GENEVA ACADEMY
Académie de droit international humanitaire et de droits humains
Academy of International Humanitarian Law and Human Rights

INPUT FOR A THEMATIC STUDY ON *NEW TECHNOLOGIES AND ENFORCED DISAPPEARANCES*

WORKING GROUP ON ENFORCED OR INVOLUNTARY DISAPPEARANCES

Introduction

The Geneva Academy of International Humanitarian Law and Human Rights is pleased to submit this input to the Working Group on Enforced or Involuntary Disappearances (WGEID), with a view to informing the latter's Thematic study on *New Technologies and Enforced Disappearances*.

The submission has been prepared in the framework of the Geneva Academy's **IHL Expert Pool**, a response mechanism that works to deliver technical assistance, capacity development and legal opinion on topical IHL issues for users within the human rights community of practice. Launched in 2022, this project works to strengthen the capacity of human rights mechanisms to incorporate IHL into their work in an efficacious and comprehensive manner, by organizing and facilitating the provision of expert advice.

The submission has been prepared by **Edward Millett**, graduate (*summa cum laude*) of the LL.M. course in IHL and Human Rights at the Geneva Academy, and by **Dr Francesco Romani**, Research Fellow at the Geneva Academy in charge of the IHL Expert Pool.[1] Their findings build, *inter alia*, on an experts' consultation on *Strengthening Accountability at the Intersection of Law, Technology, and the Humanitarian Space*, which took place under the aegis of the Geneva Academy in December 2022.

[1] [redacted]

1. Open source information: a double-edged sword?

This submission focuses on **the benefits and the risks** that open source information (OSI) poses in relation to enforced or involuntary disappearances (EIDs). First, it assesses the value of OSI for the different purposes of *searching for* the disappeared and *holding the perpetrators to account*. Second, it offers three case-studies from recent practice where OSI has been deployed in an armed-conflict setting, in order to highlight that the use of OSI often entails balancing competing rights and obligations (e.g. the right to know vs the right to privacy), and unless properly risk-assessed can in turn lead to unintended rights violations. Finally, the submission concludes with a set of recommendations.

According to the *Berkeley Protocol* – a leading soft-law framework for open-source investigations aimed at civil-society users – OSI 'encompasses publicly available information that any member of the public can observe, purchase or request without requiring special legal status or unauthorized access'.[2] Although OSI in itself is not a new phenomenon,[3] digital OSI has proliferated in recent decades, particularly 'content posted on social media; documents, images, videos and audio recordings on websites and information-sharing platforms; satellite imagery; and government-published data'.[4] Moreover, open-source investigatory activities go beyond the initial stage of collecting data and information, rather comprising a complete information 'operations cycle' that comprises data-processing, retention, exploitation and reproduction.[5]

Stepping back, international law provides a fairly robust framework that protects persons against disappearances (especially enforced ones) both in peace-time and in situations of armed conflict.[6] Applicable norms result from the interplay of several sources that can be found in international human rights law, international humanitarian law and international criminal law, and that comprise of multilateral conventions, customary norms and soft-law standards.[7] The obligation to *prevent people from going missing* is thus complemented by the State's *obligation to clarify* (and the corresponding families' right to know) the fate and whereabouts of missing persons.[8] However,

---

[2] UC Berkeley School of Law's Human Rights Centre and OHCHR, *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*, New York and Geneva 2022, para. 14 (available at: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf).

[3] The notion can include mass-media, specialised journals, photography, conference proceedings and think-tank studies.

[4] *Berkeley Protocol*, para. 1.

5 Geiß and Lahmann, 'Protection of Data in Armed Conflict', 97 *International Law Studies* (2021), p. 562; Williams and Blum, 'Defining Second Generation Open Source Intelligence (OSINT) for the Defence Enterprise', RAND Corporation (2018), p. 13; c.f. Böhm and Lolagar, 'Open source intelligence: Introduction, legal and ethical considerations', 2 *International Cybersecurity Law Review* (2021), pp. 320-1.

[6] Londono and Ortiz Signoret, 'Implementing International Law: An Avenue for Preventing Disappearances, Resolving Cases of Missing Persons and Addressing the Needs of Their Families', 99(2) *IRRC* (2017), p. 551.

[7] For an overview of these sources, see ICRC, 'Missing persons and their families', December 2015, available at: https://www.icrc.org/en/document/missing-persons-and-their-families-factsheet.

