

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



HARVARD
HUMANITARIAN
INITIATIVE



Standards and Ethics Series 02

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

Faine Greenwood

Caitlin Howarth

Danielle Escudero Poole

Nathaniel A. Raymond

Daniel P. Scarneccia

This study is a product of the Signal Program on Human Security and Technology at the Harvard Humanitarian Initiative. The authors are listed in alphabetical order.

For their contributions, insight, and review, we would like to extend our special thanks to:

- *Vincenzo Bollettino—Director of the Resilient Communities Program, Harvard Humanitarian Initiative*
- *Stuart Campo—Senior Innovation Deployment Specialist, UNICEF Office of Innovation—Global Innovation Centre*
- *Kate Crawford—Principal Researcher, Microsoft and Senior Research Fellow, New York University*
- *Sean Martin McDonald—CEO, Frontline SMS*
- *Emily Troutman—Independent Journalist*
- *Meredith Whittaker—Open Research Lead, Google*

Our thanks also go to our many reviewers:

- *Jos Berens, LL.M—Data Responsibility Officer at Humanity X and Head of Secretariate at the International Data Responsibility Group*
- *Lucy Bernholz—Director, Digital Civil Society Lab, Stanford Center on Philanthropy and Civil Society*
- *Julia Brooks—Legal Research Associate, Advanced Training Program on Humanitarian Action, Harvard Humanitarian Initiative*
- *Josiah Kaplan—Senior Research Advisor, Elrha*
- *Simon Lambert—Associate Professor, University of Saskatchewan*
- *Stephen Livingston—Senior Fellow, Carr Center for Human Rights Policy, Harvard Kennedy School*
- *Dave Polatty—Director, Humanitarian Response Program, U.S. Naval War College*
- *Gideon Shimshon—Director, Centre for Innovation, Leiden University*
- *Stefan Verhulst—Co-founder and Chief Research and Development Officer, The GovLab at New York University*
- *Tricia Wang—Fellow at Interactive Telecommunications Program at Tisch, New York University and Co-founder, Constellate Data*

Eleanor Roosevelt, speech to the United Nations Commission on
Human Rights, United Nations, New York, March 27, 1958

"Where, after all, do universal human rights begin? In small places, close to home - so close and so small that they cannot be seen on any maps of the world. Such are the places where every man, woman, and child seeks equal justice, equal opportunity, equal dignity without discrimination. Unless these rights have meaning there, they have little meaning anywhere. Without concerted citizen action to uphold them close to home, we shall look in vain for progress in the larger world."

Introduction: The Need for the Code

**Humanitarian
Information Activities**
are defined in this
document as follows:

"Activities and programs which may include the collection, storage, processing, analysis, further use, transmission, and public release of data and other forms of information by humanitarian actors and/or affected communities. HIAs also include the establishment and development of communications capacity and infrastructure by responders and/or populations. These activities occur as part of humanitarian action throughout the response cycle and include, but are not limited to, improving situational awareness; disaster preparedness and mitigation; intervention design and evaluation; connecting populations to response activities and to each other; and supporting ongoing operations, including the delivery of assistance."

In the past decade, humanitarian actors and affected populations alike have integrated advances in information communication technologies (ICTs) and the digital data they produce into humanitarian responses to crises. These crises include natural disasters, armed conflict, other forms of complex emergencies, and political unrest. This adoption and absorption of ICTs and digital data by a diverse ecosystem of actors not only profoundly affects how humanitarian action now occurs, but also fundamentally transforms the very ways that crises unfold in the 21st century and the impacts that these crises have on populations.

However, these operational and technological changes are occurring without an accepted rights-based approach (RBA) for conducting humanitarian information activities (HIAs) in the present era. The authors of this document believe that creating this rights-based approach is essential.

Some in the humanitarian community may assert that the application of an approach based on rights to address the complex issues raised by the intersection of data and information in crises is either limiting or insufficient compared to a more needs-based approach. However, a needs-based approach, when the specific rights relevant to data and information in crises have not been either identified or clarified, is fundamentally impossible.

What's more, humanitarian assistance is not simply about meeting the biological needs of those affected by disasters alone. At its core, the humanitarian project both aspires and adheres to the humanitarian principles—chief among them the belief that all people have a right to life with dignity. The Humanitarian Charter defines "dignity" as:

"...more than physical well-being; it demands respect for the whole person, including the values and beliefs of individuals and affected communities, and respect for their human rights, including liberty, freedom of conscience and religious observance."¹

Therefore, the Harvard Humanitarian Initiative's Signal Program on Human Security and Technology (Signal Program) has created "The Signal Code," with the purpose of identifying,

1. The Sphere Project, *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*, 3rd ed. (Bourton on Dunsmore, Rugby: Practical Action Publishing, 2011).

defining, articulating, and translating existing international human rights standards into the context of HIAs and the use of information, data, and ICTs in humanitarian contexts.

The humanitarian community has faced an equally critical juncture in its history before. In the aftermath of the 1994 Rwandan Genocide, evaluations of the humanitarian response to that crisis found significant gaps in technical and ethical standards for how aid was delivered, including an absence of an agreed-upon RBA for responding to complex emergencies. The result of the acknowledgement of these failures was the Humanitarian Charter and the Minimum Standards in Humanitarian Response, among other reforms. The rights-based approach to humanitarian response was articulated for the first time within the Humanitarian Charter.²

The document below was undertaken on the premise that the humanitarian community now faces an equally pivotal and defining moment requiring a new RBA specific to HIAs. Additionally, this new RBA for HIAs is a key prerequisite for the necessary development of minimum ethical and technical standards for the use of ICTs and data. Minimum ethical and technical standards cannot, and should not be undertaken until there is agreement on the application of existing human rights to these activities.

Some of the rights articulated by the Signal Code are already generally recognized. Other rights identified within the Signal Code as relevant and applying in the context of these information activities exist implicitly within and across multiple recognized sources of rights. While the Signal Code is presented with the aim of being as comprehensive and specific as possible, this document is intended to initiate an iterative debate and process within the humanitarian community around how these rights should be codified and realized. It is the hope of the authors that the resulting

2. Margie Buchanan-Smith et al., “How the Sphere Project Came into Being: A Case Study of Policy Making in the Humanitarian-Aid Sector and the Relative Influence of Research,” *Bridging Research and Policy in Development: Evidence and the Change Process*, no. July (2005), <http://www.odi.org/publications/170-bridging-research-policy-development-evidence-change-process>.

discourse leads to further discussion, research, and doctrine development amongst all actors in the humanitarian space.

The eventual goal of the process the Signal Code seeks to initiate is, in the view of the authors, to enable the creation of obligations and minimum ethical and technical standards for HIAs, grounded in an accepted foundation of human rights standards and international law. These yet-to-be-created technical standards must be based upon obligations for humanitarian practitioners that uphold basic human rights. Both state actors and non-state actors, including non-governmental organizations and private sector entities, have an obligation to protect these rights; to take steps to prevent and sanction their violation and abrogation; and to engage in actions to realize them before, during, and after crises occur.



The foundation of these rights is the idea that information itself, including the means to generate, communicate and receive it, is a basic humanitarian need that should be afforded protection equal to other such traditional needs as food, water, shelter, and medical care. An essential component of information provision as a basic need during crises are HIAs.

The HIAs that this document addresses can be performed by affected communities, humanitarian actors, government actors, and/or other non-state or international actors. They are defined as activities that aim to collect, analyze, process, transmit and communicate, share and publish, and support access to information as part of meeting the humanitarian needs of crisis-affected populations before, during, and/or after crises occur.

Increasing evidence is emerging that HIAs, particularly those employing experimental applications of digital data and ICTs, may in some cases cause harm to vulnerable populations

and violate their basic human rights. In some circumstances, those undertaking HIAs may also be at risk as well.

Duty of care is defined by Collins Dictionary of Law as:

"a requirement that a person act toward others and the public with watchfulness, attention, caution and prudence that a reasonable person in the circumstances would. If a person's actions do not meet this standard of care, then the acts are considered negligent, and any damages resulting may be claimed in a lawsuit for negligence."³

Despite the potential threats and harms that HIAs in the networked age may cause or magnify, the humanitarian community has so far failed to systematically address the critical gaps in theory and practice necessary to effectively mitigate these risks in either a comprehensive or coordinated way. The potential implications of this failure, if unaddressed, jeopardize the appropriate application of core humanitarian principles in the networked age. Additionally, the international humanitarian and human rights laws and standards that fundamentally undergird and define humanitarian action were drafted before the digital revolution. It is crucial that these instruments are translated to the operational contexts that humanitarian actors face and the technologies they now regularly employ to safeguard affected populations from intentional harms and negligence.

The recognition and codification of these rights is required to establish for the humanitarian community its duty of care³ for the populations it affects with HIAs, and thus define a standard of reasonable care for conducting these activities. Absent an agreed duty of care, humanitarian actors are at risk of these questions being resolved in multiple jurisdictions by national courts instead of by the humanitarian community itself.

The impact of ICTs and digital data on humanitarian action has been so profound that developing rights-based ethical and technical standards should no longer be treated as an issue only related to areas such as "humanitarian innovation," "crisis mapping," or "humanitarian data." How challenges stemming from the increasingly central role of HIAs in crisis response are addressed may determine the future of the humanitarian project as a whole more than any other dynamic the field currently faces.

The human rights presented herein as applying to HIAs were identified because they meet all of the following three criteria:

- The rights can be identified as existing within the Universal Declaration of Human Rights (UDHR), currently accepted human rights law such as the International Covenants on Civil and Political

3. *Collins Dictionary of Law*. S.v. "duty of care." Retrieved December 12 2016 from <http://legal-dictionary.thefreedictionary.com/duty+of+care>

- Rights (ICCPR), other instruments of currently accepted human rights law, and international humanitarian law, such as the Geneva Conventions;
- The rights apply to all people and regardless of the use of any specific technology; and
 - The rights reinforce and translate existing bedrock rights adhered to by humanitarian practitioners into the specific context of HIAs.

All human beings have fundamental human rights provided for under the UDHR and other instruments of law. While the UDHR is non-binding, it sets an important standard for the establishment of rights in individual states. The UDHR is invoked so often, and has become so critical to our understanding of universal rights, that many in the legal community defend the document as customary international law. In some cases, the UDHR directly led to the creation of binding laws, which include the International Covenant on Civil and Political Rights. In further iterations of the Signal Code, we hope legal scholars will endeavor to further this discussion. The UN itself, through the International Law Commission, is currently working on recommendations and guidelines for the identification of customary international law and we expect this work to be ongoing.⁴

Further, we acknowledge the situational applicability of both IHL and IHRL. For example, International Humanitarian Law applies only during armed conflict. Similarly, International Human Rights Law may be derogated in certain crises, including conflict. We believe that both IHL and IHRL must be taken into consideration when interpreting the rights to humanitarian information activity. Currently existing legal instruments are not fully adapted to the challenges of the 21st century. Globalization and the rise of new technologies present novel dynamism in the way information is shared, collected, and disseminated.

Although ongoing conflicts or “protracted crises” are increasingly the norm, some conflicts do have a clear beginning and an end. Data, on the other hand, lives forever. It lives outside of traditional state borders and a discrete time and space. Data

4. United Nations General Assembly, “Report of the International Law Commission,” 2016, chap. 5, http://legal.un.org/docs/?path=..//ilc/reports/2016/english/a_71_10.pdf&lang=EFSRAC.

can be collected invisibly, from populations who are not aware. Private information can be shared around the world in an instant. Where clear international law does not exist to address these problems, we refer to other well-established standards of conduct including the Nuremberg Code and the Belmont Report. The Signal Code is an important first step in articulating the human rights relating to information and data. These rights already exist in international standards and law, but may not be clearly articulated because of the era in which they were written. Over time, these rights must become essential and standard, if we are to meet the evolving technological challenges of our era. The legal obligation of states to honor and protect human rights is made clear in Article 1 of the UN Charter.

