Digital Dignity in Practice: Existing Digital Dignity Standards, Pursuing Digital Dignity and Current Gaps in Digital Dignity

In today's armed conflict landscape, digital risks range from the use of artificial intelligence and machine learning tools, to cyberattacks, mass surveillance systems, and campaigns that aim at "weaponizing information" for the purpose of disrupting information operations, spreading deliberate digital hate space campaigns, systematic manipulation of political discourse to propagate ideas and so forth.

Humanitarian action in armed conflict, as well as other situations of violence, must grapple with these new threats while simultaneously staying current with the adoption of new technological tools, which can improve and speed up humanitarian response efforts. The mass collection of data at every stage of humanitarian action feed into humanitarian databases, and predictive analytics systems that serve to support humanitarian assistance programs. Dual-use technologies such as facial recognition software and autonomous drones, which humanitarian organizations are increasingly using in action on armed conflict, present a unique challenge to the humanitarian principles and ethics to do no harm.

These dual-use technologies and collection of affected population's data create new and added harms for crisis-affected populations. As such, the application and realization of digital dignity in humanitarian action in armed conflict is critical to the success of humanitarian efforts in the current digital landscape. Specifically, the promotion of digital dignity is reliant upon the adoption of digital protection and do no digital harm standards and protocols by humanitarian organizations.

Whilst current best practice examples of digital dignity in humanitarian action in armed conflict are few and far between, digital standards, handbooks and protocols are increasingly being adopted in order to promote and ensure crisis-affected populations' digital dignity (see below). These standards offer digital

protection and rights' frameworks as a first step to the realization of digital dignity.

The following section looks dual-use technologies, third party service providers, handling requests for biometric data, humanitarian data incidents, and targeted military cyber-attacks on humanitarian and civilian data, which all lack considerations of digital dignity.

The concluding sections look to existing best practices for digital dignity in humanitarian action during armed conflict. These best practices are most obviously expressed in current digital humanitarian standards and handbooks. Several key organizations are leading the way in their efforts to promote digital dignity standards as they both produce key recommendations for digital humanitarian action and monitor the digital humanitarian landscape.

Existing Gaps: *This section highlights examples of current gaps in digital dignity, which must be examined more thoroughly by humanitarian organisations. This list is by no means exhaustive. It is here where the Wilton Park conference on digital dignity could generate important inputs:*

- **Dual-use Technologies***:* The adoption of dual-use technology in situations of armed conflict have the potential to produce increased digital dignity risks. Facial recognition software, drones, biometric and digital identity systems, crisis mapping tools and satellite imagery all represent examples of dual-use technologies. Humanitarian organisations' consideration of dual-use capabilities is critical to ensuring the digital dignity of crisis-affected populations. For instance, with reference to drones, ICRC writes, "Humanitarian Organizations should also realize that, even when identification of individuals is not possible via the use of Drones, their use may still have substantial implications for the life, liberty and dignity of individuals and communities. Humanitarian Organizations should accordingly take precautions to protect Drone-collected data, even if the individuals recorded in them are not immediately identifiable." (ICRC 2017:

88) While such considerations are increasingly mainstream in the humanitarian space, dual-use technologies remain problematic and require extra examination to ensure the digital dignity of crisis-affected populations.

- **Third-party service providers:** Humanitarian organisation's use of third-party service providers for support with digital technologies and data puts affected population's digital dignity at risk. With third-party service providers, information sharing and consent becomes increasingly difficult to obtain as more actors are involved in the collection and storage of data, in turn resulting in affected populations losing control of their personal data. Third-party service providers from the commercial sector pose an additional threat with the potential for the exploitation of beneficiary data. Recent examples of World Food Program's partnership with Palantir and Mercy Corp's partnership with Facebook's Libra cryptocurrency underscore substantial risk for digital dignity efforts as the humanitarian space becomes shared with private sector entities. Thus, examination into third party service providers must be prioritized as humanitarian organizations increasingly rely on commercial operators to support humanitarian programming.

- **Handling of requests for access to biometric data by state authorities**: The value of biometric data in locating and identifying persons of concern to States and security, law enforcement and judicial bodies is obvious and so is these authorities' interest in obtaining such data from organizations operating in humanitarian emergencies. While in some cases entirely legitimate from the point of view of the authorities, it may be incompatible with the principles of neutrality, impartiality and independence, the pillars of principled humanitarian action. In the realm of border and migration control, counter-terrorism activities and other explicitly stated national security interests, how can digital dignity be protected when responding to such request?

