REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
06/04/2021	FINAL	N/A

4. TITLE AND SUBTITLE
Addressing the Ethics Concerns of Consent and Privacy in Humanitarian Cyberspace through Blockchain Technologies

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Andrew M. Francis

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Ethics and Emerging Military Technology
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES
A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the Ethics and Emerging Military Technology Graduate Certificate.

14. ABSTRACT
The methods and procedures in which aid recipient data is requested, received, maintained, used, and disregarded must be given greater care as humanitarian aid efforts become more immersed within the humanitarian cyberspace domain. This research paper proposes the adaptation of a humanitarian aid-driven privacy-aware blockchain protocol by humanitarian organizations to help protect the privacy of aid recipients and increase their conscious unforced consent of personal data. This research also asserts that leveraging blockchain technologies may offer data protection and security to humanitarian assistance and disaster relief recipients without compromising the integrity of Humanitarian Cyberspace.

15. SUBJECT TERMS
Key terms: humanitarian cyberspace, humanitarian assistance, disaster relief, blockchain, ethics, technology, consent, privacy.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Thomas E. Creely
					19b. TELEPHONE NUMBER *(Include area code)*
Unclassified	Unclassified	Unclassified	N/A	52	401-841-7542

NAVAL WAR COLLEGE
Newport, RI

Addressing the Ethics Concerns of Consent and Privacy in Humanitarian Cyberspace through Blockchain Technologies

Andrew M. Francis

Date Submitted: 03 June, 2021

A paper submitted to the Faculty of the United States Naval War College Newport, RI in partial satisfaction of the requirements of the Ethics and Emerging Military Technology Graduate Certificate

Abstract

The preservation of human dignity is becoming increasingly more conflicted as service sectors incorporate emerging technologies. The emergence of humanitarian cyberspace is particularly susceptible to the clashes between the ideological constructs of respect, equality, and autonomy in the conservation of human dignity. Upholding the humanitarian principles of neutrality, impartiality, independence, and humanity within humanitarian cyberspace requires ethical considerations of consent and privacy. The methods and procedures in which aid recipient data is requested, received, maintained, used, and disregarded must be given greater care as humanitarian aid efforts become more immersed within the humanitarian cyberspace domain.

Furthermore, ethical considerations must expand beyond utilitarian and deontological approaches to include the proactive contemplation of virtue and principle-based methods that seek to "do no digital harm." The ethical oversight for aid recipients should seek to protect vulnerable populations from exploitation. This research paper proposes the adaptation of a humanitarian aid-driven privacy-aware blockchain protocol by humanitarian organizations to help protect the privacy of aid recipients and increase their conscious unforced consent of personal data. This research also asserts that leveraging blockchain technologies may offer data protection and security to humanitarian assistance and disaster relief recipients without compromising the integrity of Humanitarian Cyberspace while remaining in alignment with humanitarian principles and relevant International Humanitarian Law.

Key terms: humanitarian cyberspace, humanitarian assistance, disaster relief, blockchain, ethics, technology, consent, privacy.

Acknowledgments

I want to express my gratitude to all of the many individuals who have contributed to my completion of this program. I am grateful to God for the grace, strength, sustainment, and fulfilled promise to never leave me – especially during the debilitating nights that required writing through the pain. To my beautiful, brilliant, and proficient wife Kenya, and my inspirations of joy Aidan, Claire, and Kaleb, I love you, and I thank you for your continued support of my career and ongoing sacrifices of service as a military family. To my parents, Lebert and Clarice, thank you for your encouragement and continued prayers through the years.

I also want to extend my appreciation to my professional network; To my EEMT intern Noah, thank you for your research assistance and perceptive pointers; Isabel, thank you for providing your research instruction expertise and editorial skills; Professor Polatty, thank you for sparking my interest in humanitarian cyberspace; Professor Shanks Kaurin, thank you for your engaging instruction on ethical thinking; Professor Shaw, I am grateful for your mentorship in this project and invaluable insights; Professor Schultz, thank you for your sage counsel, guidance, and motivation throughout the EEMT program; and to Professor Creely, thank you for your intentional engagement and EEMT program leadership, the value you pour into this program is evident and appreciated.

Finally, to my EEMT colleagues, thank you for the thought-provoking discussions and your dedication to contemplating how the evolving technological changes in our society will shape our collective code of ethics. May we continue to examine the ethical intricacies of new technologies and challenge others to consider the complex implications on culture and humanity.

Table of Contents

Prologue

"Nam et ipsa scientia potestas est."[1]
Knowledge is power

It was a typical day filled with regular morning preparation tasks. A younger preadolescent sibling is getting ready for school, donning the issued uniform. Upon departing their apartment complex, an abrupt explosion occurs at an adjacent building sending the vicinity into dismay. Shortly thereafter, it is revealed that the city is under attack, and the morning's assault has separated this younger sibling from their family. An older sibling sets out among the rubble in an attempt to reunite with the family.

The buildings are discernibly devastated by the ongoing shelling. Reports indicate that the random indiscriminate killing of women and children is prevalent. Further complicating reunification efforts is a natural disaster that brings flooding to the region. Dejectedly, no familiar discernable faces are found during the initial search. However, still having possession of a mobile phone, a call is attempted. After trying several locations to acquire connectivity, it becomes more readily apparent that the networks have failed. Still searching for any family or a signal, this older sibling runs into a friend that informs them that the only known place with accessible internet connectivity is located several kilometers outside of town, at the military base. Still hopeful of tracking down their family, the older sibling chooses to stay in town and continue the search.

The pursuit is unsuccessful. Another attempt is made with the mobile phone to reach someone by sending a message this time. Yet, similar to the previous efforts, no signal

1. John Bartlett, *Familiar Quotations, 10th ed*., 168, http://www.bartleby.com/100/139.39.html

connectivity is available. The futile attempts lead to the decision to venture from the town towards the military base, hoping to establish a means of connection. The journey takes nearly two hours, and the procession of people with similar travel plans accumulates to form a small caravan on the way to the base. Fortunately, the older sibling is able to arrive at the military base without any additional complications.

There are more familiar faces at the military base as people attempt to charge their devices and connect with their loved ones through the internet access point. Relievedly, the older sibling learns that their parents are also at the base and reunites with them. Unpropitiously though, the older sibling is informed that their younger sibling remains missing. A few friends notify the older sibling that an online social media group is available to assist people with locating their loved ones separated by these exigent circumstances. After connecting to the base's wireless network, the older sibling decides to join the social media group and post a photo of the younger sibling and the last place seen.

The older sibling receives several responses after posting the photo, name, and last known location of the missing younger sibling to the site. Some of the messages did not provide any assistance. Far too many of the replies were filled with vitriol and content advocating for continued assaults against the civilian groups and other suggestions of implied genocidal violence. Despite that, one message managed to offer some insight about a temporary installation set up by the International Red Cross and Red Crescent Movement to help families find missing members. A follow-on message indicates that the younger sibling is located at this temporary International Red Cross and Red Crescent Movement facility near the town hall.

Concerningly, the hateful rhetoric on the social media chat board continues and grows more intense. A few explicit and disconcerting replies emote the threat of violence linked to the

confirmed knowledge of the whereabouts of the younger sibling and similarly displaced persons. The banter on the site ranges from apathy and indifference to hate speech and vehement threats. Apprehensive about the vulnerability of the younger sibling, the elder sets out back to the town to retrieve their sibling and ensure their safety.

The town appears to be in greater disarray. The crisis coupled with web-based frictions has fueled tensions. Several armed groups have taken to the streets with multiple clashes and hostilities, reflecting the overspill of the hate-filled online bigotry. Undeterred by the growing turmoil, the siblings reconnect and venture back toward the military base, only to find it under attack. During the unanticipated onslaught, the younger sibling is injured. The most prudent course of action is to take the younger sibling to the next closest town. There the older sibling locates a bar establishment with an available open Wifi signal. Upon establishing a connection, the older sibling finds multiple medical service resources, but they are all located across the border.

At the border, the border patrol requests identification. Fingerprints and the mobile phone are the only identifying items the older sibling possesses. To gain entry en route to the medical services site, the older sibling supplies the fingerprints and phone in compliance with the border patrol's request. Following the fingerprint and phone scans, the border patrol immediately arrests the older sibling. The older sibling is suspected of being an opposition collaborator based on the location data acquired from the phone. Mercifully, a local community organization steps in to secure critical medical care for the younger sibling. The organization also successfully intercedes with the border patrol on behalf of the older sibling. Additionally, the organization provides the siblings with sim cards to maintain communication in case of involuntary separation. Eventually,

the siblings apply for asylum and maintain contact with their family as they await the request for approval.[2]

2. Adapted from International Movement, ed, “Humanitarian Crises Digital Dilemmas,” Digital Dilemmas, accessed May 7, 2021, http://www.digital-dilemmas.com/

Introduction

The enhanced susceptibility to exploitation for displaced persons trapped in exigent environments raises significant ethical concerns, particularly related to the technological elements of humanitarian cyberspace. The prologue narrative, based on the Digital Dilemmas[3] interactive story, chronicles several relevant humanitarian cyberspace issues. Pertinent themes raised include the importance of data, the centrality of connectivity in crisis, the threats and benefits of social media forums, the potential for biometric abuse, the increasing universality of digital exchanges for goods and services, and the need for digital protection for people in crisis.[4] The dilemma dramatically illustrates that as a result of data misuse or abuse, persons may "be stigmatized, detained, deprived of assistance, be subject to increased vulnerability, discrimination, persecution, and attacks on their physical and psychological integrity." The implications of these vulnerabilities threaten to weaken the efficacy of humanitarian efforts, particularly in the cyber domain.

Humanitarian assistance and disaster relief (HA/DR) are essential services for ensuring humane support during complex emergencies. The increased dependence on information and communication technology (ICT) magnifies the impact of benefits and potential detriments to aid recipients. A particularly problematic area that raises protection concerns for vulnerable populations is that of privacy. The personal privacy of distressed individuals is bartered for goods and services to ensure their ability to secure physical, emotional, mental, and social

3. International Movement, ed, "Humanitarian Crises Digital Dilemmas," Digital Dilemmas, accessed May 7, 2021, http://www.digital-dilemmas.com/

4. Zahraa Khaleel Mohsin Al-Janabi, Pascal Perrot, Yannick Heiniger, and Claudiu Mateescu, "Catalogue of Experiences," Digital Dilemmas, accessed May 7, 2021, http://www.digital-dilemmas.com/sites/default/files/downloads/cicr_catalogue_prod.pdf

stability. Refusal to participate in an exchange of personal data for humanitarian relief increases their probability of being refused access to assistance, becoming disenfranchised, and remaining destitute. On the other side, relinquishing their personal data may open the door for them to be mischaracterized, denigrated, mistreated, and revictimized. Another option must be afforded to address legitimate concerns of humanitarian entities without compromising the personal safety of those desiring humanitarian assistance. This research project explores the applicable challenges and proposes a viable solution to data privacy issues for beneficiaries of humanitarian aid.