[8] *Ibid*.

although OSI is being increasingly relied upon to investigate violations of international law,[9] its potential value – and possible drawbacks – have not been fully assessed in depth in relation to EIDs. This is especially the case when looking beyond EID accountability at other aspects, such as deployment of OSI in the search for the disappeared, and its use for harmful purposes.

Against this complex backdrop of overlapping regimes and norms, OSI represents a double-edged sword. As a tool and a method, it could be used both to breach and to comply with international obligations applicable in the field of EIDs. In theory, information that is publicly available can be used to identify targets and subject them to enforced disappearances, just as much as it could be harnessed to increase the likelihood of finding missing persons and holding those responsible of enforced disappearances accountable. These usages are not mutually exclusive, insofar as different actors could employ OSI at different stages (and for different purposes) of the disappearance process. What is more, and as will be seen in greater detail below, without proper mitigation strategies nothing precludes an originally "well-intended" use of OSI (e.g. posting information to put the spotlight on an episode of enforced disappearance) from creating harmful consequences on a wide set of actors (e.g. by endangering relatives and representatives of disappeared persons).

2. Addressing enforced disappearances through OSI

A. The "hidden" conduct problem and the need for "aggregated" OSI

Critical analysis of the impact of OSI on the field of enforced disappearances has to date been fairly limited. This is likely a result of the oft-lamented reality whereby "hidden" atrocities are particularly challenging to track and tackle – even with the increased tools provided by OSI.[10] Enforced disappearances fall in this category because one of their constituent elements is the 'refusal to acknowledge the deprivation of liberty or [the] concealment of the fate or whereabouts of the disappeared person, which place such a person outside the protection of the law'.[11] However, the particularities of EIDs in criminal and human rights law should not be seen as total bar to the relevance of OSI; rather, it calls for a more fine-grained approach to the use of OSI in this context.

In recent years, OSI has been successfully employed in investigations in armed-conflict settings with an EIDs dimension. In 2017, Forensic Architecture (FA) contributed to a report by Amnesty International that covered, among other things, incommunicado and secret detention in the non-

[9] To name but a few, recent examples, see: Report of the Independent Investigative Mechanism for Myanmar, A/HRC/48/18, 5 July 2021, paras. 16-17; ICC, *The Prosecutor v. Ahmad Al Faqi Al Mahdi*, Judgment and Sentence, ICC-01/12-01/15-171, Trial Chamber, 26 September 2016, paras. 31-41; ECtHR, *Ukraine and The Netherlands v. Russia*, Decision, 25 January 2023, para. 472.

[10] McDermott, Koenig and Murray, 'Open Source Information's Blind Spot. Human and Machine Bias in International Criminal Investigations', 19 *Journal of International Criminal Justice* (2021), p. 95.

[11] Art. 2 International Convention for the Protection of All Persons from Enforced Disappearance (2006) [ICCPED]. See also Art. 1(2) of the UN Declaration on Enforced Disappearance (1992), and Art. 7(2)(i) of the Rome Statute (1998) [ICC Statute].

international armed conflict between Boko Haram and the Cameroonian security forces.[12] Through the use of satellite imagery, open-source material, and images gathered from social media, FA demonstrated the proximity of U.S. personnel to one of the sites, leading the U.S. military to conduct an inquiry into the allegations at the request of the leader of U.S. Africa Command.[13] In November 2022, the Humanitarian Research Lab (HRL) within Yale School of Public Health released a report on extrajudicial detentions and enforced disappearances that occurred in Kherson Oblast, Ukraine, between March and October 2022, during the armed conflict between the Russian Federation and Ukraine.[14] The report 'combines open source data analysis of individual accounts of detentions and disappearances with open source and satellite imagery analysis of the detention locations implicated in those accounts'.[15] The HRL report does acknowledge the limitations of its open source analysis[16] and stresses repeatedly that the allegations therein would represent violations of IHL and IHRL only if confirmed by a qualified body.[17] However, its analysis highlights the value of OSI in identifying, investigating and verifying both individuals and locations associated with alleged violations.[18]

These examples show how the peculiarities of enforced disappearance call for an "aggregated" application of OSI tools, each of them targeting a specific element of the definition of the conduct. The "hidden" character of EID conduct, as well as the presence of a specific mental element in the criminal definition makes it unlikely that OSI will provide single-handedly all the material qualifying a specific conduct as an enforced disappearance.[19] Yet, it could offer useful indications on the identity of the victim, the act of depriving liberty, the location of the detention, the identity and the affiliation of the perpetrator. Even when enforced disappearance of persons represents one of the physical elements in the commission of crimes against humanity, OSI could be used to document the contextual element of the crime – i.e., the presence of an attack directed against a civilian population, its widespread or systematic character, and the commission of the act as part of the attack.[20]