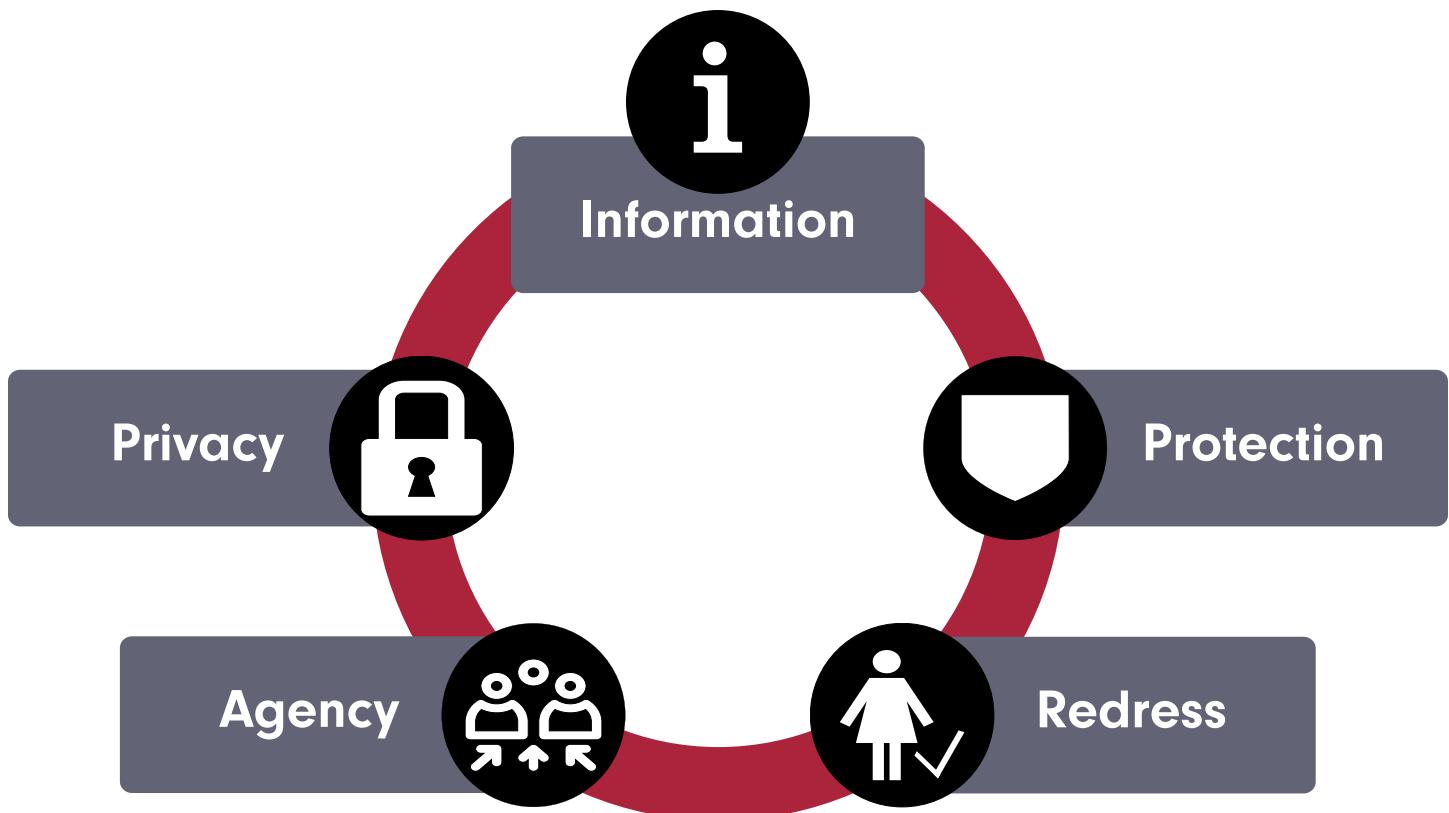
While each right described in this document is distinct, each right is also interconnected and interdependent to the others - both in terms of how they are derived from the UDHR, and how they are realized. In short, none of these rights can be fully realized without the realization of all the other identified rights.

The document below comprises four sections. Section A introduces and lays out existing rights of all people relevant to HIAs. Section B grounds these rights in existing and generally accepted human rights, humanitarian, and international law, doctrine, and standards. Section C defines specific issues addressed by each right, identifying potential harms arising from the failure to realize and respect these rights. Section D proposes a set of general next steps for realizing these rights in theory and practice.

Section A: The Signal Code

Preamble

- A1. The Right to Information**
- A2. The Right to Protection**
- A3. The Right to Data Privacy and Security**
- A4. The Right to Data Agency**
- A5. The Right to Redress and Rectification**



Preamble

Data is, formally, a collection of symbols which function as a representation of information or knowledge. The term **raw data** is often used with two different meanings, the first being uncleaned data, that is, data that has been collected in an uncontrolled environment, and unprocessed data, which is collected data that has not been processed in such a way as to make it suitable for decision making. Colloquially, and in the humanitarian context, data is usually thought of solely in the machine readable or digital sense. For the purposes of the Signal Code, we use the term data to encompass information both in its analog and digital representations. Where it is necessary to address data solely in its digital representation, we refer to it as **digital data**.

Humanitarian action adheres to the core humanitarian principles of impartiality, neutrality, independence, and humanity, as well as respect for international humanitarian and human rights law. These foundational principles are enshrined within core humanitarian doctrine, particularly the Red Cross/NGO Code of Conduct¹ and the Humanitarian Charter.² Together, these principles establish a duty of care for populations affected by the actions of humanitarian actors and impose adherence to a standard of reasonable care for those engaged in humanitarian action.

Engagement in HIAs, including the use of data and ICTs, must be consistent with these foundational principles and respect the human rights of crisis-affected people to be considered “humanitarian.” In addition to offering potential benefits to those affected by crisis, HIAs, including the use of ICTs, can cause harm to the safety, wellbeing, and the realization of the human rights of crisis-affected people. Absent a clear understanding of which rights apply to this context, the utilization of new technologies, and in particular experimental applications of these technologies, may be more likely to harm communities and violate the fundamental human rights of individuals.

The Signal Code is based on the application of the UDHR, the Nuremberg Code, the Geneva Convention, and other instruments of customary international law related to HIAs and the use of ICTs by crisis affected-populations and by humanitarians on their behalf. The fundamental human rights undergirding this Code are the rights to life, liberty, and security; the protection of privacy; freedom of expression; and the right to share in scientific advancement and its benefits as expressed in Articles 3, 12, 19, and 27 of the UDHR.³

The Signal Code asserts that all people have fundamental rights to access, transmit, and benefit from information

1. International Federation of the Red Cross and Red Crescent and International Committee of the Red Cross, “The Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief,” 1994, <http://www.ifrc.org/Global/Publications/disasters/code-of-conduct/code-english.pdf>.
2. The Sphere Project, *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*.
3. United Nations General Assembly, “Universal Declaration of Human Rights,” *United Nations General Assembly Resolutions* 217 A, no. III (December 10, 1948): 71–79.

as a basic humanitarian need; to be protected from harms that may result from the provision of information during crisis; to have a reasonable expectation of privacy and data security; to have agency over how their data is collected and used; and to seek redress and rectification when data pertaining to them causes harm or is inaccurate.

These rights are found to apply specifically to the access, collection, generation, processing, use, treatment, and transmission of information, including data, during humanitarian crises. These rights are also found herein to be interrelated and interdependent. To realize any of these rights individually requires realization of all of these rights in concert.

These rights are found to apply to all phases of the data lifecycle—before, during, and after the collection, processing, transmission, storage, or release of data. These rights are also found to be elastic, meaning that they apply to new technologies and scenarios that have not yet been identified or encountered by current practice and theory.

No right herein may be used to abridge any other right. Nothing in this code may be interpreted as giving any state, group, or person the right to engage in any activity or perform any act that destroys the rights described herein.

The five human rights that exist specific to information and HIAs during humanitarian crises are the following:

The Signal Code

The Right to Protection

All people have a right to protection of their life, liberty, and security of person from potential threats and harms resulting directly or indirectly from the use of ICTs or data that may pertain to them. These harms and threats include factors and instances that impact or may impact a person's safety, social status, and respect for their human rights. Populations affected by crises, in particular armed conflict and other violent situations, are fundamentally vulnerable. HIAs have the potential to cause and magnify unique types of risks and harms that increase the vulnerability of these at-risk populations, especially by the mishandling of sensitive data.



The Right to Information

Access to information during crisis, as well as the means to communicate it, is a basic humanitarian need. Thus, all people and populations have a fundamental right to generate, access, acquire, transmit, and benefit from information during crisis. The right to information during crisis exists at every phase of a crisis, regardless of the geographic location, political, cultural, or operational context or its severity.

The Right to Privacy and Security

All people have a right to have their personal information treated in ways consistent with internationally accepted legal, ethical, and technical standards of individual privacy and data protection. Any exception to data privacy and protection during crises exercised by humanitarian actors must be applied in ways consistent with international human rights and humanitarian law and standards.



The Right to Data Agency

Everyone has the right to agency over the collection, use, and disclosure of their personally identifiable information (PII) and aggregate data that includes their personal information, such as demographically identifiable information (DII). Populations have the right to be reasonably informed about information activities during all phases of information acquisition and use.



The Right to Rectification and Redress

All people have the right to rectification of demonstrably false, inaccurate, or incomplete data collected about them. As part of this right, individuals and communities have a right to establish the existence of and access to personal data collected about themselves. All people have a right to redress from relevant parties when harm was caused as a result of either data collected about them or the way in which data pertaining to them were collected, processed, or used.



A1. The Right to Information

The right to access, generate, communicate, and benefit from information during crisis

Access to information during crisis, as well as the means to communicate it, is a basic humanitarian need. Thus, all people and populations have a fundamental right to generate, access, acquire, transmit, and benefit from information during crisis. The right to information during crisis exists at every phase of a crisis, regardless of the geographic location, political, cultural, or operational context or its severity.

Information, including the means to generate, access, acquire, transmit and benefit from it, must be treated as a humanitarian necessity for the survival and well-being of crisis-affected populations by all actors at all times. Accordingly, information in the context of HIAs should be treated as equal in importance to other forms of humanitarian assistance such as food, water, shelter, physical protection, and medicine, and their equitable delivery should be treated as a core part of fulfilling the humanitarian imperative. The right to information is also critical for the recognition that affected persons and communities are agents of their own protection.

Individuals, organizations, and communities engaged in HIAs, including the systems, processes, and infrastructure they employ as part of these activities, should be afforded protection by all actors. This protection should be equal to the protection afforded to other forms of humanitarian assistance under international human rights standards and humanitarian law. HIAs include efforts by affected populations to request assistance from humanitarian actors and to communicate amongst their own communities, regardless of where they are located and the nature of the crisis.

A2. The Right to Protection

The right to protection from threats and harms resulting from the use of ICTs and data during crisis

All people have a right to protection of their life, liberty, and security of person from potential threats and harms resulting directly or indirectly from the use of ICTs or data that may pertain to them. These harms and threats include factors and instances that impact or may impact a person's safety, social status, and respect for their human rights.

Populations affected by crises, in particular armed conflict and other violent situations, are fundamentally vulnerable. HIAs have the potential to cause and magnify unique types of risks and harms that increase the vulnerability of these at-risk populations, especially by the mishandling of sensitive data.

These unique types of risks and harms include, though are not limited to: gross negligence, including lack of necessary technical capacity or expertise; increasing the ability of actors to target specific populations and individuals for attack; marginalizing specific populations; eroding trust between humanitarian actors and crisis-affected populations; and contributing to the potential exploitation of crisis-affected populations. These risks increase significantly in complex emergencies and conflict settings because of the threat of violence against vulnerable populations by state and non-state actors.

Exploitation as a result of HIAs can be defined as actions that include, though are not limited to: corruption, fraud, and price gouging; non-consensual experimentation; the sale or monetization of a population's data without their consent; and the intentional misuse of data to disproportionately benefit or disadvantage a specific group.

A3. The Right to Privacy and Security



All people have a right to have their personal information treated in ways consistent with internationally accepted legal, ethical, and technical standards of individual privacy and data protection. Any exception to data privacy and protection during crises exercised by humanitarian actors must be applied in ways consistent with international human rights and humanitarian law and standards.

Individuals whose data are collected as part of HIAs have a right to expect that their data are only collected for specified and legitimate humanitarian assistance-related purposes. This right ensures that these data are:

1. processed fairly and lawfully, and not further processed in a way incompatible with that purpose;
2. adequate, relevant, and not excessive in relation to that purpose;
3. accurate and, where necessary, kept up-to-date; and
4. not kept longer than necessary to achieve the stated purpose under which informed consent and/or participation was obtained.

Data encompassed by this right can include both data traditionally defined as personally identifiable information (PII) and any other forms of data that may lead to the identification of individuals or groups of individuals. This right also mandates that care be taken to identify the specific vulnerabilities of persons or groups in relation to particular threats, and to afford them additional protections for the privacy and security of their data as required.

A4. The Right to Data Agency



Everyone has the right to agency over the collection, use, and disclosure of their personally identifiable information (PII) and aggregate data that includes their personal information, such as demographically identifiable information (DII).⁴ Populations have the right to be reasonably informed about information activities during all phases of information acquisition and use.

The right to data agency encompasses the right to protection from non-consensual experimentation, and includes the concepts of informed consent, participation, and notification of data collection and uses.

Everyone has the right to protection from non-consensual experimentation. This right is explicitly articulated in Article 7 of the ICCPR, and is necessary for the realization^{5,6} of both Article 1 of the UDHR, which provides that “All human beings are born free and equal in dignity and rights,” and Article 7 of the Declaration of Helsinki, which states, “Medical research is subject to ethical standards that promote and ensure respect for all human subjects and protect their health and rights.”⁷ As such, everyone has the right to provide voluntary informed consent, consistent with international law and human rights standards, for the use of their PII in all prospective and retrospective applications, including both non-experimental and experimental uses. Informed consent for the acquisition and use of PII is required for the realization of the right to protection from harm resulting from the use of ICTs and data. Populations affected by crises should be extended additional safeguards

4. Nathaniel Raymond, “Beyond ‘Do No Harm’ and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society’s Use of Data,” in *Group Privacy: New Challenges of Data Technologies*, ed. Linnet Taylor, Luciano Floridi, and Bart van der Sloot (Springer International Publishing, 2016), doi:10.1007/978-3-319-46608-8.
5. UNESCO, “Explanatory Memorandum On The Elaboration Of The Preliminary Draft Declaration On Universal Norms On Bioethics,” in *First Intergovernmental Meeting of Experts Aimed at Finalizing a Draft Declaration on Universal Norms on Bioethics* (Paris, 2005), 5, <http://unesdoc.unesco.org/images/0013/001390/139024e.pdf>.
6. UNESCO, “Records of the General Conference,” in *Resolution 15 Adopted by the General Conference at Its 33rd Session*, vol. 1 (Paris, 2005), 74–80, <http://unesdoc.unesco.org/images/0014/001428/142825e.pdf#page=80>.
7. World Medical Association, “World Medical Association Declaration of Helsinki Ethical Principles for Medical Research Involving Human Subjects,” June 1964, <http://www.wma.net/en/30publications/10policies/b3/>.



designed to protect vulnerable populations participating in experimentation, including during the informed consent process.