- **Humanitarian Data Incidents:** Whilst data incidents are increasingly common in the private and public sectors, data incidents in the humanitarian sector are also on the rise and pose real and serious risks to digital dignity. OCHA's Centre for Humanitarian Data's *Guidence Note on Data Incidents* states, "data incidents are events involving the management of data that have caused harm or have the potential to cause harm to crisis affected populations, humanitarian organisations and their operations, and other individuals or groups." (OCHA 2019: 1) Humanitarian data incidents, particularly ones that impact crisis-affected populations, present new added harms to already vulnerable populations through the leaking of private personal, and identifiable data. Data incidents can range from accidental data sharing to targeted attacks. For example, in September 2019, Melissa Fleming, under Secretary-General of Communications at UNHCR, tweeted an image of a child refugee which showed the child's private information to 2.3 million UNHCR twitter followers. (Mckveigh 2019) In 2017, competitors exploring Red Rose's software unintentionally breached Catholic Relief Service's beneficiary data. During this incident more than 8,000 beneficiaries' data was breached, highlighting the severity and scale of risk involved in the poor management and storage of vulnerable population's data. (Raymond, Scarnecchia, Campo 2017) Additionally, inside refugee camps, examples of the spreading of malware through mobile devices and data attacks highlight the potential of unintentional nefarious data incidents by affected populations themselves. (Maitland and Bharania 2017) These examples highlight the real and grave risks to digital dignity that data incidents pose. Whether intentional or not, data incidents are increasingly common and necessitate increased precautionary action. OCHA's Guidance Note on Data Incidents does provide a useful framework for humanitarian data incident management.

- **Humanitarian and Civilian Data Targeting by Military Actors:** Targeted cyber-attacks by military actors on crisis-affected populations as well as on

humanitarian databases is increasingly common in the digital risk landscape. For example, the Signal Project has experienced targeted attacks on their satellite feed, leading to compromised data of vulnerable populations. (UN OCHA 2014: 12) In Libya, fighting between rival militias in Tripoli in August 2018 led to at least 47 deaths, which included children, 130 injured and the escape of 400 prisoners. A parallel online battle occurred on Facebook, with not only dissemination of hateful rhetoric but also with so-called 'keyboard warriors' posting precise coordinates on Facebook to help target rival bases. (Walsh and Zwayé 2018) These examples highlight new trends in military targeting of both civilian and humanitarian data. In such circumstances, critical questions arise around response protocols and mitigation efforts.

Standards/Handbooks: *The following handbooks, standards and reports offer specific guidance on digital practices in humanitarian action. Whilst this list does not claim to be exhaustive, these examples demonstrate strong foundations to the promotion of digital dignity.*

Signal Code: A Human Rights Approach to Information During Crisis 2017

- Signal Code provides the most comprehensive framework for digital dignity in the humanitarian space. Its promotion of data rights, data agency and informed consent for affected populations are grounded in humanitarian principles of humanity. Specifically, Signal Code stipulates: "The articulation of the right to data agency enshrines extant protections in international law against non-consensual human experimentation and to ensure the dignity of crisis-affected populations as mandated by core humanitarian principles" (Signal Code, 2017: 46) In 2018, Signal Code expanded on its 2017 Code with the *Signal Code: Ethical Obligations for Humanitarian Information Activities 2018*. Importantly, the 2018 Signal Code articulates the following mandates:
- "Meaningful Consent- Humanitarians promote and protect the dignity of populations by ensuring free and meaningful consent, and by abiding by

internationally accepted human subjects research protections throughout the course of a humanitarian information activity." (Campo et al. 2018: 19)

- Ensuring agency and participation for affected populations: "Facilitating participation of affected populations at every stage of an HIA [humanitarian information activity] is a critical step to ensuring agency." (Ibid: 26)
- Ensuring a people-centered approach to humanitarian action ensures participation and agency. (Ibid: 28)
- Do no harm in technological innovation or experimentation: "Humanitarian actors must always endeavor to do no harm when engaging in research and experimentation; when the potential harm of a proposed activity cannot be reasonably determined and mitigated, the activity should not be undertaken." (Ibid: 36)
- Mitigating any risks emerging from data breaches around personally identifiable information and demographically identifiable information through data collection:
    - "Potential for irrevocable harm created by loss of privacy affecting the protection status of vulnerable people and populations, including but not limited to: refoulement, arbitrary detention, human trafficking, torture and disappearance, extrajudicial killings, social exclusion, economic exploitation, and expulsion from home communities.
    - Loss of dignity due to social exclusion and emotional distress related to the breach of private data.
    - Loss of livelihood or other financial losses due to theft, identity loss, or expense of mitigating against future harms arising from the original breach.
    - Erosion of trust between humanitarian responders and the affected population and subsequent loss of access to aid by the affected.
    - Violation of right to data agency and informed consent." (Ibid: 42)