This research asserts that blockchain technologies may be leveraged to address privacy awareness and offer data protection and security to humanitarian aid recipients without compromising the integrity of Humanitarian Cyberspace. This study investigates how blockchain technologies, cryptography-based peer-to-peer distributed consensus algorithms,[5] may fill the gap to meet individual privacy needs while supporting HA/DR efforts. More specifically, this research explores how data can be protected for humanitarian aid beneficiaries in alignment with humanitarian principles and current International Humanitarian Law (IHL). It also considers how the proposed solutions may strengthen Humanitarian Cyberspace vulnerabilities related to endangered populations. The research for this study has been limited to applications within the Humanitarian Cyberspace domain. Furthermore, the scope focuses on issues of privacy and the implications suited for HA/DR. It assumes that the applications of the proposed solutions would only be valid for comparable environments that necessitate an exchange of personal data for appropriate humanitarian assistance.

5. Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil and Georgia Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives.," *Cryptography* 3, no. 1 (2019): 2, https://www.mdpi.com/2410-387X/3/1/3/pdf

The presentation of this research is organized in the following manner. The subsequent section analyzes the privacy protection issues within humanitarian cyberspace. Successively, the ethical implications of contemporary humanitarian cyberspace privacy challenges are examined. The proposed blockchain technological resolution is expounded with an accompanying assessment. Finally, notable discussion points are highlighted, along with recommendations followed by a summary.

Problem Analysis

The devastating plight of disasters set into motion a series of circumstances in which survival becomes the dominant pursuit. Various challenges can arise in a modern-day humanitarian crisis. Global digitalization exposes those affected by the crisis to new forms of risk, which include hacking disruptions, disparate digital domination, and technological coercion.[6] Additionally, contemporary humanitarian crises are increasingly infused with digital dilemmas. As calamity typically expands past an inconvenient disruption into life-altering realities, sustenance and security become critical to subsistence. When life-sustaining humanitarian aid delivery and access is tied to an exchange in order to receive that assistance, an inequitable hierarchy of viability is produced.

6. International Movement, ed, “Humanitarian Crises Digital Dilemmas,” Digital Dilemmas, accessed May 7, 2021, http://www.digital-dilemmas.com/

The Case for Dignity

Humanitarian assistance in the event of natural disasters or man-made crises is "intended to save lives, alleviate suffering and maintain human dignity."[7] The latter tasks are part and parcel of the nomenclature of humanitarian assistance and disaster relief. The association between these terms also suggests that the alleviation of suffering is linked to human dignity. Humane support is key to the effectual functions of HA/DR. Given the incorporation of emerging technologies, safeguarding human dignity encompasses expanded responsibilities.

Leveraging ICTs within the HA/DR space reflects the beneficial utility of data in providing indispensable support. The aggregated data has proved pivotal in supporting medical care and transports, logistical coordination for assets, accounting for aid distributions, modeling human migratory patterns, projecting safe computer-simulated conveyance routes, messaging, and communication.[8] Notwithstanding, a privacy exchange requirement may infringe upon preserving dignity even while administering humanitarian aid through medical care during a crisis, providing location services for displaced individuals, enabling access to communication with loved ones, or in the fulfillment of basic provisions.

Human dignity consists of a basic social recognition of the unique qualities of an individual concomitant to the provision expectation of minimum existential living conditions

---

7. "Defining Humanitarian Assistance," Global Humanitarian Assistance, accessed May 31, 2021, http://www.globalhumanitarianassistance.org/data-guides/defining-humanitarian-aid./#:~:text=Humanitarian%20assistance%20is%20intended%20to,for%20when%20such%20situations%20occur

8. Patrick Meier, *Digital Humanitarians: How Big Bata is Changing the Face of Humanitarian Response*, (Boca Raton, FL: CRC Press, 2015), 19.

incarnate to economic and social generational human rights.[9] Human dignity respects the being of an individual based exclusively on the reality of their existence. Furthermore, human dignity acknowledges the distinctive identity of each person. Lastly, human dignity is accompanied by the reasonable expectation that each human warrants the basics to sustain life and an equal opportunity to contribute to the community from a personal prerogative to pursue community. Equal opportunity speaks to self-determination, and prerogative speaks to autonomy. When respect, equality, or autonomy are endangered, human dignity is also threatened.

Privacy laws, in particular, include the arena of personal autonomy that emanates from a rubric of privacy rights.[10] In the U.S., dignity is codified within the law where the "protection of the personal sphere entails a number of strands, such as privacy, informational self-determination, and control over one's portrayal in society."[11] The European Parliament, through the Council of the European Union, adopted the General Data Protection Regulation (GDPR). [12] This regulation stated that rules "shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights." [13] Expanding beyond western centralization, the preamble of the Universal Declaration of Human Rights from the General Assembly of the United Nations opens with the "recognition of the inherent dignity and

---

9. Rinie Steinmann, "The Core Meaning of Human Ddignity," *PER: Potchefstroomse Elektroniese Regsblad* 19, no. 1 (2016): 6, http://dx.doi.org/10.17159/1727-3781/2016/v19i0a1244

10. Edward J. Eberle, "Human Dignity, Privacy, and Personality in German and American Constitutional Law," Utah L. Rev. 163, (1997): 966, https://docs.rwu.edu/cgi/viewcontent.cgi?article=1067&context=law_fac_fs

11. Eberle, *Human Dignity*, 967.

12. Luciano Floridi, "On Human Dignity as a Foundation for the Right to Privacy," *Philosophy & Technology* 29, no. 4 (2016): 307, https://link.springer.com/content/pdf/10.1007/s13347-016-0220-8.pdf

13. Floridi, *On Human Dignity*, 307.

of the equal and inalienable rights of all members of the human family."[14] The declaration continues to state in Article 12 that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." [15]

Human dignity remains intertwined with privacy in concept and in custom. As an aspect of human dignity, societies look to the legal structures to protect privacy as a right, even as the levels of privacy may vary between cultures. Eberle posits that "a right to informational privacy and self-determination plausibly could exist to safeguard human liberty and self-government in the information age."[16] As such, support for privacy remains central to upholding human dignity by humanitarian aid organizations.

Humanitarian Civil-Military Coordination

Humanitarian assistance and disaster relief (HA/DR) missions are a core capability of the U.S. Department of Defense (DoD). As a HA/DR global leader, the U.S. military is unmatched in the forward-deployed resource capacity they possess that allows them to efficiently respond to

14. United Nations, "Universal Declaration of Human Rights," Vol. 3381, Department of State, United States of America, 1949, accessed on May 14, 2021 on https://www.un.org/en/about-us/universal-declaration-of-human-rights

15. United Nations, *Universal Declaration*.

16. Eberle, *Human Dignity*, 1006.

humanitarian disasters internationally.[17] The military can rapidly deploy resources at unparalleled levels, yet implementation and execution of HA/DR missions follow a model of civilian control.[18] Notwithstanding, U.S. military doctrine is clear that foreign humanitarian assistance is conducted in support of U.S. foreign policy interests.[19] All the same, the U.S. military remains uniquely qualified to execute the critical role of "aligning operations with host government leadership [and] preserving humanitarian space."[20] The standard for the humanitarian ecosystem also requires a request or consent from an affected state in order for aid to be administered.[21] Preservation of the humanitarian ecology is fundamental to maintaining trust between varying international stakeholders.

Operations within the international humanitarian environment presuppose cooperation and coordination. Cooperation may include joint planning, support, and execution which may

17. Jennifer D. P. Moroney, Stephanie Pezard, Laurel E. Miller, Jeffrey Engstrom, Abby Doll, *Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region*, (Santa Monica, CA: RAND Corporation, 2013), xiii, https://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR146/RAND_RR146.sum.pdf

18. "UPTEMPO: The United States and Natural Disasters in the Pacific," New America, accessed May 14, 2021, https://www.newamerica.org/resource-security/reports/uptempo-united-states-and-natural-disasters/part-ii-military-humanitarian-and-disaster-relief-response-capacity-in-the-indo-pacific-region/.

19. Joint Force Development, *Foreign Humanitarian Assistance: Joint Publication 3-29*, Washington: DC: Department of Defense 2019, I-4, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_29.pdf

20. Patrick R Laraby, Margaret Bourdeaux, S. Ward Casscells, David J. Smith, and Lynn Lawry, "Humanitarian Assistance and Disaster Felief: Changing the Face of Defense," *American Journal of Disaster Medicine* 4, no. 1(2009): 33.

21. Humanitarian Civil-Military Coordination Guide for the Military 2.0, United Nations Office for the Coordination of Humanitarian Affairs (Geneva, 2017), 18, accessed on May 14, 2021 on https://www.unocha.org/sites/unocha/files/Guide%20for%20the%20Military%20v2.pdf

vary based on settings and organizational relationships.[22] The level of cooperative efforts can range from full cooperation to simple coexistence.[23] Cooperative actions may include needs assessments,[24] partnership support from the private sector for humanitarian organizations through funding, logistical or technical assistance,[25] regional organization collaborations,[26] and nurturing National Society relationships.[27] In tandem, coordination refers to the exchange of information, agreements on joint policies and actions, and synchronizing individual activities.[28] Within the first few moments following a disaster, the On-Site Operations Coordination Centre (OSOCC) "provides a platform for cooperation, coordination and information exchange."[29] In short, the core elements of "humanitarian civil-military interaction are information sharing, task division, and joint planning."[30] Cooperation and coordination both necessitate some level of information sharing.