Relatedly, populations affected by crises deserve to be reasonably informed about HIAs, even when the right to informed consent may not apply. This process—separate and distinct from informed consent—constitutes notification and informed participation. Informed participation is the effort to inform populations about how group data, including DII that may include them, will be acquired and used.

Engaging in informed participation seeks to ensure that affected populations may provide input about proposed and ongoing uses of data derived from them or relevant to them. While informed participation about current or future uses of group data may not always be possible, humanitarian actors must always endeavor to solicit informed participation as part of any HIA.



A5. The Right to Redress and Rectification

All people have the right to rectification of demonstrably false, inaccurate, or incomplete data collected about them. As part of this right, individuals and communities have a right to establish the existence of and access to personal data collected about themselves. All people have a right to redress from relevant parties when harm was caused as a result of either data collected about them or the way in which data pertaining to them were collected, processed, or used.

Individuals subject to HIAs have the right to know if their personal data are being held, by whom, and who has access to their data. Individuals should also have the right, within a reasonable time period and at a reasonable cost, to access personal data about themselves. They should be provided this data in a form intelligible to them, enabling them to verify and challenge the accuracy of data about themselves. In the event that such access needs to be restricted or denied, data managers must provide the individual with clear reasons for the denial of their request.

As part of the right to redress, affected persons and populations have a right to obtain the correction, blockage, and erasure of their data under certain circumstances. Examples of these circumstances may include:

- instances when informed consent applied but was not obtained;
- the infliction of harm as a direct result of HIAs on individuals or groups;
- non-consensual experimentation as part of a HIA;
- negligence leading to a personal data breach or group data breach;
- data are demonstrably inaccurate but unrectifiable; or
- when the means by which data are obtained or processed violates accepted human rights standards.

- Section B:**
- Sources of the Rights**
- B1. The Right to Information**
 - B2. The Right to Protection**
 - B3. The Right to Data Privacy and Security**
 - B4. The Right to Data Agency**
 - B5. The Right to Redress and Rectification**

B1. Sources of the Right to Information During Crises

Access to information during crisis, as well as the means to communicate it, is a basic humanitarian need. Thus, all people and populations have a fundamental right to generate, access, acquire, transmit, and benefit from information during crisis. The right to information during crisis exists at every phase of a crisis, regardless of the geographic location, political, cultural, or operational context or its severity.

The right to information during crises has always implicitly existed under Article 19 of the UDHR, which provides the right to “freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”¹ This is given legal force in Article 19 of the ICCPR.²

It can also be interpreted as existing as an “interdependent and interrelated right” required for the realization of Article 3 of the UDHR, the right to “life, liberty and security of person.”³ The UN Population Fund defines the interdependence and interrelatedness of rights as follows:

"The fulfilment of one right often depends, wholly or in part, upon the fulfilment of others. For instance, fulfilment of the right to health may depend, in certain circumstances, on fulfilment of the right to development, to education or to information."⁴

Realizing Article 3 of the UDHR in the networked age increasingly depends on the ability of populations to access and benefit from information during crises, including the ability to access and use ICTs and other critical communications infrastructure. Thus, a right to information during crises should be seen as an interdependent and interrelated right of Article 3 in the same way that the rights to other internationally recognized and protected forms of humanitarian assistance are protected as interdependent rights related to Article 3.⁵

Actions taken by state and non-state actors to obstruct, interdict, control, or use information and related infrastructure to otherwise harm populations during emergencies and disasters, including depriving them of the means to freely communicate, should be treated as violations of Articles 3 and 19 of the UDHR. These actions may not only be violations of

1. United Nations General Assembly, “Universal Declaration of Human Rights.”
2. United Nations General Assembly, “International Covenant on Civil and Political Rights,” *United Nations Treaty Series* 999, no. 14668 (1976): 171, <https://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf>.
3. United Nations General Assembly, “Universal Declaration of Human Rights.”
4. United Nations Population Fund, “Human Rights Principles,” *UNFPA*, 2005, <http://www.unfpa.org/resources/human-rights-principles>.
5. Ruth Abril Stoffels, “Legal Regulation of Humanitarian Assistance in Armed Conflict: Achievements and Gaps,” *Revue Internationale de La Croix-Rouge/International Review of the Red Cross* 86, no. 855 (September 27, 2004): 517, doi:10.1017/S1560775500181027.



freedom of speech, but may also constitute violations of the right of all people to freely receive humanitarian assistance.⁶

In June 2016, a non-binding resolution of the UN Human Rights Council effectively articulated a human right to the internet in response to recent incidents in which freedom of expression online has been infringed upon by governments. The resolution affirms that:

"...the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;"⁷

The value of ICTs is not the technology itself, but in its ability to access, generate, store, transmit, and transform information. Thus, the right to information during crisis should not be conflated with the right to any specific technology. However, the rapid development of information technologies from the middle of the twentieth century onwards has fundamentally altered humanity's relationship with technology.⁸

Crisis affected populations identifying technology as critical to meeting their needs and survival are not identifying the technology itself as the critical item, but the enhanced access to information provided.⁹ Insofar as specific ICTs are identifiable as critical to the survival of populations, it is

6. The Sphere Project, *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*.
7. United Nations Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, *United Nations Human Rights Council Resolutions*, 2016, <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement>.
8. Luciano Floridi, *The Ethics of Information*, Paperback (Oxford: Oxford University Press, 2013), 7–8 & Chapter 15.
9. It is critical to avoid the conflation of technology with information. By way of example, were we to interpret UNCLOS Article 24, Part 2, “The coastal State shall give appropriate publicity to any danger to navigation, of which it has knowledge, within its territorial sea” to mean lighthouses and paper maps, than GPS and digital charts would have no role in hazard identification. United Nations, “United Nations Convention on the Law of the Sea,” *United Nations Treaty Series* 1833, no. 31363 (1994), <https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280043ad5>.



because they amount to a standard of care, and right to benefit as such is identified in Article 27, Part 1 of the UDHR:

"Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits."¹⁰

B2. Sources of the Right to Protection

All people have a right to protection of their life, liberty, and security of person from potential threats and harms resulting directly or indirectly from the use of ICTs or data that may pertain to them. These harms and threats include factors and instances that impact or may impact a person's safety, social status, and respect for their human rights.

The right to protection from harm resulting from the use of ICTs and data is derived from multiple sources. The Humanitarian Charter states:

"The right to protection and security is rooted in the provisions of international law, in resolutions of the United Nations and other intergovernmental organisations, and in the sovereign responsibility of states to protect all those within their jurisdiction. The safety and security of people in situations of disaster or conflict is of particular humanitarian concern, including the protection of refugees and internally displaced persons. As the law recognises, some people may be particularly vulnerable to abuse and adverse discrimination due to their status such as age, gender, indigenous status, ethnicity, or race, and may require special measures of protection and assistance. To the extent that a state lacks the capacity to protect people in these circumstances, we believe it must seek international assistance to do so."¹¹

This right to protection from harm resulting from ICTs and data is based on the same provisions of international law referenced above, which include, though are not limited to, the UDHR, in particular Article 3: The Right to Life, Liberty and Security of Person; and the protections afforded to protected populations in situations of armed conflict under the Geneva Conventions.¹² Protection is defined by the International Committee of the Red Cross' Professional Standards for Protection Work as follows:

"...protection is a set of activities aimed at limiting the dangers to which people—civilians and detainees in particular—are exposed during armed conflict and other situations of violence, defending the rights of such people and preventing or halting any abuses they may be suffering."¹³

Protection efforts to prevent the negative effects of both the crisis and the humanitarian response to the crisis are core to

11. The Sphere Project, *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*.
12. International Committee of the Red Cross, "Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Forth Geneva Convention)," *United Nations Treaty Series* 75, no. 287 (August 12, 1949): 288–416.
13. International Committee of the Red Cross, *Professional Standards for Protection Work*, 2013th ed., vol. 0999/002 (Geneva, 2013),



the very definition of the humanitarian imperative and its implementation in practice. Relatedly, the principle of protection not only concerns the negative impacts of non-humanitarian actors, but includes the implications of humanitarian action itself. The Sphere Standards, which contain the Humanitarian Charter, also call on humanitarian actors to “Avoid exposing people to further harm as a result of your actions.”¹⁴

Protection efforts that may be required as a result of the existence of a right to protection from harm related to HIAs, for example, can include the implementation of data security practices for the handling of data from affected populations.

Specific obligations to implement data security practices are explicated in Article 7 of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*¹⁵ and Part 2, Paragraph 11 of the Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.¹⁶

<https://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf>.

14. The Sphere Project, *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*, 13.
15. The Council of Europe, “Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data” ETS No.108 (1981), <http://www.refworld.org/docid/3dde1005a.html>.
16. Organization for Economic Cooperation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” 2013, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

B3. Sources of the Right to Data Privacy and Data Security

All people have a right to have their personal information treated in ways consistent with internationally accepted legal, ethical, and technical standards of individual privacy and data protection.

Any exception to data privacy and protection during crises exercised by humanitarian actors must be applied in ways consistent with international human rights and humanitarian law and standards.

The aggregate of international agreements, covenants, and national laws that inform the concept of data privacy constitute an emerging norm, one that explicitly expands the right to privacy to include data privacy and balances it against the need for the collection and processing of information. The recognition of data privacy as the extension of an existing fundamental human right establishes a requirement for professional standards of practice for the humanitarian community. These agreements, covenants, and national laws begin from the premise that privacy is a fundamental human right, as provided for in the UDHR, and legal force in the Covenant on Civil and Political Rights.¹⁷ Article 12 of the UDHR states:

"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."¹⁸

These data privacy agreements exist to clarify and ensure the right to privacy in the era of computing and data.^{19,20} To that end, many data privacy and protection laws and regulations are expressed as obligations incumbent upon data holders and states to ensure respect of the right to privacy and the subsequent enjoyment of that right by data subjects. Legal scholarship avers that rights and obligations exist in parallel and roughly correlative fashion.^{21,22} These agreements constitute the antecedents by which the right to privacy in the context of HIAs are explicated.

There is as of yet no accepted humanitarian standard for data privacy and data security. However, a set of international norms is emerging around principles first articulated in the *Council of Europe's Convention for the Protection of Individuals with*

17. United Nations General Assembly, "International Covenant on Civil and Political Rights."
18. United Nations General Assembly, "Universal Declaration of Human Rights."
19. Council of Europe, "Explanatory Report of Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," *European Treaty Series* (Strasbourg, 1981), <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.
20. Organization for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," fig. 3.
21. Francis Leiber, *Manual of Political Ethics*, Vol 2. (Boston: Charles C. Little and James Brown, 1839), col. 1, <https://books.google.com/books?id=MwVAAAAYAAJ>.
22. William N. Eskridge Jr., "The Relationship between Obligations and Rights of Citizens," *Fordham Law Review* 69, no. 5 (2001): 1721–51.



regard to Automatic Processing of Personal Data and the *OECD Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data*. These principles include the directive to ensure that data are obtained and processed fairly and lawfully; stored for specified and legitimate purposes; are accurate; and are stored for the minimum period necessary. It also commits parties to the principle of data minimization, and transparency of purpose.²³

The last several decades have seen other regional agreements emerge that affirm the data privacy principles laid out by the OECD and establish them as minimum standards, or establish broadly similar guidelines for data protection. The EU Directive 95/46/EC establishes these principles at the heart of European Union data protection law.²⁴ The Asia-Pacific Economic Cooperation (APEC) Privacy Framework mirrors the OECD Guidelines and extends them by making explicit the principle of preventing harm to the data subject²⁵ and individual consent.²⁶

The Organization of American States (OAS) has also adopted twelve “Principles on Privacy and Personal Protection.” These principles are similar to those adopted by the EU, OECD, and APEC.²⁷ The Economic Community of West African States (ECOWAS) Supplementary Act²⁸ on Personal Data Protection draws strongly from the EU Directive and establishes

23. The Council of Europe, “Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data.”
24. European Parliament, “Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data,” *Official Journal of the European Communities* 44, no. L8 (January 12, 2001): 0001–0022, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF>.
25. Asia-Pacific Economic Cooperation, “APEC Privacy Framework,” vol. APEC#205-S (Singapore, 2005), pt. III, I.14, http://publications.apec.org/publication-detail.php?pub_id=390.
26. Ibid., vol. APEC#205-S, pt. III.V.20.& Part III V.20
27. Organization of American States, “Privacy and Data Protection” (Rio de Janeiro: Organization of American States, 2015), http://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf.
28. Communauté Economique des Etats de l’Afrique de l’Ouest/Economic Community of West African States, “Supplementary Act A/SA.1/01/10 On Personal Data Protection within ECOWAS,” 2010, <http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf>.



similar principles,²⁹ as does the African Union Convention on Cyber Security and Personal Data Protection.³⁰

On the national level, there is an emerging consensus around the principles found in European data privacy laws³¹ and the OECD Guidelines as accepted international minimum standards. As of 2015, 109 nations had implemented one or more data privacy laws that incorporate European precedents³² or share underlying principles with European Conventions and the OECD Guidelines.