The Humanitarian Metadata Problem: Doing No Harm in the Digital Era: This report highlights the ubiquity of new technologies in humanitarian response, the metadata these technologies produce, and the new threats to digital rights and dignity that emerge from the production of humanitarian metadata. By acknowledging that humanitarian organisations are increasingly using technological devices for humanitarian response, this report underscores the steps that must be taken to mitigate digital risks that infringe on the digital dignity of affected populations. In particular, this report pays close attention to the role that surveillance systems play in shaping metadata risks for all stakeholders involved in humanitarian response. Additionally, its findings look to both risks and mitigation efforts around telecommunications and messaging, messaging apps, cash transfer programs, mobile money, banking, smartcards and social media. By providing specific mitigation measures, The Humanitarian Metadata report creates concrete and material avenues to promote the digital dignity of individuals. For instance, with reference to mobile banking, it suggests humanitarian organisations should negotiate how much data can be collected and processed to limit third party access to data. (The International Committee of the Red Cross and Privacy International 2018)

ICRC Handbook on Data Protection in Humanitarian Action: ICRC's Data Protection handbook articulates the "implementation of Personal Data protection standards, even where not a legal obligation given the privileges and immunities enjoyed by certain Humanitarian Organizations, should be a priority for all Humanitarian Organizations, considering that the main objective of their activities is to work for the safety and dignity of individuals" (ICRC 2017: 16) Personal data protection and privacy are central to ICRC's data protection guidelines. Importantly, ICRC recognizes that data privacy is a fundamental right and is essential to promoting the digital dignity of affected populations. The ICRC handbook provides for example, stipulations around the further processing of information stating that, processing data for new purposes introduces new risks, which have the potential to comprise the dignity of affected populations. (Ibid: 36) As is common in other digital humanitarian standards, consent also emerges as a critical component to ensuring digital dignity. (Ibid: 55) Additionally, ICRC

specifically touches on drones and remote sensing technologies, arguing that drone use has the potential to infringe on population's digital dignity through its ability to collect data without the consent by data subjects. (ICRC 2017)

UN OCHA's (Working Draft) Data Responsibility Guidelines (March 2019): UN OCHA's data responsibility guidelines provides information on the "management of other forms of humanitarian data such as survey results and datasets containing information that could be used to target individuals in conflict areas." (UN OCHA 2019: 7) Specifically, these guidelines look at every step of the data management system: Planning, Collecting and Receiving, Storing, Cleaning, Transfer, Analysis, Communicating and Disseminating, Feedback and Evaluation, and Retention and Destruction. In providing a step-by-step guide to data management, with attention to sensitive data, OCHA's guidelines create a procedure to ensure data collection and management is done securely and uphold data rights for crisis-affected populations.

Danish Refugee Council/Global Protection Cluster Protection Information Management Principles in Action (PIM): The PIM initiative aims to provide guidance to humanitarian practitioners on information management, specifically information that is related to protection in humanitarian action. The PIM initiative outlines the need for humanitarian data collection, retention, and sharing to be principled and remain person-centric, and outlines principles that echo the principles mentioned above from other best practices. The PIM principles underscore the importance of the fundamental humanitarian principles in Protection Information Management, marrying the notion of data protection with the overarching purpose of the humanitarian imperative. The PIM principles also include the notion that data collection, retention, and sharing should have a defined purpose, and should be done across agencies in a coordinated and collaborative manner. (Danish Refugee Council 2017)

Organisations Promoting Digital Dignity: *The following organizations are actively engaging in the pursuit of digital dignity for crisis-affected populations. These*

examples showcase best practices of organisational engagement in topics of digital dignity.

- **Privacy International**: PI's latest campaign "Safeguarding People's Dignity" is actively seeking ways to ensure people's dignity online with special attention to ID systems, surveillance risks for digital activists, and data privacy and protection for vulnerable populations.
- **Centre for Humanitarian Data (OCHA)**: The Centre for Humanitarian Data focuses on the application and impact of data in humanitarian sector. The Centre's focus on data policy pays special attention to data security and responsibility by providing up-to-date policy frameworks for current digital humanitarian risks.
- **Harvard Humanitarian Initiative (HHI):** HHI's programming is grounded in efforts to enhance dignity of crisis-affected populations. Importantly, HHI has a strong focus on the application of ethical humanitarian technology in crises. As one example, the Uaviators program provides comprehensive guidelines on the deployment of UAVs with special attention to: data protection, community engagement, partnerships and conflict sensitivity. The Uaviators' Code of Conduct adheres to the humanitarian do no harm principles, thus upholding the digital dignity of populations UAVs interact with.
- **The Engine Room**: The Engine Room provides research and programming assistance to organisations using data and digital technologies. Critically, it works to ensure human rights, accountability, data privacy and ethics are upheld in the use of these technologies. For instance, The Engine Room's "Responsible Data at Oxfam" project looked into Oxfam's data management system and offered targeted solutions to support a rehaul of Oxfam's data protection program in order to ensure the responsible collection of beneficiary data. Oxfam contends its Responsible Data Management program upholds the rights and dignity of data respondents, highlighting a specific acknowledgement to the digital dignity of its beneficiary community.