B. Beyond criminal accountability: OSI and humanitarian tools to facilitate search

One key issue that is often mentioned as a practical hurdle preventing OSI's full potential as an evidence-source being realised is its admissibility in criminal proceedings. Yet, even in this regard the specific characters of EID could prompt us to look at this problem from another angle. First, OSI-based evidence and analysis can be used for political advocacy purposes, such as initiating

[12] Amnesty International, *Cameroon's Secret Torture Chambers: Human Rights Violations and War Crimes in the Fight against Boko Haram*, 20 July 2017, available at: https://www.amnesty.org/en/documents/afr17/6536/2017/en/.
[13] Forensic Architecture, 'Torture and Detention in Cameroon', available at: https://forensic-architecture.org/investigation/torture-and-detention-in-cameroon.
[14] Humanitarian Research Lab, 'Extrajudicial Detentions and Enforced Disappearances in Kherson Oblast', 18 November 2022, available at: https://hub.conflictobservatory.org/portal/apps/sites/#/home/pages/kherson-1.
[15] *Ibid*., p. 9.
[16] *Ibid*., pp. 33-34, 47 and 50-51.
[17] *Ibid*., pp. 6 and 23.
[18] *Ibid*., pp. 44-47.
[19] Art. 7(2)(i) ICC Statute: 'the intention of removing them from the protection of the law for a prolonged period of time'.
[20] *Ibid*., Art. 7(1)(i); see also Art. 5 ICCPED.

reviews and investigations, even where they do not meet admissibility requirements for criminal prosecutions. Second, such evidence may still meet less stringent standards of proof, such as the "reasonable grounds to believe" standard used by United Nations fact-finding bodies, or contribute to establishing State responsibility according to the terms set forth in international instruments.[21] Finally, OSI can contribute to procedures of a humanitarian and extra-judicial character that are focused on clarifying the fate and whereabouts of the disappeared, beyond and in addition to criminal prosecution.[22]

This latter dimension can clearly be seen in the recent State practice of Colombia. In 2006, the Constitutional Court of Colombia interpreted the obligation to provide information on the fate of disappeared persons as a requirement for the collective demobilisation of groups organised outside the law. The Court stated that the obligation to reveal the whereabouts of the disappeared, or in any case to collaborate with the justice system to find them, could not be voluntarily postponed by the State until the final judgement of the criminal trial.[23] Measures adopted in recent years to implement and follow up on the *Final Agreement* between the Government of Colombia and FARC-EP further elucidate the complementary nature of humanitarian efforts to establish the fate and whereabouts of disappeared persons, on one hand, and criminal procedures to identify and punish perpetrators, on the other.[24] For instance, the *Decreto Ley* 589 (2017), which established the 'Unit for the search for persons reported missing in the context and due to the armed conflict' (UBPD) points to the potential role of OSI in collecting all the information necessary to search for, locate and identify persons reported missing in the context of and as a result of the armed conflict. This is especially the case for those articles in the *Decreto Ley* that allow the UBPD (i) to request and receive information from persons, State entities, social and victims' organisations, including that which is of an official nature and which is contained in databases,[25] and (ii) to enter into contracts, agreements and/or protocols for access to information with any type of national or international organisation under public or private law, including national or foreign victims' and human rights organisations.[26] The Constitutional Court of Colombia has highlighted how 'the opportunity to benefit from the largest possible number of documents […] is vital for [the UBPD] to obtain the results expected of it',[27] and the all-comprehensive language used in the *Decreto Ley* does not appear to preclude the UBPD from using OSI to carry out its mandate.