These shared principles are defined as “covering the most important parts of its private sector, or its national public sector, or both,” and providing,

“a set of basic data privacy principles, to a standard at least approximating the minimum provided for by the OECD Guidelines or Council of Europe (CoE) Convention 108, plus some methods of officially-backed enforcement (i.e. not only self-regulation).”³³

While limited in jurisdiction to public health responses, these principles are well established in international law through the World Health Organization (WHO) International Health Regulations, Article 45, which stipulates the guarantees that State Parties to that treaty must extend to ensure the appropriate processing of personal data.³⁴

The principle of *primum non nocere*, or “do no harm,” is enshrined in Sphere Protection Principle 1,³⁵ and is a bedrock component of the humanitarian principle of humanity.³⁶ In

29. Graham Greenleaf, “The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108,” *International Data Privacy Law* 2, no. 2 (May 1, 2012): 68–92, doi:10.1093/idpl/ips006.
30. African Union, “African Union Convention on Cybersecurity and Personal Data Protection” EX.CL/846 (2014).
31. As laid out in The Council of Europe, “Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data.”
32. Greenleaf, “The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108.”
33. Graham Greenleaf, “Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority,” *Privacy Laws Business International Report*, January 30, 2015.
34. World Health Organization, *International Health Regulations (2005)*, 3rd ed. (Geneva, 2016), <http://www.who.int/ehr/publications/9789241580496/en/>.
35. The Sphere Project, *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*.
36. “To respect is primarily an attitude of abstaining, meaning: do not harm, do not threaten, spare the lives, integrity and the means of existence of



the networked age, doing no harm means that humanitarian actors must seek to know, prevent and mitigate harms, including violations of human rights, that may result from breaches of data privacy and security. Privacy, security, and agency are interrelated concepts in theory and practice.

others, have regard for their individual personality and dignity.” Jean Pictet, “The Fundamental Principles of the Red Cross: Commentary,” *International Federation of the Red Cross and Red Crescent Societies*, 1979.

B4. Sources of the Right to Data Agency

Everyone has the right to agency over the collection, use, and disclosure of their personally identifiable information (PII) and aggregate data that includes their personal information, such as demographically identifiable information (DII). Populations have the right to be reasonably informed about information activities during all phases of information acquisition and use.

Article 7 of the ICCPR explicitly extends the right of free consent to medical or scientific experimentation from the right to bodily integrity. It states:

"No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected without his free consent to medical or scientific experimentation."³⁷

Article 7 is the fundamental basis of the right to dignity described in the Core Humanitarian Standards.³⁸ The right to dignity requires adherence to the provisions of international law concerned with, among other things, freedom from cruel, inhumane, or degrading treatment.³⁹

The concept of data agency encompasses the principles of informed consent and the concepts of informed participation and notification. The first codification of the principle of informed consent arose in the verdict of the *United States v. Karl Brandt*, which established the ten principles for permissible medical experimentation known as the Nuremberg Code,⁴⁰ which is treated as customary international law.⁴¹ The first principle of the Nuremberg Code stipulates that "the voluntary consent of the human subject is absolutely essential."⁴²

In 1964, the Declaration of Helsinki established an internationally recognized code of conduct for experimentation. The principle of informed consent was expanded to include the provision of each subject with information about relevant aspects of experimental procedures prior to obtaining consent to participation.⁴³ In addition to reiterating the requirement for informed consent, the Declaration of Helsinki introduced special considerations for

37. United Nations General Assembly, "International Covenant on Civil and Political Rights."
38. CHS Alliance, Groupe URD, and The Sphere Project, *Core Humanitarian Standard: Core Humanitarian Standard on Quality and Accountability*, 2014, <https://corehumanitarianstandard.org/files/files/Core%20Humanitarian%20Standard%20-%20English.pdf>.
39. International Committee of the Red Cross, "Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Forth Geneva Convention)."
40. *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10: The Medical Case*, vol. 2 (Washington, DC: United States Government Printing Office, 1949).
41. Thomas Weatherall, *Jus Cogens: International Law and Social Contract* (Cambridge: Cambridge University Press, 2015).
42. Ibid., 181.
43. World Medical Association, "World Medical Association Declaration of Helsinki Ethical Principles for Medical Research Involving Human Subjects," paras. 25–32.



vulnerable populations and the concept of independent ethics review, which evolved into the Institutional Review Board (IRB).⁴⁴

Finally, in 1979, the Belmont Report defined three ethical principles, beyond the rules laid out in the Nuremberg Code and Declaration of Helsinki, necessary for the protection of human subjects: respect for persons, beneficence, and justice.⁴⁵ The principle of respect for persons establishes “first that individuals should be treated as autonomous agents, and second, that persons with diminished autonomy are entitled to protection.” Beneficence is defined as an obligation to both do no harm, and to maximize benefits while minimizing potential harm. The principle of justice incorporates formulations of equal treatment. These principles are directly consistent with the humanitarian principle of humanity, which encompasses respect for human dignity,⁴⁶ and apply in all settings beyond standard of care, including all experimental procedures.

Together, the Nuremberg Code, the Declaration of Helsinki, and the Belmont Report are the mutually-reinforcing foundation for the principles governing informed consent for all human subject experimentation.

44. Ibid., para. 23.

45. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, “Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, Report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research,” *Federal Register*, vol. 44, April 18, 1979, <http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/>.

46. United Nations General Assembly, “Strengthening of the Coordination of Humanitarian Emergency Assistance of the United Nations” A/RES/46/1 (December 19, 1991), <http://www.un.org/documents/ga/res/46/a46r182.htm>.

B5. Sources of The Right to Redress and Rectification

All people have the right to rectification of demonstrably false, inaccurate, or incomplete data collected about them. As part of this right, individuals and communities have a right to establish the existence of and access to personal data collected about themselves. All people have a right to redress from relevant parties when harm was caused as a result of either data collected about them or the way in which data pertaining to them were collected, processed, or used.

Privacy is recognized as a fundamental human right in the UDHR, which is the basis of international human rights law.⁴⁷ It is also included in the Covenant on Civil and Political Rights.⁴⁸ Article 12 of the UDHR states:

"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."⁴⁹

The United Nations has also formally commented on the importance of rectification and redress. United Nations General Assembly Resolution 45/95 of 14 December 1990 describes an international, borderless right to access, rectification, and erasure in:

"Principle of interested-person access: Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressee's. Provision should be made for a remedy, if need be with the supervisory authority specified in Principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence."⁵⁰

The right of the individual whose personal data has been collected to access and challenge that personal data is recognized as fundamental to safeguarding the right to privacy. Individuals must be able to discover whether a data manager has collected data about them. They must also be allowed to access this data,

47. United Nations, "The Foundation of International Human Rights Law," accessed September 22, 2016, <http://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html>.
48. United Nations General Assembly, "International Covenant on Civil and Political Rights."
49. United Nations General Assembly, "Universal Declaration of Human Rights."
50. United Nations General Assembly, "Guidelines for the Regulation of Computerized Personal Data Files," *United Nations General Assembly Resolutions* 45, no. 95 (1990): pt. 4, <http://www.refworld.org/pdfid/3ddcafaac.pdf>.



in a form intelligible to them. This enables them to review its accuracy and to amend, revise, or correct if necessary.

This right, sometimes called the right to individual participation, is found in the major regional covenants and agreements regarding data privacy, including the OECD Guidelines governing the protection of privacy and transborder flows of personal data,⁵¹ the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,⁵² Directive 95/46/EC of the European Parliament,⁵³ the APEC Privacy Framework,⁵⁴ the OAS Principles on Privacy and Personal Data Protection,⁵⁵ the ECOWAS Supplementary Act A/SA/.1/01/10 on Personal Data Protection within ECOWAS,⁵⁶ and the African Union Convention on Cyber Security and Personal Data Protection.⁵⁷

While the right to individual participation is not an absolute right, the OECD Expert Group nevertheless felt that it was necessary to include in the OECD Guidelines as they considered it the most important of privacy safeguards.⁵⁸ Likewise, the OAS Inter-American Judicial Committee calls this right “one of the most important safeguards in the field of privacy protection.”⁵⁹

This access should be simple to exercise, and part of the day-to-day activities of the data manager. It should not require the individual to access legal mechanisms or procedures. This right is necessarily limited: it may be modified or restricted in cases where allowing access would abrogate the human rights of the individual or others. In the event that access is denied,

51. Organization for Economic Cooperation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.”
52. The Council of Europe, “Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data.”
53. The European Parliament, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,” *Official Journal of the European Union* 38, no. L281 (1995): 0031–0050.
54. Asia-Pacific Economic Cooperation, “APEC Privacy Framework.”
55. Organization of American States, “Privacy and Data Protection.”
56. Communauté Economique des Etats de l’Afrique de l’Ouest/Economic Community of West African States, “Supplementary Act A/SA.1/01/10 On Personal Data Protection within ECOWAS.”
57. African Union, “African Union Convention on Cybersecurity and Personal Data Protection.”
58. Organization for Economic Cooperation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” 58.
59. Organization of American States, “Privacy and Data Protection,” 13.



the data manager must provide reasons for that denial, in an intelligible format and within a reasonable time period.

The right to redress is a key component of emerging international legal norms governing the use of data. The EU has taken a leading role in encoding a right for people to seek rectification of inaccurate data and redress for harms stemming from the use of their data into law.⁶⁰

Regulation (EC) 45/2001 explicitly enshrines the right to rectification in Article 14, stating: “The data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data.”⁶¹ Article 8 of the 2000 Charter of Fundamental Rights of the European Union states, “Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”⁶²

Notably, Article 8 explicitly links the right of access to the right of rectification—implying that one cannot exist without the other. The forthcoming EU Regulation 2016/679, or General Data Protection Regulation (GDPR), which will enter into force in May 2018, further describes and enhances the right to rectification and redress. Article 59 notes:

"Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within

60. The European Union describes this right in three documents, which are cited in full below: Regulation (EC) 45/2001, the 2000 Charter of Fundamental Rights of the European Union, and the upcoming EU General Data Protection Regulation (Regulation (EU) 2016/679)
61. European Parliament, “Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data.”
62. European Commission, “The Charter of Fundamental Rights of the European Union,” *Official Journal of the European Communities* 43, no. C364 (December 18, 2000): 1–22, doi:10.1108/03090550310770974.



one month and to give reasons where the controller does not intend to comply with any such request."⁶³

Article 59 not only reiterates the link between the right of access to data and the right of rectification, but also describes a specific timeframe within which data managers are obligated to respond to requests from data subjects.

63. European Parliament, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union* 59, no. L119 (May 4, 2016): 1–88.

Section C: Why the Rights Are Needed

C1. The Right to Information C2. The Right to Protection C3. The Right to Data Privacy and Security C4. The Right to Data Agency C5. The Right to Redress and Rectification

The rights identified and articulated in this document, both individually and as a group, seek to address three urgent needs stemming from current applications of ICTs and data by humanitarian actors engaged in HIAs. Growing qualitative and quantitative evidence of rights violations by multiple actors and the potential infliction of harm related to civil society applications of ICTs and data have revealed these needs by exposing the lack of clear guidance available to humanitarian actors about what rights crisis-affected populations have related to HIAs.

These three needs are the following:

1. A need for clarity and specificity about the status of information and HIAs as a basic humanitarian need, including protections afforded these activities compared to other, traditionally accepted forms of humanitarian assistance;
2. A need for humanitarian actors and crisis-affected populations to have guidance about what rights crisis-affected populations have to protection from harm related to the use of ICTs and data; rights to data privacy and security; and rights to agency over how their data is used; and
3. A need for enshrinement of the rights of crisis-affected populations to receive remedy and accountability for violations of these rights.

C1. The Need for the Right to Information

Access to information during crisis, as well as the means to communicate it, is a basic humanitarian need. Thus, all people and populations have a fundamental right to generate, access, acquire, transmit, and benefit from information during crisis. The right to information during crisis exists at every phase of a crisis, regardless of the geographic location, political, cultural, or operational context or its severity.

The generation, transmission, provision, and receipt of information during crisis has always been an essential component of crisis response by affected populations and humanitarian actors.¹ The NGO, Article 19: The Global Campaign for Free Expression identifies some of the critical roles that information can play in the aftermath of a crisis. These include the mitigation of the loss of life, reducing panic, directing people to essential services, ensuring two-way communication between assistance providers and affected communities, and other vital response functions.²

With the advent of the networked age, however, the role that ICTs and information itself plays in the response of affected communities and humanitarian actors to crises has become even more central and crucial. ICTs and the collection and analysis of data are increasingly central to how humanitarian actors determine need and manage responses, as well as to how affected communities access essential services.

Affected populations have begun to identify the enhanced access to information enabled by internet connectivity, smartphones, and other ICTs and infrastructure as a primary humanitarian need that is, in some cases, more important to them than access to traditional forms of assistance such as food, water, and shelter.³ The phenomena of ICTs and near real-time data updates being perceived by affected populations as necessary prerequisites for accessing services is a significant turning point in the history of humanitarian assistance.