- **Accessnow**: Accessnow's #keepiton campaign endeavors to ensure access to the internet for communities experiencing internet shutdowns. Internet shutdowns is an increasingly used tactic promoted by regimes to keep communities off of the internet and out of communication during crises, as recently experienced inside Sudan during its 2018-2019 revolution. Ensuring communities have access to the internet during crises promotes digital dignity in allowing individuals freedom of expression and the ability to communicate and share critical information during emergencies.
- **ICRC**: The ICRC's report on AI and machine learning for humanitarian action highlights the increasing use of AI/machine learning to inform assessments, to understand humanitarian consequences on the ground and to improve identification of missing persons. ICRC insists on using a human-centered approach to guide all AI work, which includes ensuring human control and judgements over AI technologies. ICRC also notes that it is critical to understand the technical limits of AI- such as inherent biases built into code. Moreover, machine learning systems have a problem with transparency because these systems produce outputs without explanation. (The International Committee of the Red Cross 2019:10)

Natalie Cliem Msc Candidate in International Development and Humanitarian Emergencies, the London School of Economics

Ann Marie McKenzie Msc Candidate in International Development and Humanitarian Emergencies, the London School of Economics

With inputs from:

Markus Geisser, Senior Humanitarian Policy Advisor with the International Committee of the Red Cross Regional Delegation in the UK and Ireland, London, UK

Adapted sections from a report written by candidates for the MSc in International Development and Humanitarian Emergencies at the London School of Economics and Political Science, Natalie Çilem, Emily Featherstone, Maud Lampreia Jacques, Ann Marie McKenzie, and Patty Ollé Tejero.

Bibliography

Campo, Stuart R., Caitlin N. Howarth, Nathaniel A. Raymond and Daniel P. Scarnecchia. "The Signal Code: A Human Rights Approach to Information During Crisis." Signal Program on Human Security and Technology, Standards and Ethics Series: 03. Cambridge: Harvard Humanitarian Initiative, January 2017.

Campo, Stuart R., Caitlin N. Howarth, Nathaniel A. Raymond and Daniel P. Scarnecchia. "The Signal Code: Ethical Obligations for Humanitarian Information Activities." Signal Program on Human Security and Technology, Standards and Ethics Series: 03. Cambridge: Harvard Humanitarian Initiative, May 2018.

Danish Refugee Council. 2017. "Principles of Protection Information Management." Protection Information Management.

International Committee of the Red Cross. 2017. "Handbook on Data Protection in Humanitarian Action." Geneva: International Committee of the Red Cross, 1–164. https://doi.org/S0264-410X(05)00973-4 [pii]\r10.1016/j.vaccine.2005.09.020.

Maitland, Carleen and Bharania, Rakesh, Balancing Security and Other Requirements in Hastily Formed Networks: The Case of the Syrian Refugee Response (March 31, 2017). Available at SSRN: https://ssrn.com/abstract=2944147 or http://dx.doi.org/10.2139/ssrn.2944147

McVeigh, Karen. "UN Communications Chief under Fire for Tweeting Refugee's Details." The Guardian. Guardian News and Media, September 3, 2019.

https://www.theguardian.com/global-development/2019/sep/03/un-communications-chief-under-fire-for-tweeting-refugees-details.

Raymond, Nathaniel A., Daniel P. Scarnecchia, and Stuart R. Campo. "Humanitarian Data Breaches: the Real Scandal Is Our Collective Inaction." The New Humanitarian, December 8, 2017. https://www.thenewhumanitarian.org/opinion/2017/12/08/humanitarian-data-breaches-real-scandal-our-collective-inaction.

The International Committee of the Red Cross. 2019. "Artificial Intelligence and Machine Learning in Armed Conflict : A Human-Centred Approach." Geneva.

The International Committee of the Red Cross, and Privacy International. 2018. "The Humanitarian Metadata Problem: 'Doing No Harm' in the Digital Era."

UN OCHA. 2019. "Data Responsibility Guidelines: Working Draft." OCHA: The Centre for Humanitarian Data.
———. 2019. "Guidance Note Series: Data Responsibility in Humanitarian Action. Note #2: Data Incident Management."
———.2014. "Humanitarianism in the Age of Cyber-Warfare." OCHA Policy and Studies Series.

Walsh, D., and Suliman, A. Z. (2018). A Facebook War: Libyans Battle on the Streets and on Screens, 4 September 2018, The New York Times. Available from: https://www.nytimes.com/2018/09/04/world/middleeast/libya-facebook.html