[21] See Report of the Group of Eminent International and Regional Experts on Yemen, A/HRC/42/17, 9 August 2019, para. 5; see also Wilkinson, *Standards of Proof in International Humanitarian and Human Rights Fact-Finding and Inquiry Missions*, Geneva Academy Report, 2014.
[22] See the intervention by the Head of the ICRC delegation to Colombia reproduced in: Colombia, Constitutional Court, Sentencia C-067 (2018), para. 3.6.
[23] Colombia, Constitutional Court, Sentencia C-370 (2006), paras. 6.2.2.2.1-6.2.2.2.11.
[24] Final Agreement to End the Armed Conflict and Build a Stable and Lasting Peace, 24 November 2016.
[25] Colombia, *Decreto Ley* 589 (2017), Art. 5(1)(b).
[26] *Ibid*., Art. 14.
[27] Colombia, Constitutional Court, Sentencia C-067 (2018), para. 9.4 – Análisis - (viii). Both Art. 5 and Art. 14 of the Decreto Ley 589 (2017) have been considered in conformity with the Constitution of Colombia with regard to the specific aspects recalled here: *ibid*.., paras. 3 and 9 of the Decisión.

3. Examples of uses of OSI: obstacles and challenges

A. Challenges: unintended consequences and the need to balance competing rights

The previous section has highlighted the role that OSI can play under several respects in relation to enforced disappearances, particularly in situations of armed conflict. However, one of the significant challenges to deploying OSI capabilities in such settings is the risk of unintended consequences arising, for example: interfering with the privacy rights of individual civilians and communities, risking the exposure of civilians' identities to hostile actors, or pre-emptively presuming criminal liability of suspects.

Accordingly, in conducting OSI operations, the *Berkeley Protocol* calls on investigators to respect the right to privacy, but only on the limited basis that violations may result in evidence being excluded from criminal proceedings: the Protocol therefore points to potential rights violations arising from OSI operations but does not consider this aspect in depth.[28] In the field of enforced disappearance, the concerns are broader since the challenge for actors using OSI is invariably to balance competing obligations: between the goals of the investigation (e.g. the right to truth, positive obligations incumbent on state actors to investigate death/disappearances) and the need to safeguard the rights of individuals and communities (e.g. the right to privacy, data protection). This is particularly the case where State actors use OSI, given their extensive obligations under IHL and international human rights law. The following case studies explore these tensions in greater detail. While they do not focus directly on EIDs, they deal with violations of international law in the context of armed-conflict and conflict-affected settings where OSI has been deployed either to mitigate or to facilitate such violations. In this way, they provide invaluable practical context for future deployments of OSI to tackle EIDs, highlighting some of the legal and operational issues that may arise.

B. The *Sentinel Satellite Project (SSP)*

The SSP, launched in 2011, was a pioneering early effort to use OSI as part of a large-scale early-warning system to mitigate conflict in Sudan and South Sudan, including by using OSI to predict flare-ups in violence. It provides a useful example of how the deploying team had to grapple with follow-on risks from the project while it was underway, including Demographically Identifiable Data-based (DII) risks.

The SSP used remote-sensing data gathered from satellite imagery, along with other non-image data sources, which were geo-tagged, parsed, and layered into a multi-stream dataset. Information gathered included location data, population movement patterns, size and status of civilian population and armed actor groups, while largely avoiding the need for the collection of

28 *Berkeley Protocol*, para. 62.

traditional personally identifiable information about individuals and communities.[29] By fusing these data-sources, SSP developed a 'previously unavailable, non-classified tool for situational awareness during alleged atrocity events'.[30] Moreover, SSP was prospective and real-time, tracking armed-groups moving to attack civilian population-centres[31] and locating grave-sites while killings were ongoing.[32]

The potential value of SSP as a conflict-mitigation tool is fairly clear from the above. However, over time, one of the key challenges for the project team was managing the unintended consequences of publicising information and images about vulnerable populations, when the likely audience of publications included belligerent parties to the conflict, who might use published data for criminal purposes.[33] SSP's approach exemplified a growing awareness of risks to individuals and communities emanating from multi-stream Demographically Identifiable Data (DII) of the kind collected and published by SSP. Studies show that knowing as few as four data-points is enough to re-identify 87-95% of people in a de-identified dataset, indicating that simple anonymisation may be insufficient to safeguard individual privacy.[34] Further, where different data-types are combined together, inferences can be drawn that enable re-identification of potentially vulnerable individuals and groups – the so-called 'Mosaic Effect'.[35]

The emergence of such unintended risks from a pioneering use of multi-stream, open-source data in a peacebuilding project points to the ongoing challenge that the use of OSI in non-permissive and remote settings poses. This has a significant read-across for projects deploying OSI in such settings to tackle EIDs. At the experts' consultation convened by the Geneva Academy, legal analysts involved in the SSP highlighted an assumption that now guides their risk-assessment of projects: *any material published will immediately be accessed by the person most likely to use it for the most harm*. This approach can be used to inform risk-assessments undertaken prior to the launching of OSI projects.