Information Sharing

Information sharing is central to humanitarian civil-military action. The adjudication of action is determined "through consensus, cooperation, and information sharing, to gain a clear picture of the situation and prioritize resources to address needs and avoid duplication of

22. Ibid., 35.
23. Ibid., 5.
24. Ibid., 10.
25. Ibid., 18.
26. Ibid., 19.
27. Ibid., 22.
28. Ibid., 35.
29. Ibid., 32.
30. Ibid., 44.

effort."[31] Information management is imperative during humanitarian coordination to connect the dots and prevent duplication by employing varying existing tools to collect, analyze, and disseminate the data.[32] Disaster conditions for the operational space are evaluated through mitigation measures by sharing humanitarian assessment data using humanitarian information tools.[33]

As data has become more central to implementing professional international humanitarian assistance, one of the primary tasks associated with the United Nations Humanitarian Civil-Military Coordination (UN-CMCoord) function is to "establish a mechanism for information exchange and humanitarian interaction with military forces and other armed actors."[34] Information sharing may be limited in complex emergencies to relevancy for addressing safety and security concerns of humanitarian workers or for the protection of civilians.[35] One such system is the establishment of a Humanitarian Notification System for Deconfliction (HNS4D) that shares information necessary to safeguard humanitarian convoys and facilities.[36] More precisely, the HNS4D "shares global positioning system (GPS) coordinates of humanitarian locations, activities, and personnel (static and non-static) with warring parties, especially those using airpower, for the purpose of protection against attacks (mainly

31. Ibid., 31.
32. Ibid., 36.
33. Ibid., 13.
34. Ibid., 54.
35. Ibid., 44.
36. Ibid., 45.

airstrikes)."[37] The implication is that information sharing data enables the coordination mechanisms for belligerent parties to be more attentive to the safeguarding of humanitarian pursuits.

The information-sharing challenges within the humanitarian space are not unique to the civilian-military HA/DR relationship. Several sizable humanitarian organizations have noted the emerging concerns and have crafted data protection guidelines with the purpose of protecting aid recipient data. Some of the abovementioned humanitarian organizations, as noted by the Center for Human Rights & Humanitarian Studies in the Humanitarian Civil-Military Information-Sharing in Complex Emergencies, include: [38]

(i) International Committee of the Red Cross (ICRC) and Brussels Privacy Hub's (BPH) *Handbook on Data Protection in Humanitarian Action*

(ii) UN Privacy Policy Group's (UN PPG) *Principles on Personal Data Protection and Privacy*

(iii) OCHA's *Data Responsibility Guidelines*

(iv) UN World Food Programme's (WFP) *Data Privacy and Protection Framework*

(vi) Harvard Humanitarian Initiative's (HHI) *Signal Code.* [39]

---

37. Naysan Adlparvar, "Humanitarian Civil-Military Information-Sharing in Complex Emergencies," 2.0, Center for Human Rights & Humanitarian Studies, *Watson Institute for International Public Affairs Brown University*, August 2020, 6, accessed on May 14, 2021 on https://watson.brown.edu/chrhs/files/chrhs/imce/research/Humanitarian%20Civil-Military%20Information-Sharing%20in%20Complex%20Emergencies_Adlparvar.pdf

38. Adlparvar, *Humanitarian Civil-Military*, 14.

39. Ibid.

The recognition of the need for aid recipient data protections highlights not only the necessity but also the wider roles big data and technology have come to play within modern-day humanitarian efforts. This intersection of humanitarian aid and the digital domain has given rise to the formation of humanitarian cyberspace.

Humanitarian Cyberspace

Operations within the cyberspace realm widen the aperture for humanitarian action, which expands the traditional functions of humanitarian aid.[40] The National Institute of Standards and Technology defines cyberspace as a "global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[41] Given these parameters, an applicable working definition for humanitarian cyberspace is the superimposed domain of humanitarian interaction and cyber operations, characterized by humanitarian principles and protected by IHL with the purpose of providing sustainable humanitarian action. [42]

Though humanitarian technology has been on the international policy agenda since the mid-1990s,[43] humanitarian cyberspace has been a more recent evolvement. Operating within the

---

40. Kristin Bergtora Sandvik, "The Humanitarian Cyberspace: Shrinking Space or an Expanding Frontier?," *Third World Quarterly* 37, no.1 (2016): 18, http://dx.doi.org/10.1080/01436597.2015.1043992

41. National Institute of Standards and Technology, ed., "Cyberspace - Glossary," Computer Security Resource Center (U. S. Department of Commerce), accessed May 14, 2021, https://csrc.nist.gov/glossary/term/cyberspace.

42. Faine Greenwood, Caitlin Howarth, Danielle Escudero Poole, Nathaniel A. Raymond, and Daniel P. Scarnecchia. "The Signal Code: A Human Rights Approach to Information During Crisis," *Harvard Humanitarian Initiative,* (2017): 41.

43. Sandvik, *The Humanitarian Cyberspace*, 18.

information environment takes on additional considerations. Various actors have entered into cyber operations that employ "cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace."[44] As telecommunications networks, computer systems, and related communications technology rapidly evolve, the potential for cyberattacks, cyberthreats, and other cybersecurity threats also expands. These threats necessitate governance laws, adaptations, and unique solutions.

The query of applicable regulations has been raised to confront the issue of addressing cyber operation standards. For the Department of Defense, "DOD policy states that the fundamental principles of the law of war will apply to cyberspace operations."[45] The ICRC, entrusted by the international community as the guardians of IHL,[46] maintains that the law of armed conflict governs cyber operations.[47] In addition to IHL, the 1948 Universal Declaration of Human Rights (UDHR) also applies in cyberspace as persons exercise their right to "seek, receive and impart information and ideas through any media and regardless of frontiers."[48]

---

44. University of Adelaide, "Cyber101x: Tallinn Manual on Cyber Operations," YouTube Video, 10:14, Jun 17, 2015, https://youtu.be/Am4gOf-KDG0

45. Catherine A. Theohary, "Defense Primer: Cyberspace Operations," Congressional Research Service (Congress.gov, December 15, 2020), 2, accessed on May 14, 2021 at https://crsreports.congress.gov/product/pdf/IF/IF10537

46. Yves Sandoz, "The International Committee of the Red Cross as Guardian of International Humanitarian Law," ICRC (*International Committee of the Red Cross*,) December 31, 1998, https://www.icrc.org/en/doc/resources/documents/misc/about-the-icrc-311298.htm

47. Ben Parker, "Bots and Bombs: Does Cyberspace Need a 'Digital Geneva Convention'?," *The New Humanitarian*, November 15, 2017, https://www.thenewhumanitarian.org/analysis/2017/11/15/bots-and-bombs-does-cyberspace-need-digital-geneva-convention

48. Harold Hongju Koh, "International Law in Cyberspace," Harvard International Law Journal 54, (December 2012): 10, https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

In addition to the applicable laws and anticipated adaptations, there have also been suggested solutions put forth to address cyberspace challenges and threats. One such unique solution was the proposal from Microsoft for a Digital Geneva Convention.[49] Such a convention would invite the public sector to take on additional global systems to assist in shaping humanitarian protections as well as human rights for the digital age.[50] Part of the proposal put forth for this Digital Geneva Convention included:[51]

1. No targeting of tech companies, private sector, or critical infrastructure
2. Assist private-sector efforts to detect, contain, respond to, and recover from events.
3. Report vulnerabilities to vendors rather than stockpile, sell, or exploit them.
4. Exercise restraint in developing cyberweapons and ensure that any developed are limited, precise, and not reusable.
5. Commit nonproliferation activities to cyberweapons.
6. Limit offensive operations to avoid a mass event.

The suggestions put forth by the Digital Geneva Convention have practical utility in delineating civilians from state actors, employing the merits of ethical hacking, and reducing intentional cyber-harm. At a minimum, the proposal may encourage conversation on the need for legal norms for cyberspace operations. [52] Opponents point out the glaring conflict of interest and the

---

49. Brad Smith, "The Need for a Digital Geneva Convention," *Microsoft On the Issues,* February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv

50. Joseph Guay and Lisa Rudnick, "What the Digital Geneva Convention Means for the Future of Humanitarian Action," *UNHCR Innovation Service,* June 25, 2017, https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

51. Smith, *The Need.*

52. Parker, *Bots and Bombs.*

danger of outsourcing critical infrastructure resources to the corporate sector, even if the sector is pushing for a neutral digital Switzerland.[53]

The dangers from potential cyber harms to humanitarian information activities (HIAs) put vulnerable populations at risk. There is no denying that humanitarian aid agencies are consistently developing and deploying data in forms that constitute humanitarian assistance to include coordination of aid delivery, health services, and safe shelter.[54] Some level of mitigation is needed to protect vulnerable populations from their inadvertent exposure to the emerging cyber threats raised in operating from a new data-driven framework.[55] Humanitarian cyberspace has the potential to transform humanitarian organizations "into entities that threaten the privacy and physical security of people of concern."[56] Failing to proactively face these challenges head-on may also threaten the core humanitarian principles of neutrality, impartiality, operational independence, and humanity.[57]

The humanitarian principles each play a significant role in shaping humanitarian cyberspace. The principle of humanity is seen as a core principle and the impetus behind humanitarian actions.[58] The principle states that "Human suffering must be addressed wherever it is found. The purpose of humanitarian action is to protect life and health and ensure respect for human beings."[59] By the given definition, the qualifier "wherever it is found" must include

53. Ibid.
54. Guay, *What the Digital*.
55. Ibid.
56. Sandvik, *The Humanitarian,* 25.
57. *Humanitarian Civil-Military Coordination Guide,* 8.
58. Ibid.
59. Ibid.

cyberspace. Thus, addressing life protection measures, health sustainment, and respect for humanity, even in the cyberspace domain, remains a task in line with the core principle of humanity. The principle of impartiality speaks to the characteristic necessary to respect aid recipients with equality and fairness "regardless of their nationality, race, gender, religious beliefs, class, or political opinion."[60] Within humanitarian cyberspace, this has implications for the technologically deficient as well as those with technological access. Aid or assistance that is based solely on the technological capabilities of those in need would inherently carry a bias toward the technologically able populations. The practice of the principle of impartiality in cyberspace would need to account for the capabilities as well as the deficiencies of the populations which humanitarians intend to serve.

