclusion

The concept of consent is a longstanding feature of international law. However, given the ethics lag related to digital open-source investigations, and the heightened importance of securing victim consent when investigating and prosecuting CRSV, it's critical that investigators pay particular attention to the when, why, how, and by whom consent should be secured when working with online information. The importance of each of the elements of explicit, voluntary, specific, informed, and continuous consent is significant.

Ultimately, victim consent must be prioritized in digital open source investigations to avoid re-traumatization, ensure sound investigatory practices, and promote effective evidence gathering. The authors hope that this article sparks conversation in the digital investigations community, and that future research will expand on and refine our recommendations in ways that increasingly protect survivors' interests.

There is a cruel irony that increasing hurdles to gathering evidence of CRSV — including an obligation to secure consent to use digital open source information — could make investigations and prosecutions of such crimes even more difficult. And yet, the more that victims trust practitioners to respect their wishes, and the more that practitioners return control to those from whom such control has been stolen, the more likely victims are to provide their consent. In this way, our proposed approach will hopefully serve the dual aims of prioritizing victim autonomy

[71] ICPSR Recommendations, *supra* note 58.

and increasing trust in investigators to act in victims' best interests where that trust is deserved, ultimately strengthening pathways to justice.

ACKNOWLEDGEMENTS

The authors are grateful to the Oak Foundation for its financial support of the Human Rights Center at U.C. Berkeley, which made this research possible. The authors also thank Hayley Durudogan, Malak Afaneh, Justine DeSilva, Pascal Jakowec, Ishita Mattoo, Melina Rezai, Nicole Waddick, and Jane Yang for their research contributions to this article; Ulic Egan and Libby McAvoy for their comments on earlier drafts; Andrea Richardson and Hannah Bagdasar for being helpful thought partners on issues involving digital open source investigations and SGBV; and several anonymous reviewers for their feedback. Any errors are, of course, the authors' own.