There appears to be a potential relationship between the resiliency of populations and their access to telecommunications

1. Chris McIvor, “Data or Dialogue? The Role of Information in Disasters,” in *World Disasters Report 2005* (International Federation of the Red Cross and Red Crescent Societies, 2005), <http://www.ifrc.org/en/publications-and-reports/world-disasters-report/wdr2005/wdr-2005---chapter-1-data-or-dialogue-the-role-of-information-in-disasters/>.
2. Article XIX: Global Campaign for Free Expression, “Humanitarian Disasters and Information Rights: Legal and Ethical Standards on Freedom of Expression in the Context of Disaster Response,” no. April (April 2005), <http://article19.org/data/files/pdfs/publications/freedom-of-information-humanitarian-disasters.pdf>.
3. Matthew Brunwasser, “A 21st-Century Migrant’s Essentials: Food, Shelter, Smartphone,” *The New York Times*, August 25, 2015, http://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=0.



and social media. A July 2016 BBC Media Action study of refugees in Greece and Germany found the following:

"The analysis shows that refugees who stay in regular contact with other refugees and who have wide communication networks of family members and friends (via mobile networks and social networking sites such as Facebook and WhatsApp) were likely to be more resilient than those who were less connected."⁴

A 2014 Humanitarian Innovation Project (HiP) study titled *Refugee Economies* found that refugees who use technology in their daily lives identified mobile technology and the internet as important for their economic well-being. Mobile technology enabled the creation of supply chains, provided refugees with pricing information, and enabled the easy transfer of money. In some professions, such as agriculture, refugees cited mobile technology as critical to facilitate and sustain trade networks.⁵

The relationships between access to ICTs, social media platforms, network infrastructure, and HIAs and the human security, well-being, and survivability of crisis-affected populations have only just begun to be studied. The anecdotal evidence available suggests that these little understood relationships between information access and crisis-affected populations are profoundly transforming the very nature of how crises unfold in the 21st century—both positively and negatively.

Relatedly, the *Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations* acknowledges the essential role ICTs play in potentially reducing the vulnerability of populations to crises.⁶ As a whole, however, international treaties and law have not fully kept pace with these changes and remain relatively vague about the role

4. Theodora Hannides et al., "Voices of Refugees: Information and Communication Needs of Refugees in Greece and Germany," 2016, <http://www.bbc.co.uk/mediaaction/publications-and-resources/research/reports/voices-of-refugees>.
5. Alexander Betts et al., "Refugee Economies: Rethinking Popular Assumptions" (Oxford, 2014), 33, <http://www.rsc.ox.ac.uk/files/publications/other/refugee-economies-2014.pdf>.
6. United Nations, "Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operation," *Treaty Series* 2296, no. 40906 (January 8, 2005): 5, <https://treaties.un.org/doc/Publication/UNTS/Volume%201522/v1522.pdf>.



of information in crises, as well as how and when information activities and communications infrastructure are protected.

These major gaps in current International Humanitarian Law (IHL) have critical implications that have not yet sufficiently addressed. The most important example of these gaps is the current language of the Geneva Convention regarding the rights of protected populations to request humanitarian assistance.

The Fourth Geneva Convention, Article 30 states that,

"Protected persons shall have every facility for making application to the Protecting Powers, the International Committee of the Red Cross, the National Red Cross (Red Crescent, Red Lion and Sun) Society of the country where they may be, as well as to any organization that might assist them."⁷

This language may be interpreted as the right of crisis-affected populations to call for help by any means necessary, including, in the 21st century, the use of ICTs.

However, this language only applies in international conflicts, as Ruth Abril Stoffels notes. She identifies, in her commentary for the *International Committee of the Red Cross on Legal regulation of humanitarian assistance in armed conflict: Achievements and gaps*, the clearly unmet legal need and operational realities that limit the value of Article 30 in this regard:

"In the case of international conflicts the entitlement to request aid from third parties is established in Article 30 of the Fourth Geneva Convention. In the case of internal conflicts, however, there is no provision referring either directly or indirectly to such an entitlement. This right therefore needs to be expressly enshrined in law or its effectiveness will not be guaranteed in cases in which the international community fails to take spontaneous action, the authorities responsible for the victims do not disclose the situation to the outside world

7. International Committee of the Red Cross, "Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)."



and the media do not have access to the affected area and are unable to sound the alarm.⁸

At present, this is the only language in current IHL that appears to specify a right to populations to request humanitarian assistance. Additionally, information in the context of emergencies and disasters has traditionally been treated within the context of freedom of speech, rather than as a humanitarian resource necessary for the sustainment of life unto itself. With the advent and proliferation of ICTs, communications infrastructure and the means to access it require intentional protection equal to other traditionally protected physical humanitarian resources, such as food, water, shelter, and medical treatment.

Thus, the explicit recognition of a right to information during crises—including both the right to request assistance regardless of the nature of the crisis and IHL protection for relevant communications infrastructure and activities—is now required. While the Additional Protocol I to the Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) provides for the protection of objects indispensable to the survival of the civilian population,⁹ the interconnectedness of civilian, military, and armed non-state actor communication networks is a feature of modern telecommunications, thus creating ambiguity as to what constitutes a legitimate target under the Additional Protocol.¹⁰ This constitutes a gap in existing IHL, and the articulation and codification of a specific right to information during crises will also necessitate the development of prohibitions under IHL for what constitutes violations of this right, including intentional obstruction of and attacks upon, HIAs and infrastructure.

This right, in effect, also acknowledges the existence of “humanitarian cyberspace.” However, there is no current

8. Stoffels, “Legal Regulation of Humanitarian Assistance in Armed Conflict: Achievements and Gaps.”
9. International Committee of the Red Cross, “Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I),” *United Nations Treaty Series* 1125, no. 17512 (1978): 3–608, https://treaties.un.org/doc/Publication/UNTS/Volume_1125/v1125.pdf Article 54.
10. Robin Geiss, “Cyber Warfare: Implications for Non-International Armed Conflicts,” *International Law Studies* 89 (2013): 639.



agreement on what constitutes “humanitarian space,”^{11,12} let alone humanitarian cyberspace. Humanitarian cyberspace is a differentiated zone that likely includes servers, sensors, telecommunications networks, and mobile devices employed for humanitarian purposes and subject to humanitarian protections wherein aid organizations and their personnel are recognized as not being legitimate targets.¹³ Humanitarian cyberspace encompasses the people connected to its functions as directly related to its secure and consistent operation and use.

This concept builds on the well-established but poorly defined analog concept of “humanitarian space.”¹⁴ The right to information during crises requires clearer delineation and codification, including descriptions of what infrastructure is used by which actors, and in what contexts may actually constitute humanitarian cyberspace.

11. Nathaniel Raymond, Britney Card, and Ziad Al-Achkar, “What Is ‘Humanitarian Communication?’ Towards Standard Definitions and Protections for the Humanitarian Use of ICTs,” *European Interagency Security Forum*, no. August (2015): 1–5, <https://www.eisf.eu/wp-content/uploads/2015/10/2041-EISF-2015-What-is-humanitarian-communication.pdf>.
12. Johanna G. Wagner, “An IHL/ICRC Perspective on Humanitarian Space,” *Humanitarian Exchange* (London, December 2005), 24–26, <http://odihpn.org/wp-content/uploads/2006/01/humanitarianexchange032.pdf>.
13. Daniel Gilman and Leith Baker, “Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Humanitarian Emergencies,” *UN Office for the Coordination of Humanitarian Affairs Policy and Studies Series*, no. 11 (October 2014), <https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf>.
14. Overseas Development Institute, “Humanitarian Space: Concept, Definitions and Uses Meeting Summary Humanitarian Policy Group,” in *Roundtable*, 2010, 1–7, <https://www.odi.org/events/2655-humanitarian-space-concepts-definitions-uses>.

C2. The Need for the Right to Protection

All people have a right to protection of their life, liberty, and security of person from potential threats and harms resulting directly or indirectly from the use of ICTs or data that may pertain to them. These harms and threats include factors and instances that impact or may impact a person's safety, social status, and respect for their human rights.

The use of ICTs and digital data in humanitarian response has grown considerably over the past decade. There is an emerging understanding of the potential harm that these technologies and the related HIAs that employ them may cause in certain operational contexts.¹⁵ In some limited cases, specific harmful impacts of ICTs have been documented as a result of deployments by civil society actors.^{16,17}

Some efforts have been made to begin capturing best practices relevant to ICT use in HIAs during past humanitarian responses.¹⁸ Despite the growing awareness of the unique threats to vulnerable populations that these approaches may cause or magnify, there is no accepted ethical doctrine or minimum technical standard for their mitigation and prevention.¹⁹

In many cases, the ethical and operational guidance employed is not current with either changes to the technological state-of-the-art, as well as to the technological adaptations of humanitarian actors, affected populations, and alleged human rights abusers. There are many understandable reasons that this “blind spot” in current humanitarian practice has occurred.

Chief amongst these reasons is the absence of an intentionally and explicitly articulated right for affected populations to be protected from harm related to HIAs. Relatedly, this right must be articulated to specifically create a corresponding obligation for humanitarian actors to prevent and mitigate the potential harm. Realization of this right depends on this critical gap in current practice being urgently addressed. The identification and articulation of a right to protection from harm related to HIA’s is the first step.

15. Rahel Dette, “Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts,” 2015, 2.
16. Ibid., 15.
17. Sean Martin McDonald, “Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation,” *The Centre for Internet and Society*, no. 2016.01 (March 1, 2016), <http://cis-india.org/papers/ebola-a-big-data-disaster>.
18. George Chamales and Rob Baker, “Securing Crisis Maps in Conflict Zones,” in *2011 IEEE Global Humanitarian Technology Conference* (IEEE, 2011), 426–30, doi:10.1109/GHTC.2011.47.
19. Nathaniel Raymond, Caitlin Howarth, and Jonathan Hutson, “Crisis Mapping Needs an Ethical Compass,” *Global Brief*, February 2012, <http://globalbrief.ca/blog/2012/02/06/crisis-mapping-needs-an-ethical-compass/>.

C3. The Need for the Right to Data Privacy and Security

All people have a right to have their personal information treated in ways consistent with internationally accepted legal, ethical, and technical standards of individual privacy and data protection. Any exception to data privacy and protection during crises exercised by humanitarian actors must be applied in ways consistent with international human rights and humanitarian law and standards.

Humanitarian action is primarily an information-driven practice. From needs assessments to logistics, assistance and response is predicated at every stage by information collection and sharing. Crises, by their very nature, necessitate the sharing of sensitive and confidential personal information by individuals—information that would otherwise remain private.²⁰

Privacy, by its nature, is a complex and at times nebulous concept. In its breadth, it encompasses a broad range of allied interests. These can include compromised physical security, financial and property harms, reputational harms, relationship and contractual harms, emotional and psychological distress, and vulnerability to future harms. It can cover personal identity, family life, the home, and correspondence, which has come to mean all forms of communication.²¹ In the networked age, potential violations of a data subject's right to privacy arise from a number of activities, each of which encompass a range of potential harms. These activities include (but are not limited to:) the collection, processing, and dissemination of data and metadata, and direct privacy invasions.²² Philosophical and legal conceptualizations of privacy have evolved throughout the 19th and 20th centuries, and continue to do so. Data protection laws have arisen specifically in response to the pressures of new technologies on older conceptions of privacy²³ and broad conceptualizations of privacy are an important tool for both understanding the impact of technology on affected populations and individuals and serve as a reminder that the impact of future technology on privacy is unclear and thus must be constantly reassessed.

The adoption of ICTs to manage this information may increase the speed and efficiency by which information can be collected and shared, but this adoption also increases the volume of sensitive information collected, as well as the potential number of avenues by which a malicious party might gain access to these data. Thus, the use of ICTs creates additional burdens and challenges with regards to protecting

20. Gilman and Baker, "Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Humanitarian Emergencies."^G
21. Anthony Paul Lester, David Pannick, and J.W. Herberg, eds., *Human Rights Law and Practice*, Third (London: LexisNexis, 2009), 359.
22. Daniel J. Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2010), 103–4.
23. Organization for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 42.



individual privacy in the context of humanitarian crises, during which pre-existing risks are magnified considerably.

One of these new challenges is the aggregation effect, also known as the “data mosaic effect.” This phenomenon occurs when certain data that might not appear to be sensitive are combined with additional data that makes the impact on an individual’s privacy potentially dangerous and unpredictable.²⁴

Thus, individuals have a limited ability to predict what impact seemingly trivial data they share might have when aggregated with other data in the future. In addition to complicating the ability of individuals to provide informed consent, this phenomenon becomes even more complex during crises when individuals may prioritize privacy, as well as their willingness to share information, differently.²⁵

The risks posed by the aggregation effect increasingly, critically, and uniquely impact the humanitarian sector. Data products resulting from the derivation and aggregation of individual data with one or more additional stream(s) of data from other sources are increasingly commonplace during response operations.

In the context of humanitarian response, the resulting risks are no longer limited to only the exposure of PII, but also the creation and exposure of DII. Raymond describes the challenges inherent in the creation and management of DII as follows:

"…DII can result from the transformation of seemingly disparate, unrelated data sets into an amalgamated data product that can be easily 'weaponized' into a means for doing harm. The potential harm of DII is often most apparent, if not entirely, to the perpetrator of potential harm, rather than to the holder of one or all of the pieces of a potentially actionable mosaic of DII.

Whereas PII’s potential harm comes from when it is leaked or breached, DII’s harm, and thus its

24. Daniel J. Solove, “Privacy Self-Management and the Consent Dilemma,” *Harvard Law Review* 126, no. 7 (2013): 1880–1903.
25. Kate Crawford and Megan Finn, “The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters,” *GeoJournal* 80, no. 4 (August 1, 2015): 491–502, doi:10.1007/s10708-014-9597-z.



ethical implications, often emanates from simply whether the possibility exists that it can be even created. This reality makes the overall ethical imperative to understand, manage, and protect potential sources of DII as important, if not more so in some cases, than those commensurate with holding only one source of PII."²⁶

Data privacy and ensuring protection from harm, including the provision of data security, are therefore fundamentally linked—and neither can be realized without the other. Data security is an intrinsic part of protecting data privacy, regardless of the type of data being utilized.

The number of data records leaked, stolen, or accidentally exposed to the public numbers numbered over half a billion in the first six months of 2016, with the majority constituting personal information.²⁷ The right to data privacy and security explicitly enshrines the moral and existing legal obligation of humanitarian actors to implement appropriate security practices to safeguard sensitive data from unauthorized access, alteration, and destruction.