The principle of neutrality conveys the expectation that humanitarians do not take sides in conflicts or contribute to political or social controversies.[61] The challenge in humanitarian cyberspace is the role perception plays in maintaining neutrality. Misperceptions can be magnified as the human element is removed from the equation in cyberspace. Protocols and procedures would need to be constantly reassessed to evaluate how cyber actions are being perceived by all stakeholders. Taking a particular action or failing to act may threaten that perception of neutrality. Furthermore, cyber leaks that may even be the result of targeted attacks would still jeopardize that perception of neutrality.

Lastly, the ability to uphold the principles of humanity, impartiality, and neutrality rest on the final humanitarian principle of operational independence. Autonomy is critical to

60. Ibid.

61. Ibid.

humanitarian assistance, as well as the ability to operate self-sustained and independently from military, political, or economic entities.[62] Humanitarian cyberspace is especially challenged in this regard as no singular humanitarian entity owns the totality of the operating space, access points, cyber tools, or required hardware. When conflicts arise, and one of those aforementioned elements is outside the onus of the humanitarian organization, that lack of autonomy brings into question neutrality and impartiality. Any arrangement to acquire deficient resources may challenge perceptions. Furthermore, the operation of inefficient tools within cyberspace that lack adequate support, security, or critical capabilities would fail to meet the standard of autonomy. Additionally, such neglect would raise the matter of ethical oversight for aid recipients.

Ethical Concerns

Humanitarian cyberspace is a data-driven framework; thus, the primary set of ethical considerations must focus on the information curated by humanitarian organizations. If the information collected is not properly protected, it will inevitably be exposed to vulnerabilities that jeopardize the safety and well-being of aid recipients. Linking people to places through traceable data like geopositioning, open channel communications, open-source crisis maps, identity theft, subject surveillance, and insider abuse are all feasible ICT threats that carry significant ethical implications if neglected.[63] Geopositioning, open-source crisis maps, and subject surveillance data may be triangulated to create targets rather than avoid them, as in the proposed HNS4D. Furthermore, following the intended utilization of HNS4D, the white space or

62. *Humanitarian Civil-Military Coordination Guide*, 8.

63. Matthew Hunt, John Pringle, Markus Christen, Lisa Eckenwiler, Lisa Schwartz, Anushree Davé, "Ethics of Emergent Information and Communication Technology Applications in Humanitarian Medical Assistance," *International Health* 8, no. 4, July 2016: 241, https://doi.org/10.1093/inthealth/ihw028

unmarked exclusion area may provide information to opposing belligerent forces, which causes the information to morph into intelligence, thus compromising impartiality and neutrality.

Even in competition below the level of armed conflict, such as in the case of the U.S. and China, the prospect of information morphing into intelligence limits joint nation participation in combined HA/DR efforts.[64] As previously stated, military participation in HA/DR efforts includes a state interest. Those interests may range from coercive diplomacy to international legitimacy. As those entities lobby for favorable recognition in HA/DR efforts, impartiality and neutrality appear to be diminished, given the stated intentions of participating military, political, or economic entities. While the utilitarian ethical lens gives weight to the ends, the deontological lens considers the means.[65] In this particular instance, the means would compromise the humanitarian principles of independence, impartiality, and neutrality. This potential for undermining influence is acknowledged by the principle of last resort that intentionally separates humanitarian organizations from militaries.[66]

An additionally valid humanitarian cyberspace ethical concern is the marginalization of technology deficient communities. The social advantages of technology access must be considered in the context of impartiality. In an attempt to provide access to technologically deprived communities, collateral effects may also result. Centralized access points also engender

64. Hugh Harsono, "HA/DR: A Case Study for Potential Bilateral U.S.-China Interoperability," WAR ROOM, November 19, 2019, https://warroom.armywarcollege.edu/articles/ha-dr-sof/

65. Lawrence M. Hinman, *Ethics: A Pluralistic Approach to Moral Theory*, (Boston, MA: Wadsworth, 2013), 125-126, 161-163.

66. Andrea H. Cameron, *Civil-Military Cooperation In Humanitarian Response: An International Practices Approach*, PhD dissertation, (Naval Postgraduate School, Montery, CA, 2020), 3, https://apps.dtic.mil/sti/pdfs/AD1114641.pdf.

points of attacks for malicious actors. On the other hand of this ethical dilemma is the challenge of providing equal access to aid for technologically marginalized communities. Humanitarian decisions based on the technological capabilities of a community may exclude needed aid on account of the humanitarian provider's self-imposed limitations.[67] Such an aid deployment structure would threaten the principle of impartiality.

The absence of an exclusive humanitarian cyberspace ecosystem raises the ethical questions of third-party influences. As humanitarian organizations rely on third-party services, concerns of data control, continuity of service, and dual-use technologies present ethical challenges to the principle of autonomy with effects for impartiality and neutrality.[68] How data is collected, used, maintained, and secured has effects on aid recipients. When humanitarian organizations must rely on third-party entities to collect that data, the ethics of how that information was solicited comes into question. Was the data mined or freely offered? Was consent given to obtain the data? Was informed consent granted for the duration and methods in which the data may be used? When and how could aid recipients revoke their consent? How will that data be retrieved once consent is revoked?

Furthermore, if third-party entities are in control of the data, questions about their affiliations bring true neutrality into question. The political stances of those third-party entities, their activism stances or lack thereof, as well as how society may wish to hold those entities accountable for current or past behaviors, all have ethical implications. In terms of continuity of service, reliance on a third-party entity also raises the issue of joint capabilities and

67. Hunt, *Ethics of Emergent*, 242.

68. Ibid., 241.

responsibilities. Is the third-party entity capable of sustaining the required level of support? If not, what does that promised or loss of expected care mean for aid recipients? Another aspect of that ethical dilemma deals with dual purposed technologies. A tool that gathers population data may potentially be used for political purposes or to deliver military effects, fundamentally manifesting a reality in which humanitarian organizations test run technologies that may be re-designated for other non-humanitarian purposes. Those ethical quandaries are plausible and valid, even more so when humanitarian endeavors are characterized by urgency, an immediate need for a particular population, third-party donor interests, or the desired programming of national governments. [69]

The ethics of consent and privacy are central to the humanity principle discussion of humanitarian aid. Establishing consent normally necessitates a "clearly defined scope of action that an individual gives permission for another person (or group) to do to that person."[70] Without consent, the autonomy of an individual is threatened. Similarly, deprived privacy threatens the dignity of an individual. How data that is collected, with or without consent, and is utilized speaks to the issue of privacy. However, humanitarian organizations do not generally work from a position of forced compliance but from one of intended consent. The term intended consent is used as a complete understanding of consent seems to be lacking in the humanitarian cyberspace realm.

---

69. Catherine R. McGowan, Louisa Baxter, Marc DuBois, Julian Sheather, Ruma Khondaker, Rachael Cummings & Kevin Watkins, "Preparing Humanitarians to Address Ethical Problems," *Conflict and Health* 14**, no.** 72 (2020): 2, https://doi.org/10.1186/s13031-020-00319-4

70. Meg Leta Jones, Ellen Kaufman, and Elizabeth Edenberg, "AI and the Ethics of Automating Consent," *IEEE Security & Privacy* 16, no. 3 (2018): 65, https://doi.org/10.1109/MSP.2018.2701155

An analogy that clarifies a more holistic view of consent can be taken from the illustration of being offered a cup of tea. If someone is offered a cup of tea, they may agree to the offer and respond in the affirmative. They may also change their mind after responding in the affirmative, deciding not to drink the tea, at which point it should not be forced upon them. They may also respond in the negative to which tea should then not be made or forced upon them at all. If they are unsure of their desire to have a cup of tea, it may still be prepared for them, but they may choose not to drink that cup of tea. Moreover, it would not be expected that they are forced to drink that cup of tea either. An incompetent person is unable to consent to tea because of their inability to comprehend the offer for tea. Similarly, an incapacitated individual is incapable of consenting to tea due to their impairment. If an individual consented to tea prior to becoming incapacitated or deemed incompetent, the tea should not be forced upon them. Along those same lines, an acceptance of tea one day does not translate into a desire for tea every day. Lastly, if someone is given a choice between death or harm and tea, even if tea was chosen from the options that would not be consent, it would be considered coercion at best.[71]

When applied to humanitarian cyberspace in terms of aid recipient data, the consent seems lacking. Data may be requested from recipients of humanitarian aid, and they may respond in the affirmative, consent, and supply that data. For the most part, this is how digital consent has been presented and applied. Aid recipients may also change their minds after responding in the affirmative, deciding not to supply the data, at which point it should not be forced upon them. They may also respond in the negative to which they should then not be forced to supply the requested data. If recipients are unsure about supplying their personal data, they may take some

71. Adapted from Emmeline May and Blue Seat Studios, “Tea Consent (Clean),” YouTube Video, May 13, 2015, https://youtu.be/fGoWLWS4-kU

time to weigh their options and decide not to supply their personal data, and it should not be expected that they would provide that data simply because they took the time to consider the request. It remains true that an incompetent person is unable to consent to a request for data as they would be unable to comprehend the request fully. Similarly, an incapacitated individual is incapable of consenting to a request for data due to their impairment. This speaks to humanitarian interactions with children, but more importantly, the online interactions that may be overlooked.

If an individual consented to provide data and, due to an unforeseen circumstance, became incapacitated or deemed incompetent, the data should not be extracted regardless. Along those same lines, an acceptance to provide data on one day does not translate into an agreement for data to be continually provided. This speaks to the duration in which data is kept, how it is used once acquired, and how it is responsibly discarded. Lastly, if someone is given a choice between death and harm or providing their data, even if the option they chose was to provide the requested data, that would not be consent; it would be considered coercion at best. This is where humanitarian organizations must take a deep ethical look at how they interact and request information from vulnerable populations seeking assistance. All the more so when one takes into account how AI systems may collect, store, and process data in ways for which consent may have never been sought.[72] If an individual is not in a position to offer full consent, then another means that does not infringe upon their humanity, autonomy, and privacy should be sought. Applied in research, the National Commission for the Protection of Human Subjects stated that

72. Jones, *AI and the Ethics*, 64.

"the purpose of consent provisions is the protection of autonomy and personal dignity, including the personal dignity of incompetent persons incapable of acting autonomously."[73]

A utilitarian ethical philosophy may seek to do the most good for the most number of people, but any unintentional harm is damaging to the efforts of humanitarian aid. While the axiom of humanitarian aid may be to do no harm while alleviating human suffering, the ethical axiom must include a refrain from unintended harm. In addition to tracking, exploitation, and abuse of aid recipient data, humanitarian organizations must also consider the collateral effects of adopting a system that relies too heavily upon technology. Systems that produce harm, though unintentional, still remain responsible for the consequences of their actions.