C. OSCE's *Special Monitoring Mission in Ukraine* (SMM)

The OSCE's SMM highlights the need to balance competing rights and obligations while undertaking OSI operations. Until its closure in 2022, the SMM was mandated under the Minsk Agreements ceasefire arrangements to gather information and report facts in Ukraine's Donbas

29 Raymond, 'Beyond "Do No Harm" and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data' in Taylor, Floridi, van der Sloot (eds.), *Group Privacy: new challenges of data technologies* (2017), p. 96.
30 Raymond, Davies, Card, al Achkar and Baker, 'While We Watched: Assessing the Impact of the Satellite Sentinel Project', 7 *Georgetown Journal of International Affairs* (2013), p. 187.
31 Satellite Sentinel Project, 'Crime Scene: Evidence of Mass Graves in Kadugli', 14 July 2011, available at: http://www.satsentinel.org/sites/default/files/SSP%2016%20Final%20Smaller.pdf.
32 Satellite Sentinel Project, 'State of Emergency: Threat of Imminent SAF Attack on Kurmuk, Blue Nile', 23 September 2011, available at: http://www.satsentinel.org/sites/default/files/Satellite Sentinel Project report 092311.pdf.
33 For an example of the real risks emanating from DII, see Raymond, 'Beyond "Do No Harm" and Individual Consent', pp. 93-95.
34 UN OCHA, 'Humanitarianism in the Age of Cyber-Warfare', 11 *OCHA Policy and Studies Series* (2014), p. 15.
35 Capotosto, 'The Mosaic Effect: the revelation risks of combining humanitarian and social protection data', ICRC *Humanitarian Law and Policy* (2021), available at: https://blogs.icrc.org/law-and-policy/2021/02/09/mosaic-effect-revelation-risks/.

region.[36] It deployed drones, along with OSI and geospatial information analysts, to monitor adherence to ceasefire provisions, publishing extensive open-source reports and frequently releasing drone footage online for further analysis and republication by civil society and the media,[37] although its mandate precluded attribution of responsibility to a conflict-party.[38]

The project highlights the privacy and data-protection ramifications of conducting drone flights for OSI-gathering over contested civilian areas. For example, publicly-identifying local civilians crossing the Donbas Line of Contact at unofficial crossing-points could result in punishment by the authorities and closure of crossings, with knock-on impacts on access to schools, workplaces and services – an unintended human rights threat vector to the use of OSI for ceasefire-monitoring purposes.[39] Nevertheless, where possible the SMM did attempt to obtain consent from civilian community-leaders before undertaking drone-surveillance and information gathering in a given area – highlighting the fact that even where informed consent is obtained at a community level it may not be a sufficient safeguard alone against impacting on individual and group privacy with real-world ramifications for rights of access to public services.

SMM staffers have highlighted other issues with the practices used in Donbas: the Mission lacked sufficient capacity to properly classify and secure data collected on individuals in line with data-protection best-practice,[40] while the use of private-sector subcontractors to operate long-range drones raised concerns about reliance on entities not adherent to humanitarian principles such as impartiality and respect for civilians.[41] Both of these issues raise concern about the safeguarding of data-protection rights of civilians and communities involved in the conflict.

This example highlights the role for new technologies – in particular, open-source evidence gathering and publication – in supporting existing ceasefire-monitoring processes, but also the risks for monitors of utilising such technology in an unregulated and potentially chaotic fashion. The real-world ramifications of unregulated collection and reproduction of OSI-gathered data are clearly visible, and highlight the balancing exercise that organisations may need to do in order to comply with their responsibilities to the privacy and safety of individuals and communities.