26. Raymond, “Beyond ‘Do No Harm’ and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society’s Use of Data.”
27. Gemalto, “Data Breach Statistics 2016: First Half Results Are in,” 2016, <http://blog.gemalto.com/security/2016/09/20/data-breach-statistics-2016-first-half-results/>.

C4. The Need for the Right to Data Agency

Everyone has the right to agency over the collection, use, and disclosure of their personally identifiable information (PII) and aggregate data that includes their personal information, such as demographically identifiable information (DII). Populations have the right to be reasonably informed about information activities during all phases of information acquisition and use.

The articulation of the right to data agency enshrines extant protections in international law against non-consensual human experimentation and to ensure the dignity of crisis-affected populations as mandated by core humanitarian principles. Article 3 of the UDHR can be read as inherently providing a right for data agency and protection from non-consensual experimentation as an inherent aspect of realizing the right to liberty and security of person,²⁸ while Article 7 of the ICCPR explicitly provides this right.

Fulfilling the humanitarian imperative compels the collection and use of PII and DII in crises. However, that requirement to collect and use PII and DII data to support response operations must be balanced with the humanitarian principle of humanity, which requires ensuring respect for the individual. The right to data agency exists at the intersection of the need for humanitarians to access data from individuals and the right of individuals to have their autonomy respected when this data is collected and used.

The right to data agency is of particular importance in the context of the often widely held assumption that data collection and use is, itself, inherently beneficial. In the recent Ebola outbreak, international humanitarian actors accessed call detail records (CDRs) to model predictions of the epidemic and to conduct contact tracing.

Critically, the potential harms of acquiring and using CDRs, which contain PII, were deemed insignificant in the face of the potential benefits humanitarian actors aimed to achieve with the data. Sean McDonald's *Ebola, A Big Data Disaster*—provides an account of the unmitigated risks and apparent violations of human rights resulting from this experimental use of PII. To date, no clear benefit of this operation has been demonstrated.²⁹

Similarly, DII was collected and transmitted to alleged perpetrators of gross human rights abuses as part of the 2007 “Eyes on Darfur” intervention conducted by Amnesty International. The creation and transmission of DII was to the apparent detriment of the human security of the civilians the intervention was intended to protect. In an analysis of the intervention, Grant Gordon found that the collection

28. United Nations General Assembly, “Universal Declaration of Human Rights.”
29. McDonald, “Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation.”



of satellite imagery and the public release of metadata about villages being monitored resulted in a 20-percentage point increase in the number of attacks on those villages.³⁰

In the above case studies, the populations affected by crises were not included in decisions about the collection and use of their data (PII) or data relevant to their human security (DII). Until now, there has been no clear codification of the right to data agency. Evidence of the potential harm of HIAs presented above demonstrates the urgent necessity of the explicitation of the right to data agency.

The harm caused by the current practice of collecting and using information without informed consent, or at a minimum, notification, underscores the current relevance of the right to data agency. Populations affected by crises have the right to provide informed consent to the collection and use of their PII for experimental HIAs and to receive protection from non-consensual experimentation. Populations affected by crises also have the right to be afforded notification regarding the collection and use of their DII, whenever possible.

Furthermore, the realization of the right to data agency is necessary for the inclusion of affected populations in decision-making about humanitarian responses that affect them. The right to data agency positions affected populations at the center of the humanitarian response, and is therefore fundamental to enfranchising affected populations, consistent with the Core Humanitarian Standard.³¹

30. Grant Gordon, “Monitoring Conflict to Reduce Violence: Evidence from a Satellite Intervention in Darfur,” March 3, 2016, <http://www.grantmgordon.com/wordpress/wp-content/uploads/2010/06/GG-EoD.pdf..>
31. CHS Alliance, Groupe URD, and The Sphere Project, *Core Humanitarian Standard: Core Humanitarian Standard on Quality and Accountability*.

C5. The Need for the Right to Redress and Rectification

All people have the right to rectification of demonstrably false, inaccurate, or incomplete data collected about them. As part of this right, individuals and communities have a right to establish the existence of and access to personal data collected about themselves. All people have a right to redress from relevant parties when harm was caused as a result of either data collected about them or the way in which data pertaining to them were collected, processed, or used.

The right to redress is rooted in pragmatic need and human rights principles: humanitarians will inevitably make both foreseen and unforeseen errors in the realm of data, and must establish clear methods of addressing these errors. Crisis-affected population have the right to receive redress for these errors, which may include the rectification of inaccurate data, the deletion of data that cannot be rectified, and reparations for damage that is caused by erroneous data.

In the EU context, these rights are directly linked to an individual's right to access data³² that has been collected about them, as enumerated in Article 8 of the European Charter of Fundamental Rights. These rights are also linked to the "data quality" principle,³³ a common (albeit unclearly-defined) concept that links many different national privacy laws.

The right to redress acknowledges the increasing reach and import of personal data. This information touches on many important aspects of an individual's life, including the workplace and the educational, health, and judicial systems. This wide reach means that data that is incomplete, inaccurate, or collected in both lawful and illegal fashions can cause demonstrable harm to individuals and to groups. This reality therefore obliges the humanitarian community to actively address this source of harm—it obliges them to "set right" errors.

The right pertains to both potential harm and to harm that has already taken place. As part of the right to redress, individuals hold a right to rectify incorrect or incomplete data about them, with the goal of avoiding future harm. If they have been harmed by actions humanitarians take on the basis of incorrect or incomplete data, or data gathered illegally or in violation of their right to data agency, they have the right to receive redress in the appropriate form.

The right to redress, as described in the EU context and in this document, ensures that errors on the part of the party who collects and harbors the data are not ignored or addressed in

32. European Data Protection Supervisor, "Guidelines on the Rights of Individuals with Regard to the Processing of Personal Data," February 25, 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf.
33. Jay Cline, "Data Quality -- the Forgotten Privacy Principle," *ComputerWorld*, September 2007, <http://www.computerworld.com/article/2541015/security0/data-quality----the-forgotten-privacy-principle.html>.



a minimal or haphazard fashion. It gives individuals a clear path to correcting the record, and in some cases, a clear path to recovering financial damages for the harms suffered.

Algorithmic research and assessment methods deserve particular scrutiny on the basis of this right, as they are often built on incomplete, prejudiced, or otherwise biased data. These data can potentially entrench errors and compound harm if they are not accurate. Individuals are entitled to redress if they are harmed by algorithmic methods based on inaccurate or incomplete prior information.

Section D: Realizing the Rights

- D1. The Right to Information**
- D2. The Right to Protection**
- D3. The Right to Data Privacy and Security**
- D4. The Right to Data Agency**
- D5. The Right to Redress and Rectification**

Realizing the rights identified by the Signal Code will involve the participation of a diverse set of actors, including humanitarian NGOs, governments, international agencies, private sector actors, and most importantly, crisis affected populations themselves. The following section, however, focuses as an initial first step on specifically articulating core responsibilities of humanitarian actors for the realization of the rights. This step is a prerequisite for the eventual identification and formal codification of the obligations humanitarian actors have when designing and conducting HIAs.

D1. Realizing the Right to Information

Access to information during crisis, as well as the means to communicate it, is a basic humanitarian need. Thus, all people and populations have a fundamental right to generate, access, acquire, transmit, and benefit from information during crisis. The right to information during crisis exists at every phase of a crisis, regardless of the geographic location, political, cultural, or operational context or its severity.

Measuring the degree to which the right to information during crises is realized has at least three core groups of metrics. These core groups are as follows:

- *Ensuring Protection of HIAs:* The protection of HIAs can include the clear delineation of what constitutes humanitarian cyberspace, ensuring free and unfettered access of humanitarian actors to infrastructure necessary to connect with affected populations, and the enforcement of prohibitions against attacks on and exploitation of humanitarian information infrastructure and activities.¹
- *Equitable Provision of Communication Infrastructure and Capacity:* Realizing the right to information during a crisis should also be measured by how populations are equitably provided with the necessary physical infrastructure and the capacity to generate, transmit, and receive information. Equitable provision of these resources can include ensuring that economically and socially marginalized communities can connect to telecommunications networks, training and capacity building for communities to conduct HIAs when crises occur, and supporting efforts to strengthen and secure communications infrastructure in crisis-prone communities.
- *Removing Economic, Social, Cultural, and Political Barriers to Humanitarian Information:* The right to information during crises requires state and non-state actors to remove economic, social, cultural, and political barriers that often prevent communities from accessing information during crises. Examples of this work can include supporting the translation of humanitarian information products into local languages and culturally appropriate formats, addressing the role gender plays in access to data and ICTs, and removing regulatory barriers preventing relevant data from being accessible to specific affected communities and responders, in a

1. Gilman and Baker, “Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Humanitarian Emergencies.”



manner that respects the rights articulated herein.

Further metrics and indicators are necessary to identify related obligations and establish minimum technical standards.

D2. Realizing the Right to Protection

All people have a right to protection of their life, liberty, and security of person from potential threats and harms resulting directly or indirectly from the use of ICTs or data that may pertain to them. These harms and threats include factors and instances that impact or may impact a person's safety, social status, and respect for their human rights.

Realizing the right to protection from harm resulting from the use of ICTs and data can be measured by at least four core metrics, which include:

- *Building an Evidence Base for Understanding the Potential Threats and Harms Caused by HIAs:* To date, there has been little intentional and evidence-based research done to understand the unique threats and harms caused by HIAs in specific operational contexts. The development of protection standards tailored to HIAs depends on better studying these threats and harms, including the impacts of HIAs on particularly vulnerable populations.
- *Development and Adoption of Protection Standards for HIAs:* Current professional standards for protection work do not fully encompass the diverse range of actors and technologies that make up the current HIA ecosystem.² Protection standards specific to HIAs, drawing from the evidence base of past practice described above, will need to be both technologically and contextually detailed enough to be applied in specific operational environments.
- *Ensuring the Capacity to Protect Data, Including Data Minimization:* The right to protection from harm stemming from HIAs requires humanitarian information actors to establish and maintain an appropriate capacity necessary for secure data in full at each stage of its life cycle.³ Relatedly, capacity and approaches for minimizing data collection only to the defined scope of the activity planned should be established as well.^{4,5} Minimizing data collection to the defined scope of the planned activity may include limiting or eliminating collection of personal identifying information such as family names,

2. International Committee of the Red Cross, *Professional Standards for Protection Work*.
3. “Data Life Cycle,” accessed August 16, 2016, <http://www.bu.edu/datamanagement/background/data-life-cycle/>.
4. International Committee of the Red Cross, *Professional Standards for Protection Work*.
5. Nathaniel Raymond and Ziad Al-Achkar, “Building Data Responsibility into Humanitarian Action,” *UN Office for the Coordination of Humanitarian Affairs Policy and Studies Series*, no. 18 (May 17, 2016), https://docs.unocha.org/sites/dms/Documents/TB18_Data%20Responsibility_Online.pdf.



physical characteristics, or unique identification numbers, to name a few possible indicators.⁶

Securing the data lifecycle in full, from design and collection points through storage and subsequent analysis, may include combinations of digital and physical security measures designed to ensure that those contributing data cannot be tracked and subsequently targeted in association with the HIA.

- *Ensuring Accountability and Learning Through Documenting Critical Incidents:* At present, critical incidents (i.e., the loss of life, breaches of data storage facilities, and other injurious incidents or violations of human rights) are not captured and publicly shared by humanitarian actors in a routinized way, nor to the degree necessary for improving practice and being accountable to affected populations. Standard procedures and venues for capturing and sharing these incidents are necessary to realize the right to protection from harm related to HIAs, as well as the right to redress and rectification.

D3. Realizing the Right to Data Privacy and Security

All people have a right to have their personal information treated in ways consistent with internationally accepted legal, ethical, and technical standards of individual privacy and data protection. Any exception to data privacy and protection during crises exercised by humanitarian actors must be applied in ways consistent with international human rights and humanitarian law and standards.

Realization of the right to data privacy and security means that humanitarians have an obligation to build processes and safeguards into the implementation and governance of ICTs which minimize the potential for harm and privacy violations. They must provide mechanisms for the evaluation of humanitarian performance in upholding these rights and accountability to the populations served. These obligations proceed from the Red Cross/NGO Code of Conduct,⁷ which stipulates, “we hold ourselves accountable to both those we seek to assist and those from whom we accept resources,” the Sphere Protection Principles, which provide the imperative, “avoid exposing people to further harm as a result of your actions,”⁸ as well as the Humanitarian Charter,⁹ the Sphere Core Standards,^{10,11,12} and the nine commitments of the Core Humanitarian Standard.¹³

Notification: Subjects of data collection as part of HIAs should be made aware that their data will be collected prior to its collection occurring. This should include identification of the organization collecting the data, the uses for which the data is being collected, and any third parties which may be recipient to the data. Also identified should be the nature of the data collected and the means by which it shall be collected, policies that ensure the quality, security, and integrity of the data, and the means by which the subject can seek redress and rectification.

Data Minimization: Humanitarians must limit data collected to that which is necessary for specified purposes. These purposes must be explicit, legitimate, and determined at the time of data collection. Data must be obtained by lawful

7. International Federation of the Red Cross and Red Crescent and International Committee of the Red Cross, “The Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief.”
8. The Sphere Project, Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response, 33.
9. Ibid., 19.
10. Ibid., 68.
11. Ibid., 65.
12. Ibid., 58.
13. CHS Alliance, Groupe URD, and The Sphere Project, Core Humanitarian Standard: Core Humanitarian Standard on Quality and Accountability.



and fair means, with respect to the rights of the data subject, and with the consent of the subject where applicable.