The future-thinking ethical deliberation necessary to apply cutting-edge technology in humanitarian cyberspace goes beyond utilitarian and deontological ethics. As described earlier, a utilitarian ethic is concerned with how things turn out, while a deontological ethic is concerned about how the results were achieved.[74] Both of those perspectives require reflection or retrospection to determine if the results, actions, or intent behind the actions were indeed ethical. In respect to emerging technologies, especially within the humanitarian aid realm, the luxury of retrospective analysis is attenuated by the maxim to "do no harm," digital harm included.

As such, humanitarian cyberspace should apply more proactive ethical models that are forward-looking. A character-oriented approach attempts to address the ethical challenges presented by emerging technologies by asking who or what kind of entity should this

---

73. Franklin Miller and Alan Wertheimer, eds, *The Ethics of Consent: Theory and Practice* (Oxford University Press, 2010), 59.

74. Lawrence M. Hinman, *Ethics: A Pluralistic Approach to Moral Theory*, (Boston, MA: Wadsworth, 2013), 125-126, 161-163.

humanitarian organization become within humanitarian cyberspace?[75] The answer to that question should point back to the values reflected through the humanitarian principles of neutrality, impartiality, independence, and humanity. The ways in which technology may be employed will either allow the organization to ordinate toward those principles or promote misalignment away from those principles.

Over the years, several humanitarian technological tools have been introduced that proved useful in providing access to information during a crisis. Some of these tools include Translators Without Borders, Open Data Kit, Kobo Toolbox, SenseMaker, crowdsourcing, geomatics, and crisis mapping.[76] However, the use of technological tools in the humanitarian space is accompanied by a set of its own challenges, as noted above. Over-reliance on technology without intentional deliberation on impact to core humanitarian principles jeopardizes the valuable relationship between humanitarians and aid recipients.[77] Humanitarian practitioners must realize that any quest to actualize technological solutions "should acknowledge that the application of principles to real-world situations requires experience, self-reflection, and interpretation."[78] Furthermore, humanitarian entities need to understand all of the regulatory measures that apply within the domain they wish to operate, especially in regards to "privacy regulations related to the use and control of personal data."[79] The deliberative,

---

75. Lawrence M. Hinman, *Ethics*, 249.

76. Joe Belliveau, "Humanitarian Access and Technology: Opportunities and applications," *Procedia Engineering* 159, (2016): 301.

77. Belliveau, *Humanitarian Access*, 305

78. McGowan, *Preparing Humanitarians*, 4.

79. Hunt, *Ethics of Emergent*, 242.

reflective aspect of humanitarian technology solutions is an essential exercise for considering the ethical implications and effects to core humanitarian principles a proposed solution may offer.

Proposed Solution

Many of the ethical considerations mentioned will require continuous dialogue, proposed mitigation, and reassessment. Several of the ethical concerns are byproducts of the technology employed to address other challenges like efficiency, capability gaps, and maximized welfare. Be that as it may, it would stand to reason that if technology is responsible for some of the ethical dilemmas presented, then those particular concerns may also be addressed by considering the technology. This does not neglect the reality that is relying too heavily on technology lends itself to less empathic humanitarian service,[80] possibly infringing upon the core principle of humanity. Technology must still be used in a responsible manner, even when used to solve technological challenges. Succinctly put, technological problems may have technological solutions.

One technological remedy may reside in the adaptation of blockchain technologies to address consent and privacy transaction concerns. A blockchain is "basically a peer-to-peer integrated multi-field network framework, composed of cryptography, algorithms, and mathematical expressions aimed at solving traditional distributed database synchronization limitations by using distributed consensus algorithms."[81] Blockchain refers to a "chain of blocks that contains a complete record of transactions that may be publicly or privately distributed

80. Belliveau, *Humanitarian Access*, 305.

81. Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil and Georgia Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives.," *Cryptography* 3, no. 1 (2019): 2, https://www.mdpi.com/2410-387X/3/1/3/pdf

(hence, decentralized) to all users of the chain."[82] The decentralized aspect is based on a trusted protocol between billions of computers around the world that verify the data based on their internal records, which eliminates the need for authentication from a trusted third party.[83] Blockchain technology offers an enhanced security option for transactions by maintaining a digital ledger that provides an extra layer of privacy. [84] Blockchain has been used in various applications in diverse non-monetary systems to include "online voting, decentralized messaging, distributed cloud storage systems, proof-of-location, healthcare and so forth."[85] In healthcare, the blockchain public ledger was successfully used in smart medical systems to discretely share patient data and collaborate with practitioners.[86] The distributed ledger technology has universal visibility[87] and a globalized reach that connects users across the world while "allowing them to carry out cryptograph-enabled, data-secure, decentralized transactions."[88]

The basic components of a blockchain consist of a transaction and a block.[89] The transaction is the "action triggered by the participant," [90] and the block within the blockchain

---

82. Jaideep Ghosh, "The Blockchain: Opportunities for Research in Information Systems and Information Technology," *Journal of Global Information Technology Management* 22:4 (2019): 236, accessed on May 7, 2021, doi:10.1080/1097198X.2019.1679954

83. Ghosh, *The Blockchain*, 236.

84. Mahdi H. Miraz and Maaruf Ali, "Applications of Blockchain Technology Beyond Cryptocurrency," *Annals of Emerging Technologies in Computing (AETiC)*, 2, no. 1, (2018): 1, http://aetic.theiaer.org/archive/v2n1/p1.pdf

85. Miraz, *Applications of Blockchain*, 2.

86. Ghosh, *The Blockchain*, 239.

87. Ibid., 240.

88. Ibid.

89. Miraz, *Applications of Blockchain*, 2.

90. Ibid.

consists of "a collection of data recording the transaction and other associated details such as the correct sequence, timestamp of creation,"[91] and other details. The blockchain may be either public or private, where the public blockchain allows all users with the proper permissions access to it, and a private blockchain limits the "access to selected trusted participants only, with the aim to keep the users' details concealed."[92] As such, blockchain technologies may improve privacy by leveraging "decentralization, persistency, anonymity, and auditability."[93] Following each transaction in a blockchain, "the information stored on the distributed ledger is replicated over all the blockchain nodes."[94] A node is the connection point for blockchain and the user, generally represented by a computer, that can verify transactions through communication with other nodes.[95] In essence, the node is able to compare information across the network to verify authenticity, based on its own copy of the data, in relation to the other copies. This consensus mechanism is derived from a cryptographic algorithm referred to as proof of work, or PoW,[96] and is decentralized due to the peer-to-peer network verification process. In order for there to be a new transaction added to an existing blockchain, the data "has to be validated by all the participants of the relevant Blockchain ecosystem."[97] New data is added to the chain, instead of

91. Ibid.

92. Ibid.

93. Md Mehedi Hassan Onik, Chul-Soo Kim, Nam-Yong Lee, and Jinhong Yang, "Privacy-Aware Blockchain for Personal Data Sharing and Tracking," *Open Computer Science* 9, no. 1 (2019): 83, https://doi.org/10.1515.comp-2019-0005

94. Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen, "Differential Privacy in Blockchain Technology: A Futuristic Approach," *Journal of Parallel and Distributed Computing* 145, (2020): 50.

95. Onik, *Privacy-Aware Blockchain*, 83.

96. Ghosh, *The Blockchain*, 237.

97. Miraz, *Applications of Blockchain*, 2.

replacing any particular block of data on the chain; thus, a record of all transactions is maintained. Figure 1 illustrates the blockchain transaction.[98]

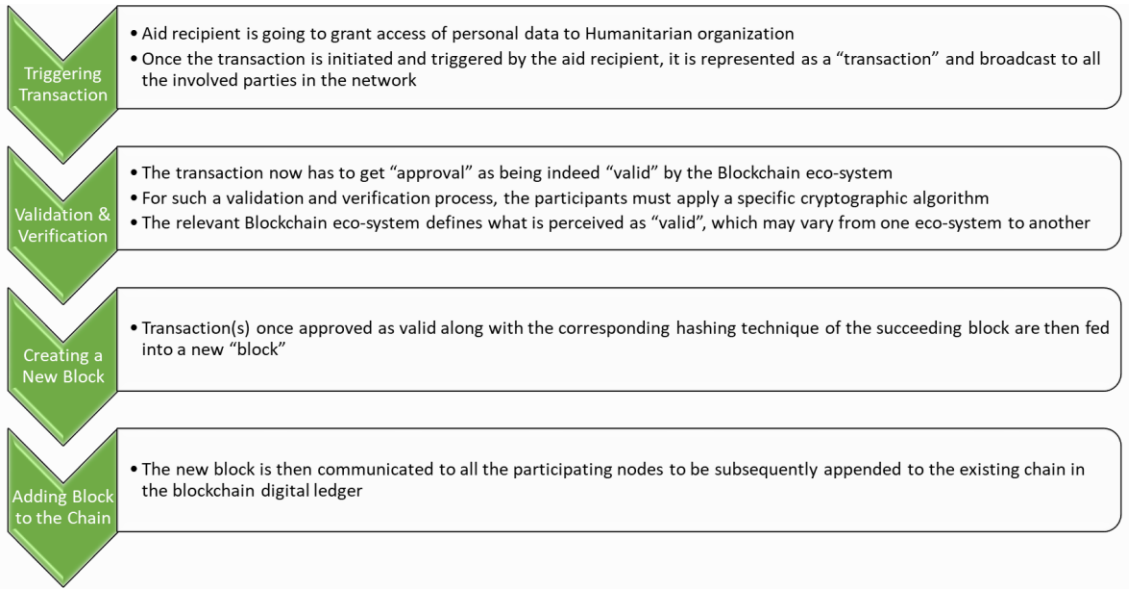


Figure 1. Blockchain Operation[99]

There are six elements to blockchain technology that contribute to the trust mechanism of the technology. Those key elements are: "decentralized, transparent, immutable, autonomy, open-source, and anonymity (as described in Table 1)."[100] The combination of these key elements provides for privacy through the anonymity element while instilling faith in the accuracy of the system for users to interact, given the checks and balances of the immutable element.