D. The German military in Afghanistan

A final example highlights real-life risks associated with open-source information that emanate from the failure to adequately *secure* open-source data in conflict-affected settings, where actors are able to use vulnerable data to facilitate human rights violations. As part of the International Security Assistance Force (ISAF) in Afghanistan from 2001-21, the German armed forces collected biometric data (fingerprints, iris images and 'face geometry' data) from Afghan citizens,

36 OSCE Permanent Council, 'Decision No. 1117 21 March 2014', PC.DEC/1117 (2014) (See https://www.osce.org/special-monitoring-mission-to-ukraine-closed).
37 International Partnership for Human Rights (IPHR), Norwegian Helsinki Committee, Ukrainian Helsinki Human Rights Union, Truth Hounds, 'Where did the shells come from? Investigation of cross-border attacks in eastern Ukraine' (2016).
38 Dorn and Giardullo, 'Analysis for Peace: The Evolving Data Tools of UN and OSCE Field Operations', 31 *Security and Human Rights* (2020), pp. 95-96.
39 Based on interviews with OSCE-SMM staffers by Edward Millett in 2022.
40 Dorn and Giardullo, 'Analysis for Peace', pp. 96-97.
41 OSCE Code of Conduct 2003, Art. 3; Dette, 'Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts', in Hostettler, Besson and Bolay (eds.), *Technologies for Development* (2018), p. 22.

which was handed over to US authorities. Mobile devices were used to identify people by matching biometric data against US databases.[42]

The German authorities have since acknowledged that no data protection standards were applied to information gathered – rather, they considered that domestic data protection laws did not apply extra-territorially to non-nationals' data.[43] However, the real-terms impacts of such failings to comply with legal obligations and best-practice can be drastic; in the chaotic departure from Afghanistan in 2021, Coalition forces were required to undertake a complex process of 'scrubbing' the digital presence of Afghan supporters from governmental websites to avoid enabling the Taliban regime to target collaborators.[44]

This example highlights the risks that arise from inadequate data-protection and management practices. Where an actor is capable of accessing open (and closed i.e. hacked, stolen, or classified) data sources such as biometric information databases, this gives rise to significant risks for individuals. There is a clear read-across to the enforced disappearance context, where actors may seek to gain access to information on individuals through the exploitation of poor data-protection practices.

Conclusion and recommendations

Our research has highlighted several areas where OSI can have a positive impact and help fulfil the international obligations in the field of enforced disappearance. At the same time, available practice suggests that even the most well-intended uses of OSI can result in harmful consequences, ultimately reversing the cost-benefit calculation of relying on OSI tools if appropriate safeguards are not put in place. To build on existing experience and with a view to achieving the aims of the international legal framework preventing and protecting from disappearance, we propose the following recommendations for further research and consideration:

- To advance accountability, take advantage of the full range of tools offered by OSI, aggregating different types of publicly available information to prove the various elements of which the conduct is composed.

- To facilitate the search of the disappeared, take stock of the complementary nature of accountability and search procedures; adapt the requirements, standards and strategies for recourse to OSI to the different *fora* (whether judicial or extra-judicial, whether focused on accountability or on the clarification of the fate and whereabouts of the disappeared).

- When deploying OSI in EID research and accountability initiatives, undertake a full risk assessment prior to commencement of the project. The *Berkeley Protocol* Annexes may serve as an initial guide to formulating risk-assessment, but may need updating/tailoring

42 Lubin, 'The Duty of Constant Care and Data Protection in War', in Dickinson and Berg (eds.), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (2022), p. 19; Cymutta, 'Biometric data processing by the German armed forces during deployment', NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 4 (2021).
43 Cymutta, *ibid*.
44 Freeze, 'Fearing reprisals, Afghans rush to scrub digital presence after Taliban takeover', GLOBE & MAIL CANADA (Aug. 21, 2021), https://www.theglobeandmail.com/canada/article-fearing-reprisals-afghans-rush-to-scrubdigital-presence-after-taliban/

to specific use/context. Risk-assessment should include consideration of privacy and data protection aspects, the obtaining – where feasible – of informed consent from relevant individuals and communities, DII risks. Before publishing, keep in mind that *any material published will immediately be accessed by the person most likely to use it for the most harm.*

- Consider DII risks and secondary human rights impacts emanating from the use of OSI during the project.

- Where extensive datasets are to be retained and/or published, consider adopting data-protection policies in line with international best-practice. For example, by adopting data-minimisation policies, deleting unnecessary footage and coarsening image-resolution on published imagery and video. Consider also the data-protection legal regime of the State of operations, as some are more restrictive / invasive than others.

- When dealing with varied users and entities in the context of OSI projects – States, International Organisations, NGOs, Individuals – acknowledge that the scope of legal responsibilities and rights may vary depending on the nature of the user.

For inquiries about the submission, please contact:
Dr Francesco Romani, Research Fellow at the Geneva Academy in charge of the IHL Expert Pool
Email: francesco.romani@geneva-academy.ch
Telephone: +41 (0) 22 908 44 76