Use Limitations: Humanitarians must not disclose, make available, share, or use personal data for purposes beyond the scope of those purposes explicitly defined at the time of collection, except with the consent of the data subject.

Security: Humanitarian actors must impose managerial and technical measures to protect against loss and the unauthorized access, destruction, use, modification, or disclosure of the data collected as a result of HIAs. Humanitarians must also adopt best practices for the handling of data to ensure against inadvertent misuse or loss, and develop a culture of security and privacy that guards against privacy and security breaches and ensures that all personnel can recognize common threats to data security and privacy. Organizations should:

- adopt and implement humanitarian sector minimal technical standards governing systems handling sensitive and personal data; adopt minimum training standards to ensure that ICT and information security personnel, individuals working with sensitive data, and other personnel are qualified; and
- implement standardized risk assessment protocols, third party independent audits of systems and personnel, and compliance testing and assurance.¹⁴

Governance & Accountability: Humanitarian actors engaged in HIAs must establish appropriate internal governance for the handling of PII and DII. This, at a minimum, includes:

- policies and procedures that are capable of handling sensitive data across the humanitarian data ecosystem;¹⁵
- implementation of privacy management programs appropriate to the scope of a project's

14. The Sphere Project, *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*, 305.

15. Raymond and Al-Achkar, "Building Data Responsibility into Humanitarian Action."

- 
- exposure to sensitive and personal data;¹⁶
 - mechanisms by which a data subject can seek recourse within a timely manner and with minimal costs;
 - internal mechanisms for oversight, critical incident response, the ongoing monitoring and reassessment of data collection;
 - routine and independent auditing of data governance and management practices; and
 - standardized legal agreements for data sharing where appropriate, including minimum technical standards to facilitate data sharing in a secure manner.

16. Organization for Economic Cooperation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.”

D4. Realizing the Right to Data Agency

Everyone has the right to agency over the collection, use, and disclosure of their personally identifiable information (PII) and aggregate data that includes their personal information, such as demographically identifiable information (DII). Populations have the right to be reasonably informed about information activities during all phases of information acquisition and use.

Realizing the right to data agency depends on the development of, and adherence to, minimum technical and ethical standards for data acquisition and use. Developing minimum standards to realize the right to data agency begins with identifying the legal, ethical, regulatory, and technical rules and norms that govern data agency in specific response contexts.¹⁷ Minimum technical and ethical standards for data acquisition and use must meet the following metrics:

- *Procedures for Notification and Informed Consent:* Any use of HIAs must be planned in a manner consistent with the principles of notification, informed participation, consent, and informed consent. Initial project planning must determine the level of notification and consent required, and standardized guidelines for this determination must be developed. Informed consent must be obtained prior to the collection of data with experimental purposes. The informed consent process must meet minimum standards for the provision of information, comprehension, and voluntariness.¹⁸
- *Experimental Review:* All HIAs which are experimental in nature should be subject to review by Institutional Review Boards (IRBs). There must be research and sector-wide agreement on what constitutes experimental procedures in the context of HIAs. Humanitarian actors also require training in how to determine which HIAs constitute experimental procedures and to identify which require IRBs.
- *Developing a Chain of Consent:* Data aggregation presents unique challenges to the realization of data agency. The aggregation of data may create data products that pose additional risks to affected populations compared to the unaggregated data. Because future technological developments

17. Raymond and Al-Achkar, “Building Data Responsibility into Humanitarian Action.”
18. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, “Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, Report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.”



and partnerships leading to data aggregation may not be foreseen, humanitarian actors must create and adhere to standardized data licensing agreements informed by assessments of additional risks attributable to data aggregation. Data licensing agreements must also capture the chain of consent, or the parameters of data use obtained in the informed consent process, at each stage of data aggregation and sharing.

- *Best Practices for Enfranchising Populations in HIA Design and Execution:* Humanitarian actors should use approaches, tools, and techniques that are culturally, logically, and operationally appropriate to the context in which HIAs are deployed. Participatory design is an ultimate goal of the development of HIAs, in order to ensure that the intent and effect of HIAs are first and foremost suited to the needs and preferences of the local population. Consistent feedback loops and formal channels for populations affected by crises to provide input about decisions that affect their right to data agency must be established. As part of these feedback loops and channels, crisis-affected populations must be enfranchised to participate in these processes, including the provision of information about their right to data agency.

D5. Realizing the Right to Redress and Rectification

All people have the right to rectification of demonstrably false, inaccurate, or incomplete data collected about them. As part of this right, individuals and communities have a right to establish the existence of and access to personal data collected about themselves. All people have a right to redress from relevant parties when harm was caused as a result of either data collected about them or the way in which data pertaining to them were collected, processed, or used.

To realize the right to redress, humanitarians and other actors must be accountable to crisis-affected populations. Humanitarians should keep the following in mind as they work with HIAs: Who is responsible if a HIA based on “bad” data causes harm, and what might adequate redress look like?

Realizing the right to redress will involve at least three metrics:

- *Designation of humanitarian actors who are accountable for addressing critical incidents and complaints:* The right to redress requires humanitarian agencies to have designated personnel who process and address relevant complaints, and who have certain obligations when critical incidents occur. This function may best be implemented as an independent and inter-agency humanitarian data supervisory body that has jurisdiction across organizations.
- *Clearly define who is accountable for data-related harms, and what they will do to address these harms:* Humanitarian organizations must clearly define who holds ultimate responsibility for harms to affected populations that stem from HIAs. Responsible parties must then create protocols for addressing complaints and engaging in rectification, erasure, and redress activities. This must be done *before these protocols are actually needed*, not after. These protocols should be as transparent as possible, enabling affected populations to comment on and improve them.
- *Build awareness amongst affected populations of their right to redress:* Affected populations must be aware that they have the right to access and rectify their data, and to receive redress if this data has caused them harm. Humanitarians need to develop plans and best practices for communicating this right to populations in clear and context-sensitive ways, with an emphasis on transparency and inclusion.

Conclusion: Towards a Rights-Based Approach

Humanitarianism has traditionally been anchored on two foundational concepts: all human beings have certain unalienable rights to assistance and protection, and humanitarian actors have obligations to adhere to agreed standards of professional ethics rooted in a duty to realize these rights. In the networked age, the continued relevance of the humanitarian project thus depends on translating these rights and obligations into a normative framework appropriate for the unique challenges and opportunities that the growing reliance on digital data and ICTs presents.

This initial articulation of a rights-based approach to these issues is the necessary first step in the continued evolution of humanitarian practice. It is now incumbent on the humanitarian sector to use the Signal Code as one tool among many to begin to address the gaps in international humanitarian and human rights law and standards around humanitarian information activities. These gaps will continue to be laid bare by the adoption of new information technologies by responders and affected populations alike in both predictable and unexpected ways.

Emerging international legal norms around data privacy and security make this effort all the more urgent. Without concerted and intentional action by all stakeholders, standards of professional ethics for humanitarians risk becoming increasingly anachronistic and out of step with the impact technology is having on both the contexts in which humanitarians operate and the populations they seek to serve.

Four crucial, interconnected steps are required of humanitarian actors, governments, private sector entities, and international agencies:

- The human rights of all people to information during crisis, including their rights to protection from harm and human rights violations related to the use of information, must be formally and explicitly recognized and codified under international humanitarian and human rights law;
- The ethical obligations of humanitarian actors engaged in humanitarian information activities to realize these rights must be articulated and agreed as

- part of accepted standards of professional conduct;
- Minimum technical standards for the responsible design and execution of humanitarian information activities based on agreed human rights principles and ethical obligations must be developed and integrated into current humanitarian practice; and
- Humanitarian actors, governments, private sector entities, and international agencies must collaboratively and quickly support the emergence of an accepted normative framework for humanitarian information activities that fuses human rights, law, ethics, and practice.

The networked age is one of new promise and new peril for crisis affected populations and those who assist them. Technological advancement alone is never enough to navigate the dangers and opportunities of any emerging historical epoch. The continued protection, articulation, and integration of human rights into how humanitarians apply any technology has historically proven the only pathway to responsibility and justice.

The networked age is no different. While the challenges the field faces from the issues raised by The Signal Code may be complex, the way forward is now clear. How any rights-based approach to humanitarian information activities will be formulated, agreed and implemented is a matter for rigorous debate. Whether a rights-based approach is now required, however, is not.

Glossary

The primary sources for the glossary below include the ReliefWeb Glossary of Humanitarian Terms, the International Committee of the Red Cross' "Exploring Humanitarian Law Glossary", the glossary included in the Sphere Standards, and other relevant sources.

Accountability: The means or process by which organizations and individuals are held accountable by different stakeholders, with the goal of ensuring their activities are conducted appropriately and resources are used responsibly.

Affected Population: People (individuals and groups) impacted by a disaster or crisis situation. May also be called “crisis-affected population” or “disaster-affected population.”

Complex Emergency: A humanitarian crisis in a country, region, or society where there is total or considerable breakdown of authority resulting from internal or external conflict, and which requires an international response that goes beyond the mandate or capacity of any single agency and/or the ongoing UN country program (IASC).

Conflict: A social, factual situation in which at least two parties are in serious, usually protracted, disagreement. In humanitarian contexts, “conflict” usually refers to violent or armed disagreement, or scenarios in which there is a threat of violence to certain populations.

Crisis Response Cycle: All activities pertaining to crisis preparedness and response, including pre-crisis preparedness, early crisis response, and long-term activities. These activities tend to be (but are not always) organized in a predictable, cyclical system.

Data: Information—either quantitative or qualitative—that is collected and analyzed for the purpose of decision-making. In the humanitarian context, “data” usually refers to information in an unprocessed or unorganized form that can be digitally stored and interpreted.

Data Controller: A party competent to make decisions about the contents and use of personal data, whether that data is collected, stored, or processed by that party or an agent or agents operating on its behalf.

Data Life-Cycle: The life-cycle that a datum or data set undergoes –usually including collection, storage, processing, transmission, and consumption as stages.

Data Minimization: The principle that a data controller should limit the amount of data collected and the length of time the data is stored to that which is strictly necessary for accomplishing

a specified purpose. In the humanitarian context, the principle directly opposes the collection of as much data as possible in the service of unanticipated or currently unknown future needs.

Data Preparedness: The ability of organizations to be ready to responsibly and effectively deploy and manage data collection and analysis tools, techniques and strategies in a specific operational context before a disaster strikes.

Demographically Identifiable Information (DII): Data points that enable the identification, classification, and tracking of individuals, groups, or multiple groups of individuals by demographically defining factors. These may include ethnicity, gender, age, occupation, and religion. May also be referred to as Community Identifiable Information, or “CII.”

Emergency: An event (usually unforeseen) in which it is necessary to immediately meet the needs of people at risk. This can include natural and technological disasters as well as armed conflict.

Experiment: To explore the effects of manipulating a variable. To test or implement a new invention or process based on untested theory, procedures, or techniques.

Humanitarian Actor(s): Organization(s) or individual(s) of a humanitarian and impartial nature involved in crisis response.

Humanitarian Information Activities (HIAs): Activities and programs that may include the collection, storage, processing, analysis, further use, transmission, and public release of data and other forms of information. HIAs also include the establishment and development of communications capacity and infrastructure by responders and/or populations. These activities occur as part of humanitarian action throughout the response cycle and include, but are not limited to, improving situational awareness; disaster preparedness and mitigation; intervention design and evaluation; connecting populations to response activities and to each other; and supporting ongoing operations, including the delivery of assistance.

Information Communication Technologies (ICTs): Devices, sensors, software, hardware, systems, and networks used for

the collection, processing, analysis, and dissemination of information often, though not always, in a digital format.

Informed Consent: Informed consent is when subjects of data collection or interventions agree to participate in an experiment, intervention, or process after having achieved a full understanding of what the activity involves and its potential impact on them and their own welfare.

Informed Participation: A state in which populations participate in a given experiment or project with an understanding of how their data will be used, and with the knowledge that they can give input into the ongoing use of this data.

International Humanitarian Law (IHL): A set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare. International humanitarian law is also known as the law of war or the law of armed conflict and includes the Geneva Conventions. These laws govern what constitutes humanitarian action, the conduct of war, and protected persons.

Natural Disaster: Events brought about by natural hazards with catastrophic results, often including loss of life and damage to infrastructure and local economies.

Networked Age: Refers to the currently ongoing proliferation of information communication technologies and the commonplace use of digital data through online networks, including the impact these technologies have on humanitarian activity.

Personal Data Breach: A security breach that leads to the accidental or intentional release of secure data to untrusted or unknown sources can include the loss, alteration, and destruction of data.

Personally Identifiable Information (PII): Information that can be used to identify a specific individual, this may include a name, a personal address, online accounts,

and identifiers that are specific to a person's "physical, physiological, mental, economic, cultural or social identity."¹

Preparedness: Actions and activities taken in advance of a disaster, intended to minimize the impact of either expected or unforeseen hazards on people and property.

Protection: Term describing all activities "aimed at ensuring full respect for the rights of the individual in accordance with the letter and the spirit of the relevant bodies of law, i.e. human rights law, international humanitarian law and refugee law."² These activities include actions and programs to safeguard the human security and wellbeing of vulnerable populations.

Processing: Operations and theory concerned with gathering, describing, manipulating, storing, retrieving, and classifying data or information.

Rectification: The correction of inaccurate or incomplete personal data.

Redress: Satisfaction of some kind for damages or injury incurred by another's actions.

Transparency: Refers to a state of honesty and openness about one's actions and motivations—linked to accountability.