98. Ibid.

99. Adapted from Mahdi H. Miraz and Maaruf Ali, "Applications of Blockchain Technology beyond Cryptocurrency", *Annals of Emerging Technologies in Computing (AETiC)*, 2, no. 1, (2018): 1, http://aetic.theiaer.org/archive/v2n1/p1.pdf

100. Siyal, *Applications of Blockchain*, 2.

Table 1. Key elements of blockchain technology, 2019.[101]

Key Elements	Functionality Description
Decentralized	A database system with open access control to anyone connected to the network. The data can be accessed, monitored, stored, and updated on multiple systems.
Transparent	The recorded and stored data on blockchain is transparent to potential users, which can be further updated easily. The transparent nature of blockchains could certainly prevent data from being altered or stolen.
Immutable	The records, once stored, become reserved forever and cannot be modified easily without having control of more than 51% of the node concurrently.
Autonomy	The blockchain system is independent and autonomous, meaning that each node on the blockchain system can access, transfer, store, and update the data safely, making it trustworthy and free from any external intervention.
Open Source	The blockchain technology is formulated in a way that provides an open source access to everyone connected to the network. This inimitable versatility entitles anyone, not only to check the records publicly, but also develop various impending applications.
Anonymity	As data transfer occurs between node to node, the identity of the individual remains anonymous, thus making it a more secure and reliable system.

Blockchain technology is currently used in several sectors in various ways. Some of those applications include saving and verifying legal documents through distributed ledger technologies (DLTs)[102] or a "World Wide Ledger,"[103] which may include smart contracts that cover deeds (also referred to as smart deeds), various certificates, healthcare data, the Internet of Things (IoT), and Cloud operations.[104] The additional applications include real estate transactions, "records of legal and public proceedings, such as marriage and birth certificates,

101. Ibid.

102. Giulio Coppi and Larissa Fast, *Blockchain and Distributed Ledger Technologies in the Humanitarian Sector*, HPG Commissioned Report, 2019, London: Overseas Development Institute, 5, accessed on May 14, 2021 at http://hdl.handle.net/10419/193658

103. Miraz, *Applications of Blockchain*, 3.

104. Siyal, *Applications of Blockchain*, 5.

court notices, registration and sale deeds,"[105] other "hard assets, such as gold, diamonds, and vehicles,"[106] with "real-time record updates, decentralization and disintermediation, and persistency."[107]

More specific examples of blockchain technology implementation in non-crypto currency domains include the "fields of medicine, genomics, telemedicine, tele-monitoring, e-health, neuroscience, and personalized healthcare applications."[108] Electronic Health Records (EHR) have seen blockchain implementations through MedRec, to manage the privacy and security of patient's data.[109] Similar initiatives include the Neurogress system in the neuroscience field[110] and a Hyperledger Fabric initiative in the pharmaceutical research industry that uses a digital drug control system (DDCS) to track production, location, and traceability to the end-users. [111] Hyperledger Fabric is a permissioned blockchain meaning it is designed "where participants in the network are predefined for read/write actions and forever identify within the system."[112] Ra et al. proposed "an anonymous protocol that features improved user privacy in permissioned

105. Ghosh, The Blockchain, 236.

106. Ibid.

107. Ibid.

108. Siyal, *Applications of Blockchain*, 2.

109. Ibid., 6.

110. Ibid., 8.

111. Ibid., 9.

112. Ahmed Raza Rajput, Qianmu Li, and Milad Taleby Ahvanooey, "A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition," *Healthcare* 9, no. 2 (2021): 206. https://www.mdpi.com/2227-9032/9/2/206/pdf

blockchains and fulfills the requirements of anonymity, linking, and user identification."[113] Similarly, Onik et al. proposed a consensus mechanism blockchain-based personally identifiable information management system (BcPIIMS) as a private blockchain using off-the-chain storage to move personally identifiable information (PII), potential personally identifiable information (PPII), and non-personally identifiable information (NPII) that requires consent before any private data is being analyzed providing accountability to offer and confirm data withdrawal or deletion.[114]

Specifically, within the humanitarian domain, there have been several uses of blockchain DLT. The World Food Programme's Building Blocks utilized Ethereum for voucher-based transfers of cash that were "more efficient, transparent and secure, and to improve collaboration across the humanitarian system."[115] World Vision International Nepal Innovation Lab created Sikka, also using Ethereum, "to address the challenge of financial access during times of crises for financially marginali[z]ed and in-need communities."[116] Helperbit used Bitcoin to create a "decentralized, parametric peer-to-peer insurance service and donation system (multi-signature e-wallet) to change practices of humanitarian assistance both before and after an emergency."[117] Lastly, through Red Rose, the IFRC and Kenya Red Cross implemented the Blockchain Open Loop Payments Pilot Project "to explore how blockchain could increase the transparency and

113. Gyeongjin Ra, Deahee Seo, Md Zakirul Alam Bhuiyan, and Imyeong Lee, "An Anonymous Protocol with User Identification and Linking Capabilities for User Privacy in a Permissioned Blockchain," *Electronics* 9, no. 8 (2020): 2, https://www.mdpi.com/2079-9292/9/8/1183/pdf

114. Onik, *Privacy-Aware Blockchain*, 81.

115. Coppi, *Blockchain and Distributed*, viii.

116. Ibid.

117. Ibid.

accountability of cash transfer program[s], including in relation to self-sovereign digital identities."[118]

The implementation of blockchain technology systems in the humanitarian domain is often touted for the transparency and trust assets; however, at the systems level, "improved efficiency, bureaucracy and project cost savings brought about by DLTs have proved to be more important for humanitarian actors."[119] Nevertheless, too often, technology is held as a panacea to cure what ails the sectors in which they are applied.[120] Though blockchain technology may present some solutions to the issues that have been previously raised, there are additional considerations that must also be taken into account.

First, the humanitarian sector must contemplate how unintentional bias, biases, and assumptions are embedded into technology and the assumptions attributed to these tools.[121] By addressing those challenges first, organizations will be in a better position to make informed decisions and mitigate the identified risks.[122] One of those assumptions centers around digital access and an abundance of the resources necessary to keep the access available. Consideration must be given to populations that experience constant shutdowns or where a poor energy infrastructure results in frequent brownouts are common, which limit and reduce the network availability necessary to sustain access to DLT blockchain transactions.[123] This constraint is in

---

118. Ibid.

119. Ibid., 1.

120. Andrej Zwitter and Mathilde Boisse-Despiaux, "Blockchain for Humanitarian Action and Development Aid," *Journal of International Humanitarian Action* 3, no. 1 (2018): 5, https://jhumanitarianaction.springeropen.com/track/pdf/10.1186/s41018-018-0044-5.pdf

121. Coppi, *Blockchain and Distributed*, 1.

122. Ibid.

123. Zwitter, *Blockchain for Humanitarian*, 5.

addition to the lack of resources necessary to keep the computers, servers, and other hardware from operating due to the lack of constant and reliable electricity. [124]

Another consideration is how the implementation of this technology will continue inequitable trends already in practice. For instance, with regards to women and girls in low-income countries, women do not have the same access to a foundational ID (15% higher deficit than men), and worldwide, women are disproportionately more unbanked than men (12 percent deficit).[125] A blockchain DLT technology that is applied without addressing these inequities will only serve to exacerbate the pre-existing inequity. Coppi and Fast noted that blockchain DLT programs tend to have a reformative vice transformative approach that risks "reproducing many of the underlying power dynamics, hierarchical structures, funding flows and deployment strategies that already exist."[126] For women and girls, this would serve to broaden the inequality gap, thus increasing their exposure to neglect, poverty, and violence.

Finally, the greatest challenge to the implementation of any new technology is the human factor. Recognizing this quandary, Disberse partnered with the Start Network, Dorcas Aid International, and Trócaire to create a blockchain DLT pilot program with the purpose of increasing the humanitarian community's comfortability with the new technology.[127] The human element and the margin for "clerical error" must also be accounted for and even expected. While no system can be expected to be completely foolproof, there are measures that can be put in

---

124. Ibid.

125. Theresia Thylin and María Fernanda Novelo Duarte, "Leveraging Blockchain Technology in Humanitarian Settings–Opportunities and Risks for Women and Girls," *Gender & Development* 27, no. 2 (2019): 321, https://doi.org/10.1080/13552074.2019.1627778

126. Coppi, *Blockchain and Distributed*, 1.

127. Coppi, *Blockchain and Distributed*, viii.

place ahead of time to mitigate the risks inherent in the human factor. Part of that risk is in acknowledging that the absence of the human factor may also reduce interactions with affected populations, limiting the opportunities to read the pulse on the ground. As a result, the reduced interaction with beneficiaries may remove occasions to implement complementary programming or risk assessments.[128] Foreknowledge of these possibilities, however, does afford the chance to formulate viable contingencies.

The first consideration in the adoption of any new technology to solve a perceived problem is to invite the communities affected by the problem to have a seat at the table. Including impacted communities, aid recipients, end-users, and humanitarian organization members together at the table will ensure that the proper itch is being scratched in a way that is feasible and sustainable. Having the end-users involved in the conceptualizations will prevent past missteps of introducing technological solutions into impacted communities.[129] The process must inform end-users of potential impacts that the technology may have on the community with "clear roles and responsibilities for all stakeholders."[130] Furthermore, this mechanism should also include grievance and reparation policies as humanitarian organizations seek to "do no digital harm."[131] Additionally, it is vital to have marginalized communities represented at the table, specifically women and girls, being actively involved "at every step along the way, from the identification of problems and potential solutions, to the design and implementation of projects."[132] This intentionality should be accompanied by strategies to mitigate the gender

128. Thylin, *Leveraging Blockchain*, 330.

129. Coppi, *Blockchain and Distributed*, 2.

130. Ibid.

131. Ibid.

132. Thylin, *Leveraging Blockchain*, 330.

inequity and resolve to have women and girls represented at each of the various stages from concept, development, implementation, and re-evaluation. [133] Some vital questions should address the specific purpose, balance of benefits and scaling cost, necessary features, immutability requirements, compliance with the law and humanitarian principles, and how to implement the right to be forgotten.[134]

Vannini, Gomez, and Clayton offer the following "Mind the Five" privacy-aware considerations of vulnerable populations for HIAs.[135] The main guidance is to exercise prudence, protect and secure information from and about migrants, provide training, share-alike, and practice non-discrimination.[136] When the adapted "Mind the Five" guidelines in Figure 2 are paired with a feasible blockchain DLT technology such as the Onik et al. proposed BcPIIMS consensus mechanism, a viable smart contract solution emerges that can handle PII, PPII, NPII, requiring consent for private data analysis, providing accountability, and the ability to withdraw consent to delete the user-owner data per the GDPR.