Vulnerable Populations: Refers to particular groups who are especially susceptible to certain difficulties and hazards, often due to specific factors.

1. European Parliament. "Directive 2016/680 of the European Parliament and the Council of the European Union." Official Journal of the European Union 59, no. L119 (2016): 89–131. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN>.
2. International Committee of the Red Cross. "Strengthening Protection in War: A Search for Professional Standards." Geneva, 2001. <https://shop.icrc.org/strengthening-protection-in-war-a-search-for-professional-standards-2369.html>.

Bibliography

- African Union. "African Union Convention on Cybersecurity and Personal Data Protection" EX.CL/846 (2014).
- Article XIX: Global Campaign for Free Expression.
"Humanitarian Disasters and Information Rights: Legal and Ethical Standards on Freedom of Expression in the Context of Disaster Response," no. April (April 2005). <http://article19.org/data/files/pdfs/publications/freedom-of-information-humanitarian-disasters.pdf>.
- Asia-Pacific Economic Cooperation. "APEC Privacy Framework." Vol. APEC#205-S. Singapore, 2005. http://publications.apec.org/publication-detail.php?pub_id=390.
- Betts, Alexander, Louise Bloom, Josiah Kaplan, and Naohiko Omata. "Refugee Economies: Rethinking Popular Assumptions." Oxford, 2014. <http://www.rsc.ox.ac.uk/files/publications/other/refugee-economies-2014.pdf>.
- Brunwasser, Matthew. "A 21st-Century Migrant's Essentials: Food, Shelter, Smartphone." *The New York Times*. August 25, 2015. http://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=0.
- Buchanan-Smith, Margie, J Court, I Hovland, and J. Young. "How the Sphere Project Came into Being: A Case Study of Policy Making in the Humanitarian-Aid Sector and the Relative Influence of Research." *Bridging Research and Policy in Development: Evidence and the Change Process*, no. July (2005). <http://www.odi.org/publications/170-bridging-research-policy-development-evidence-change-process>.
- Chamales, George, and Rob Baker. "Securing Crisis Maps in Conflict Zones." In *2011 IEEE Global Humanitarian Technology Conference*, 426–30. IEEE, 2011. doi:10.1109/GHTC.2011.47.
- CHS Alliance, Groupe URD, and The Sphere Project. *Core Humanitarian Standard: Core Humanitarian Standard on Quality and Accountability*, 2014. https://corehumanitarianstandard.org/files/files/Core_Humanitarian_Standard - English.pdf.
- Cline, Jay. "Data Quality -- the Forgotten Privacy Principle." *ComputerWorld*, September 2007. <http://>

www.computerworld.com/article/2541015/security/0/data-quality----the-forgotten-privacy-principle.html.

Communaute Economique des Etats de l'Afrique de l'Ouest/Economic Community of West African States. "Supplementary Act A/SA.1/01/10 On Personal Data Protection within ECOWAS," 2010. <http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf>.

Council of Europe. "Explanatory Report of Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." *European Treaty Series*. Strasbourg, 1981. <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

Crawford, Kate, and Megan Finn. "The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters." *GeoJournal* 80, no. 4 (August 1, 2015): 491–502. doi:10.1007/s10708-014-9597-z.

"Data Life Cycle." Accessed August 16, 2016. <http://www.bu.edu/datamanagement/background/data-life-cycle/>.

Dette, Rahel. "Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts," 2015.

Eskridge Jr., William N. "The Relationship between Obligations and Rights of Citizens." *Fordham Law Review* 69, no. 5 (2001): 1721–51.

European Commission. "The Charter of Fundamental Rights of the European Union." *Official Journal of the European Communities* 43, no. C364 (December 18, 2000): 1–22. doi:10.1108/03090550310770974.

European Data Protection Supervisor. "Guidelines on the Rights of Individuals with Regard to the Processing of Personal Data," February 25, 2014. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf.

European Parliament. "Directive 2016/680 of the European Parliament and the Council of the European Union." *Official Journal of the European Union* 59, no. L119 (April 4, 2016): 89–131. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN>

———. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of

Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.” *Official Journal of the European Union* 38, no. L281 (1995): 0031–0050.

———. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).” *Official Journal of the European Union* 59, no. L119 (April 4, 2016): 1–88

———. “Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data.” *Official Journal of the European Communities* 44, no. L8 (January 12, 2001): 0001–0022. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF>.

Floridi, Luciano. *The Ethics of Information*. Paperback. Oxford: Oxford University Press, 2013.

Geiss, Robin. “Cyber Warfare: Implications for Non-International Armed Conflicts.” *International Law Studies* 89 (2013): 627–45.

Gemalto. “Data Breach Statistics 2016: First Half Results Are in,” 2016. <http://blog.gemalto.com/security/2016/09/20/data-breach-statistics-2016-first-half-results/>.

Gilman, Daniel, and Leith Baker. “Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Humanitarian Emergencies.” *UN Office for the Coordination of Humanitarian Affairs Policy and Studies Series*, no. 11 (October 2014). <https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf>.

Gordon, Grant. “Monitoring Conflict to Reduce Violence: Evidence from a Satellite Intervention in Darfur,” March

3, 2016. <http://www.grantmgordon.com/wordpress/wp-content/uploads/2010/06/GG-EoD.pdf>.

Greenleaf, Graham. "Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority." *Privacy Laws Business International Report*, January 30, 2015.

———. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108." *International Data Privacy Law* 2, no. 2 (May 1, 2012): 68–92. doi:10.1093/idpl/ips006.

Hannides, Theodora, Nicola Bailey, Dwan Kaoukji, Leila Younes, Reem Karssli, Tony Spence, Farsi translators Ajmal Wafa, et al. "Voices of Refugees: Information and Communication Needs of Refugees in Greece and Germany," 2016. <http://www.bbc.co.uk/mediaaction/publications-and-resources/research/reports/voices-of-refugees>.

Institute, Overseas Development. "Humanitarian Space: Concept, Definitions and Uses Meeting Summary Humanitarian Policy Group." In *Roundtable*, 1–7, 2010. <https://www.odi.org/events/2655-humanitarian-space-concepts-definitions-uses>.

International Committee of the Red Cross. "Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Forth Geneva Convention)." *United Nations Treaty Series* 75, no. 287 (August 12, 1949): 288–416. <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/7c4d08d9b287a42141256739003e636b/6756482d86146898c125641e004aa3c5?OpenDocument>.

———. *Professional Standards for Protection Work*. 2013th ed. Vol. 0999/002. Geneva, 2013. <https://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf>.

———. "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)." *United Nations Treaty Series* 1125, no. 17512 (1978): 3–608. https://treaties.un.org/doc/Publication/UNTS/Volume_1125/v1125.pdf.

———. "Strengthening Protection in War: A Search for Professional Standards." Geneva, 2001. <https://shop.icrc.org/strengthening-protection-in-war-a-search-for-professional-standards-2369.html>.

International Federation of the Red Cross and Red Crescent, and International Committee of the Red Cross. "The Code of

Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief," 1994. <http://www.ifrc.org/Global/Publications/disasters/code-of-conduct/code-english.pdf>.

Leiber, Francis. *Manual of Political Ethics, Vol 2.* Boston: Charles C. Little and James Brown, 1839. <https://books.google.com/books?id=MwVAAAAAYAAJ>.

Lester, Anthony Paul, David Pannick, and J.W. Herberg, eds. *Human Rights Law and Practice.* Third. London: LexisNexis, 2009.

McDonald, Sean Martin. "Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation." *The Centre for Internet and Society*, no. 2016.01 (March 1, 2016). <http://cis-india.org/papers/ebola-a-big-data-disaster>.

McIvor, Chris. "Data or Dialogue? The Role of Information in Disasters." In *World Disasters Report 2005*. International Federation of the Red Cross and Red Crescent Societies, 2005. <http://www.ifrc.org/en/publications-and-reports/world-disasters-report/wdr2005/wdr-2005---chapter-1-data-or-dialogue-the-role-of-information-in-disasters/>.

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. "Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, Report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research." *Federal Register*. Vol. 44, April 18, 1979. <http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/>.

Organization for Economic Cooperation and Development. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2013. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Organization of American States. "Privacy and Data Protection." Rio de Janeiro: Organization of American States, 2015. http://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf.

Pictet, Jean. "The Fundamental Principles of the Red Cross: Commentary." *International Federation of the Red Cross and Red Crescent Societies*, 1979.

Raymond, Nathaniel. "Beyond 'Do No Harm' and Individual Consent: Reckoning with the Emerging Ethical Challenges of

Civil Society's Use of Data." In *Group Privacy: New Challenges of Data Technologies*, edited by Linnet Taylor, Luciano Floridi, and Bart van der Sloot. Springer International Publishing, 2016. doi:10.1007/978-3-319-46608-8.

Raymond, Nathaniel, and Ziad Al-Achkar. "Building Data Responsibility into Humanitarian Action." *UN Office for the Coordination of Humanitarian Affairs Policy and Studies Series*, no. 18 (May 17, 2016). https://docs.unocha.org/sites/dms/Documents/TB18_Data%20Responsibility_Online.pdf.

Raymond, Nathaniel, Britney Card, and Ziad Al-Achkar. "What Is 'Humanitarian Communication'? Towards Standard Definitions and Protections for the Humanitarian Use of ICTs." *European Interagency Security Forum*, no. August (2015): 1–5. <https://www.eisf.eu/wp-content/uploads/2015/10/2041-EISF-2015-What-is-humanitarian-communication.pdf>.

Raymond, Nathaniel, Caitlin Howarth, and Jonathan Hutson. "Crisis Mapping Needs an Ethical Compass." *Global Brief*, February 2012. <http://globalbrief.ca/blog/2012/02/06/crisis-mapping-needs-an-ethical-compass/>.

Solove, Daniel J. "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126, no. 7 (2013): 1880–1903.

———. *Understanding Privacy*. Cambridge: Harvard University Press, 2010.

Stoffels, Ruth Abril. "Legal Regulation of Humanitarian Assistance in Armed Conflict: Achievements and Gaps." *Revue Internationale de La Croix-Rouge/International Review of the Red Cross* 86, no. 855 (September 27, 2004): 515. doi:10.1017/S1560775500181027.

The Council of Europe. "Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data" ETS No.108 (1981). <http://www.refworld.org/docid/3dde1005a.html>.

The European Parliament. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the

Free Movement of Such Data.” *Official Journal of the European Union* 38, no. L281 (1995): 0031–0050.

The Sphere Project. *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*. 3rd ed. Bourton on Dunsmore, Rugby: Practical Action Publishing, 2011.

Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10: The Medical Case. Vol. 2. Washington, DC: United States Government Printing Office, 1949.

UNESCO. “Explanatory Memorandum On The Elaboration Of The Preliminary Draft Declaration On Universal Norms On Bioethics.” In *First Intergovernmental Meeting of Experts Aimed at Finalizing a Draft Declaration on Universal Norms on Bioethics*, 16. Paris, 2005. <http://unesdoc.unesco.org/images/0013/001390/139024e.pdf>.

———. “Records of the General Conference.” In *Resolution 15 Adopted by the General Conference at Its 33rd Session*, 1:250. Paris, 2005. <http://unesdoc.unesco.org/images/0014/001428/142825e.pdf#page=80>.

United Nations. “Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operation.” *Treaty Series* 2296, no. 40906 (January 8, 2005): 5. <https://treaties.un.org/doc/Publication/UNTS/Volume%201522/v1522.pdf>.

———. “The Foundation of International Human Rights Law.” Accessed September 22, 2016. <http://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html>.

United Nations General Assembly. “Guidelines for the Regulation of Computerized Personal Data Files.” United Nations General Assembly Resolutions 45, no. 95 (1990). <http://www.refworld.org/pdfid/3ddcafaac.pdf>.

———. “United Nations Convention on the Law of the Sea.” *United Nations Treaty Series* 1833, no. 31363 (1994). <https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280043ad5>.

United Nations General Assembly. “International Covenant on Civil and Political Rights.” *United Nations Treaty Series* 999, no. 14668 (1976): 171.

<https://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf>.

———. “Report of the International Law Commission,” 2016. http://legal.un.org/docs/?path=..ilc/reports/2016/english/a_71_10.pdf&lang=EFSRAC.

———. “Strengthening of the Coordination of Humanitarian Emergency Assistance of the United Nations” A/RES/46/1 (December 19, 1991). <http://www.un.org/documents/ga/res/46/a46r182.htm>.

———. “Universal Declaration of Human Rights.” *United Nations General Assembly Resolutions* 217 A, no. III (December 10, 1948): 71–79.

United Nations Human Rights Council. *The Promotion, Protection and Enjoyment of Human Rights on the Internet. United Nations Human Rights Council Resolutions*, 2016. <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement>.

United Nations Population Fund. “Human Rights Principles.” *UNFPA*, 2005. <http://www.unfpa.org/resources/human-rights-principles>.

Wagner, Johanna G. “An IHL/ICRC Perspective on Humanitarian Space.” *Humanitarian Exchange*. London, December 2005. <http://odihpn.org/wp-content/uploads/2006/01/humanitarianexchange032.pdf>.

Weatherall, Thomas. *Jus Cogens: International Law and Social Contract*. Cambridge: Cambridge University Press, 2015.

World Health Organization. *International Health Regulations (2005)*. 3rd ed. Geneva, 2016. <http://www.who.int/ihr/publications/9789241580496/en/>.

World Medical Association. “World Medical Association Declaration of Helsinki Ethical Principles for Medical Research Involving Human Subjects,” June 1964. <http://www.wma.net/en/30publications/10policies/b3/>.