---

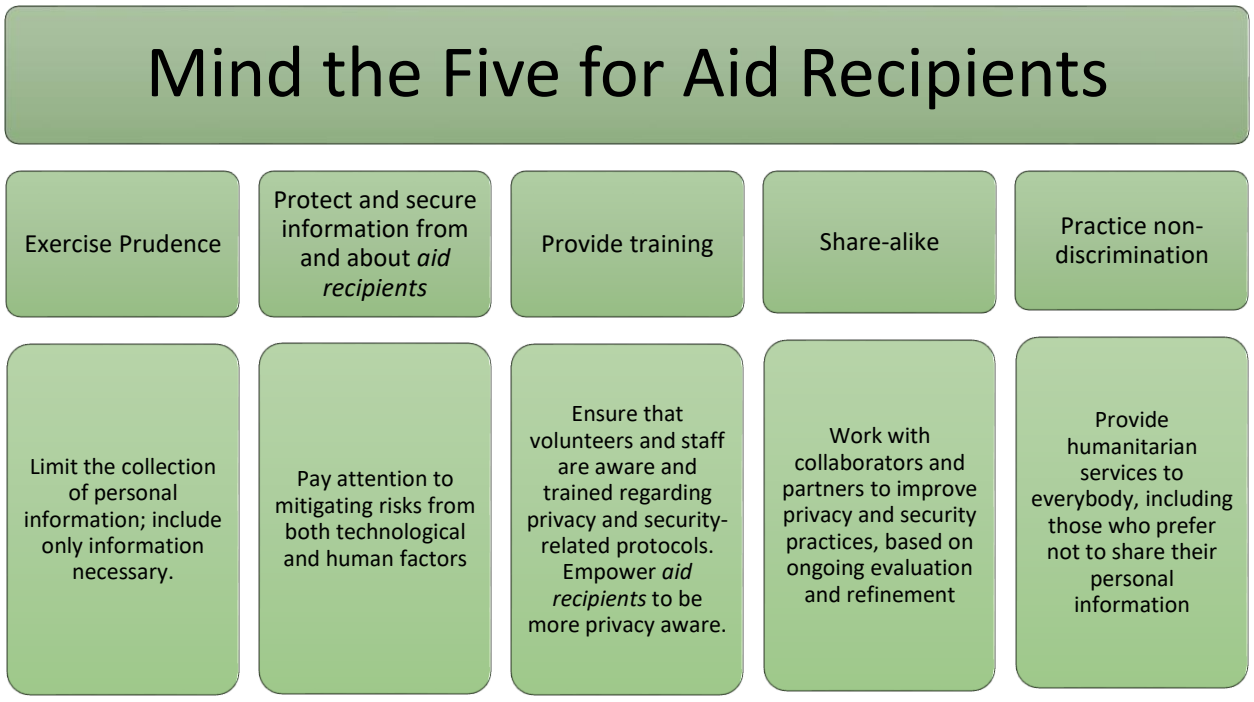
133. Ibid., 331.

134. Zwitter, *Blockchain for Humanitarian*, 5-6.

135. Sara Vannini, Ricardo Gomez, and Bryce Clayton Newell, "'Mind the Five': Guidelines for Data Privacy and Security in Humanitarian Work with Undocumented Migrants and Other Vulnerable Populations," *Journal of the Association for Information Science and Technology* 71, no. 8 (2020): 9, https://doi.org/10.1002/asi.24317

136. Vannini, *Mind the Five*, 9.

Figure 2. Adapted from Mind the Five, 2019[137]



A humanitarian aid-driven privacy-aware BcPIIMS protocol may grant aid recipients more control over how their data is accessed, used, managed, moved, and relinquished. The BcPIIMS is a more privacy-friendly blockchain technique that combines on-chain and off-chain storage refraining from storing personal data on the blockchain, thus allowing blockchain transactions to serve as "mere pointers or other access control mechanisms to more readily"[138] manage the storage solution. This mitigation may help address the ethical challenges surrounding

137. Vannini, *Mind the Five*, 10.

138. Pritesh Shah, Daniel Forester, Davis Polk, Matthias Berberich, and Carolin Raspé, "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies," *Practical Law* (2019), 7, https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf

the mishandling of aid recipient data that may be exploited for surveillance, retributive actions, or mere capitalistic purposes.[139]

Conclusion

As humanitarian assistance enters deeper into the humanitarian cyberspace domain, careful consideration must be given to how aid recipient data is requested, received, maintained, used, and disregarded. The onus remains with humanitarian organizations to reflect the humanitarian principles of neutrality, impartiality, independence, and humanity. While crowdsourced data may present various benefits to humanitarian aid work, caution must also be exercised when an over-reliance on technology may disproportionately affect those in need of assistance. Thoughtful attention should also be devoted to ways in which to include community members, stakeholders, intended aid recipients, and humanitarians together at the table from the conception stage of any proposed technology and throughout the implementation and evaluation processes. Inclusion methodologies should intentionally seek out marginalized populations, such as women and girls, to be a part of the technological solutions discussion. A practical idea raised in this research is the adaptation of a humanitarian aid-driven privacy-aware BcPIIMS protocol to help protect the privacy of aid recipients and increase their conscious volitional consent. Holding true to the humanitarian principles should include doing "no digital harm," even when unintentional while doing good.

139. Mark Duffield, Post-Humanitarianism: Governing Precarity in the Digital World, (Woboken, NJ: John Wiley & Sons, 2018).

Epilogue

It was a typical day filled with regular morning preparation tasks. A younger preadolescent sibling is getting ready for school, donning the issued uniform. Upon departing their apartment complex, an abrupt explosion occurs at an adjacent building sending the vicinity into dismay. Shortly thereafter, it is revealed that the city is under attack, and the morning's assault has separated this younger sibling from their family. An older sibling sets out among the rubble in an attempt to reunite with the family.

The buildings are devastated by the ongoing shelling. Reports indicate that the random indiscriminate killing of women and children is prevalent. Further complicating reunification efforts is a natural disaster that brings flooding to the region. Dejectedly, no familiar discernable faces are found during the initial search. However, still having possession of a mobile phone, a call is attempted. After trying several locations to acquire connectivity, it becomes more readily apparent that the networks have failed. Still searching for any family or a signal, this older sibling runs into a friend that informs them that the only known place with accessible internet connectivity is located several kilometers outside of town, at the military base. Still hopeful of tracking down their family, the older sibling chooses to stay in town and continue the search.

The pursuit is unsuccessful. Another attempt is made with the mobile phone to reach someone by sending a message this time. Yet, similar to the previous efforts, no signal connectivity is available. The futile attempts lead to the decision to venture from the town towards the military base, hoping to establish a means of connection. The journey takes nearly two hours, and the procession of people with similar travel plans accumulates to form a small caravan on the way to the base. Fortunately, the older sibling is able to arrive at the military base without any additional complications.

There are more familiar faces at the military base as people attempt to charge their devices and connect with their loved ones through the internet access point. Relievedly, the older sibling learns that their parents are also at the base and reunites with them. Unpropitiously though, the older sibling is informed that their younger sibling remains missing. A few friends notify the older sibling that an online social media group is available to assist people with locating their loved ones separated by these exigent circumstances. After connecting to the base's wireless network, the older sibling decides to join the social media group and post a photo of the younger sibling and the last place seen.

The older sibling receives several responses after posting the photo and last known location of the missing younger sibling to the site. Some of the messages did not provide any assistance. Far too many of the replies were filled with vitriol and content advocating for continued assaults against the civilian groups and other suggestions of implied genocidal violence. Despite that, one message managed to offer some insight about a temporary installation set up by the International Red Cross and Red Crescent Movement to help families find missing members. A follow-on message indicates that the younger sibling is located at this temporary International Red Cross and Red Crescent Movement facility near the town hall.

Concerningly, the hateful rhetoric on the social media chat board continues and grows more intense. A few explicit and disconcerting replies emote the threat of violence linked to the confirmed knowledge of the whereabouts of the younger sibling and similarly displaced persons. *Having received confirmation that the younger sibling is located at the IRC facility, the older sibling withdraws the photo and location from the site that was posted using a humanitarian aid-driven privacy-aware BcPIIMS protocol.* The banter on the site ranges from apathy and indifference to hate speech and vehement threats. Apprehensive about the vulnerability of the

younger sibling, the elder sets out back to the town to retrieve their sibling and ensure their safety.

The town appears to be in greater disarray. The contemporary crisis coupled with web-based frictions has fueled tensions. Several armed groups have taken to the streets with multiple clashes and hostilities, reflecting the overspill of the hate-filled online bigotry. Undeterred by the growing turmoil, the siblings reconnect and venture back toward the military base, only to find it under attack. During the unanticipated onslaught, the younger sibling is injured. The most prudent course of action is to take the younger sibling to the next closest town. There the older sibling locates a bar establishment with an available open Wifi signal. *Using the humanitarian aid-driven privacy-aware BcPIIMS protocol, the sibling establishes a connection and locates multiple medical service resources,* but they are all located across the border.

At the border, the border patrol requests identification. Fingerprints and the mobile phone are the only identifying items the older sibling possesses. To gain entry en route to the medical services site, the older sibling supplies the fingerprints and phone in compliance with the border patrol's request. Following the fingerprint and phone scans, *the border patrol confirms the identity of the older sibling*. The older sibling is connected to a local community organization that is able to step in and secure critical medical care for the younger sibling. The organization also successfully intercedes with the border patrol on behalf of the *siblings*. Additionally, the organization provides the siblings with sim cards to maintain communication in case of involuntary separation. Eventually, the siblings *are able to reunite with their family, and they all*

apply for asylum, where they await the request approval together, having survived the life-altering events of the past couple of days.[140]

140. Adapted from International Movement, ed, "Humanitarian Crises Digital Dilemmas," Digital Dilemmas, accessed May 7, 2021, http://www.digital-dilemmas.com/

Bibliography

Belliveau, Joe. “Humanitarian Access and Technology: Opportunities and Applications.” *Procedia Engineering* 159, (2016): 300-306. https://doi.org/10.1016/j.proeng.2016.08.182

Broussard, Grant, Leonard S. Rubenstein, Courtland Robinson, Wasim Maziak, Sappho Z. Gilbert, and Matthew DeCamp. “Challenges to Ethical Obligations and Humanitarian Principles in Conflict Settings: A Systematic Review.” *Journal of International Humanitarian Action* 4, no. 1 (2019): 1-13. https://doi.org/10.1186/s41018-019-0063-x

Cameron, Andrea H. *Civil-Military Cooperation In Humanitarian Response: An International Practices Approach*. PhD diss., Naval Postgraduate School, Montery, CA, 2020.

Coppi, Giulio, and Larissa Fast. *Blockchain and Distributed Ledger Technologies in the Humanitarian Sector*. London: Overseas Development Institute, 2019. http://hdl.handle.net/10419/193658

“Defining Humanitarian Assistance.” Global Humanitarian Assistance. accessed May 31, 2021. http://www.globalhumanitarianassistance.org/data-guides/defining-humanitarian-aid./.

Duffield, Mark. *Post-Humanitarianism: Governing Precarity in the Digital World*. Hoboken, NJ: John Wiley & Sons, 2018.

Eberle, Edward J. “Human dignity, privacy, and personality in German and American constitutional law.” *Utah L. Rev.* (1997): 963.

Floridi, Luciano. “On Human Dignity as a Foundation for the Right to Privacy.” *Philosophy & Technology* 29, no. 4 (2016): 307-312.

Ghosh, Jaideep. “The Blockchain: Opportunities for Research in Information Systems and Information Technology.” *Journal of Global Information Technology Management* 22, no. 4 (2019): 235-242. https://doi.org/10.1080/1097198X.2019.1679954

Greenwood, Faine, Caitlin Howarth, Danielle Escudero Poole, Nathaniel A. Raymond, and Daniel P. Scarnecchia. “The Signal Code: A Human Rights Approach to Information During Crisis,” *Harvard Humanitarian Initiative*, (2017).

Harsono, Hugh. “HA/DR: A Case Study for Potential Bilateral U.S.-China Interoperability.” WAR ROOM: November 19, 2019. https://warroom.armywarcollege.edu/articles/ha-dr-sof/

Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. “Differential Privacy in Blockchain Technology: A Futuristic Approach.” *Journal of Parallel and Distributed Computing* 145 (2020): 50-74. https://arxiv.org/pdf/1910.04316.pdf

Hinman, Lawrence M. *Ethics: A Pluralistic Approach to Moral Theory*. Boston, MA: Wadsworth, 2013.

Hunt, Matthew, John Pringle, Markus Christen, Lisa Eckenwiler, Lisa Schwartz, and Anushree Davé. “Ethics of Emergent Information and Communication Technology Applications in Humanitarian Medical Assistance.” *International Health* 8, no. 4 (2016): 239-245. https://doi.org/10.1093/inthealth/ihw028

Ishmaev, Georgy. “The Ethical Limits of Blockchain-Enabled Markets for Private IoT Data.” *Philosophy & Technology* 33, no. 3 (2020): 411-432. https://link.springer.com/content/pdf/10.1007/s13347-019-00361-y.pdf

Joint Force Development. *Foreign Humanitarian Assistance: Joint Publication 3-29.* Washington: DC: Department of Defense 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_29.pdf.

Jones, Meg Leta, Ellen Kaufman, and Elizabeth Edenberg. “AI and the Ethics of Automating Consent.” *IEEE Security & Privacy* 16, no. 3 (2018): 64-72. https://doi.org/10.1109/MSP.2018.2701155

Koh Hongju, Harold. “International Law in Cyberspace.” Harvard International Law Journal 54, (December 2012): 1-12. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

Laraby, Patrick R., Margaret Bourdeaux, S. Ward Casscells, David J. Smith, and Lynn Lawry. “Humanitarian Assistance and Disaster Relief: Changing the Face of Defense.” *American Journal of Disaster Medicine* 4, no. 1 (2009): 33-40.

May, Emmeline and Blue Seat Studios. “Tea Consent (Clean).” May 13, 2015. YouTube Video. [2:49]. https://youtu.be/fGoWLWS4-kU

McGowan, Catherine R., Louisa Baxter, Marc DuBois, Julian Sheather, Ruma Khondaker, Rachael Cummings, and Kevin Watkins. “Preparing Humanitarians to Address Ethical Problems.” *Conflict and Health* 14, no. 1 (2020): 1-7.

Meier, Patrick. *Digital Humanitarians: How Big Data is Changing the Face of Humanitarian Response*. (Boca Raton, FL: CRC Press, 2015).

Miller, Franklin, and Alan Wertheimer, eds. *The Ethics of Consent: Theory and Practice*. Oxford University Press, 2010.

Miraz, Mahdi H., and Maaruf Ali. “Applications of Blockchain technology beyond cryptocurrency.” *Annals of Emerging Technologies in Computing (AETiC)*, 2, no. 1, (2018): 1, http://aetic.theiaer.org/archive/v2n1/p1.pdf

Mohsin Al-Janabi, Zahraa Khaleel, Pascal Perrot, Yannick Heiniger, and Claudiu Mateescu. “Catalogue of Experiences.” Digital Dilemmas. http://www.digital-dilemmas.com/sites/default/files/downloads/cicr_catalogue_prod.pdf

Moroney, Jennifer DP, Stephanie Pezard, Laurel E. Miller, Jeffrey G. Engstrom, and Abby Doll. *Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region.* (Santa Monica, CA: RAND Corporation, 2013). https://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR146/RAND_RR146.sum.pdf

Nakamoto, Satoshi. “Bitcoin: What’s in the Whitepaper?” (2008). https://huobi-1253283450.cos.ap-beijing.myqcloud.com/1543476765952_IgOT7VVGO4Vr3QUjymBa.pdf

O’Mahony, Conor. “There is No Such Thing as a Right to Dignity.” *International Journal of Constitutional Law* 10, no. 2 (2012): 551-574.

Onik, Md Mehedi Hassan, Chul-Soo Kim, Nam-Yong Lee, and Jinhong Yang. “Privacy-Aware Blockchain for Personal Data Sharing and Tracking.” *Open Computer Science* 9, no. 1 (2019): 80-91. https://doi.org/10.1515.comp-2019-0005

Ra, Gyeongjin, Deahee Seo, Md Zakirul Alam Bhuiyan, and Imyeong Lee. “An Anonymous Protocol with User Identification and Linking Capabilities for User Privacy in a Permissioned Blockchain.” *Electronics* 9, no. 8 (2020): 1183. https://www.mdpi.com/2079-9292/9/8/1183/pdf

Rajput, Ahmed Raza, Qianmu Li, and Milad Taleby Ahvanooey. “A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition.” *Healthcare* 9, no. 2 (February 2021): 206. https://www.mdpi.com/2227-9032/9/2/206/pdf

Sandoz, Yves. “The International Committee of the Red Cross as Guardian of International Humanitarian Law.” International Committee of the Red Cross, December 31, 1998. https://www.icrc.org/en/doc/resources/documents/misc/about-the-icrc-311298.htm

Sandvik, Kristin Bergtora. “The Humanitarian Cyberspace: Shrinking Space or an Expanding Frontier?.” *Third World Quarterly* 37, no. 1 (2016): 17-32. http://dx.doi.org/10.1080/01436597.2015.1043992

Searls, Martin Stanley. “Is Use of Cyber-Based Technology in Humanitarian Operations Leading to the Reduction of Humanitarian Independence?.” (S. Rajaratnam International Studies, June 11, 2018). https://think-asia.org/bitstream/handle/11540/8711/WP315.pdf

Shah, P., D. Forester, D. Polk, M. Berberich, and C. Raspé. “Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies.” *Practical Law* (2019): 1-8. https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf

Siyal, Asad Ali, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil, and Georgia Soursou. “Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives.” *Cryptography* 3, no. 1 (2019): 3. https://www.mdpi.com/2410-387X/3/1/3/pdf

Smith, Brad. “The Need for a Digital Geneva Convention.” *Microsoft On the Issues*. February 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv.

Steinmann, Rinie. "The Core Meaning of Human Dignity." *PER: Potchefstroomse Elektroniese Regsblad* 19, no. 1 (2016): 1-32. http://dx.doi.org/10.17159/1727-3781/2016/v19i0a1244

Stoddard, Abby, Adele Harmer, and Victoria DiDomenico. “Providing Aid in Insecure Environments: 2009 Update.” *HPG Policy Brief* 34, no. 10 (2009).

Thylin, Theresia, and María Fernanda Novelo Duarte. “Leveraging Blockchain Technology in Humanitarian Settings–Opportunities and Risks for Women and Girls.” *Gender & Development* 27, no. 2 (2019): 317-336. https://doi.org/10.1080/13552074.2019.1627778

United Nations. General Assembly. *Universal Declaration of Human Rights*. Vol. 3381. Department of State, United States of America, 1949. https://www.un.org/en/about-us/universal-declaration-of-human-rights

"UPTEMPO: The United States and Natural Disasters in the Pacific." New America. Accessed May 14, 2021. https://www.newamerica.org/resource-security/reports/uptempo-united-states-and-natural-disasters/part-ii-military-humanitarian-and-disaster-relief-response-capacity-in-the-indo-pacific-region/.

Vannini, Sara, Ricardo Gomez, and Bryce Clayton Newell. "'Mind the Five': Guidelines for Data Privacy and Security in Humanitarian Work with Undocumented Migrants and Other Vulnerable Populations." *Journal of the Association for Information Science and Technology* 71, no. 8 (2020): 927-938. https://doi.org/10.1002/asi.24317

Wallace, Amelia. "Protection of Personal Data in Blockchain Technology: An investigation on the compatibility of the General Data Protection Regulation and the public blockchain." (2019). https://www.diva-portal.org/smash/get/diva2:1298747/FULLTEXT01.pdf

Yale Digital Humanities Lab. "Neural Neighbors: Pictorial Tropes in the Meserve-Kunhardt Collection." Beinecke Rare Book & Manuscript Library. Yale University. Accessed May 7, 2021. https://dhlab.yale.edu/neural-neighbors/.

Zwitter, Andrej, and Mathilde Boisse-Despiaux. "Blockchain for Humanitarian Action and Development Aid." *Journal of International Humanitarian Action* 3, no. 1 (2018): 1-7.