IAGS
INTERNATIONAL ASSOCIATION OF GENOCIDE SCHOLARS

Genocide Studies and Prevention: An International Journal

Volume 11 | 2017 Information and Communications Technologies in Mass Atrocities Research and Response

Issue 1 | Article 5

Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response

Kristin Bergtora Sandvik
University of Oslo

Nathaniel A. Raymond
Harvard University

Abstract.
Information Communication Technologies (ICTs) are now being employed as a standard part of mass atrocity response, evidence collection, and research by non-governmental organizations, governments, and the private sector. Deployment of these tools and techniques occur for a variety of stated reasons, most notably the ostensible goal of "protecting" vulnerable populations. However, these often experimental applications of ICTs and digital data are occurring in the absence of agreed normative frameworks and accepted theory to guide their ethical and responsible use. This article surveys the current state-of-the-art of ICT use in mass atrocity response and research to identify harms and hazards inherent in the use of ICT-centric approaches in mass atrocity producing environments. The article proposes an initial theory of harm for evaluating the potential risks and impacts of these applications as a critical component of developing ethical standards for the responsible use of ICTs in the mass atrocity response context.

Recommended Citation
Sandvik, Kristin Bergtora and Raymond, Nathaniel A. (2017) "Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response," *Genocide Studies and Prevention: An International Journal*: Vol. 11: Iss. 1: 9-24.
DOI:
http://doi.org/10.5038/1911-9933.11.1.1454

Available at: https://scholarcommons.usf.edu/gsp/vol11/iss1/5

Keywords.
Mass Atrocity, Information Communication Technology, Crisis Mapping, Humanitarian, Human Rights, Ethics

Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response

Kristin Bergtora Sandvik
University of Oslo
Oslo, Norway

Nathaniel A. Raymond
Harvard University
Cambridge, Massachusetts, USA

Introduction

Historically, the international community's response, or lack thereof, to mass atrocities, has been shaped by the absence of timely and accurate information.[1] The past two decades have witnessed non-governmental organizations, international agencies, governments, and private sector actors designing, adopting, and employing information communication technologies (ICTs) including smartphone apps, remote sensing platforms such as satellite imagery analysis, surveillance drones and other forms of digital data collection and analytics, as standard components of sectoral and cross-sectoral responses to both the threat and alleged committal of mass atrocities in a variety of operational and geographic contexts. Throughout this period, the use of ICTs has metamorphosed from consisting of a series of prototype use cases of these tools and techniques to become a commonplace component of the human rights and humanitarian sector's response to mass atrocity and human security crisis scenarios. Accompanying this mainstreaming is a set of generalized and, to date, largely unsubstantiated claims that ICT changes the nature and effectiveness of mass atrocity response.

So far, limited conceptual scholarly attention has been given to the progress-claims made on behalf of ICT technologies and how these claims correspond to their actual impact on the broader field of mass atrocity response. This is problematic, because this form of technology optimism, or even utopianism, impacts the distribution of resources, field practices and the rules and norms that regulate the use of these interventions. In this article, we contest the theory of change presented by various actors in the mass atrocity field. According to this theory, ICTs are not only force multipliers with respect to civil society's ability to address atrocities, but the use of ICT in itself represents a form of response that enhances the protection of civilians. In doing so, we make three arguments.

First, we argue that there is no evidence of the existence of what can be referred to as a causal Protective or Preventative Effect (PPE) from the use of ICTs in mass atrocity producing environments. In our coinage, the PPE is conceptualized as the following: The use of technology in mass atrocity contexts are largely preceded by the encoding of assumptions and aspirations into ICTs having an inherently Ambient Protective Effect (APE); i.e. casually transforming the threat matrix of a particular atrocity producing environment in a way that improves the human security status of targeted populations. Second, we suggest that more attention needs to be paid to the reverse effect, namely that the collection and distribution of demographically identifiable information (DII) in disasters can instead be a causal vector for harm. Building on Raymond, we define DII as either individual and/or aggregated data points that allow inferences to be drawn that enable the classification, identification, and/or tracking of both named and/or unnamed individuals, groups of individuals, and/or multiple groups of individuals according to ethnicity, economic class, religion, gender, age, health condition, location, occupation, and/or other demographically defining

[1] Scott Strauss, "Identifying Genocide and Related Forms of Mass Atrocity," *United States Holocaust Memorial Museum* 7 (2011), accessed May 21, 2017, https://www.ushmm.org/m/pdfs/20111219-identifying-genocide-and-mass-atrocity-strauss.pdf. As observed by Strauss, conceptual clarity matters: For mass atrocity prevention and response alike, it is necessary to have a working definition of the class of events that can trigger civic activity or political and military responses. At the same time, the term "mass atrocity" covers a range of events (beyond common standards such as genocide, crimes against humanity or mass violence) that are themselves the objects of contestation and analytical confusion. For the purposes of this article, we take up the commonly understood notion of mass atrocity as widespread and systematic violence against civilians.

Kristin Bergtora Sandvik and Nathaniel A. Raymond, "Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response" *Genocide Studies and Prevention* 11, 1 (2017): 9-24. ©2017 *Genocide Studies and Prevention*.
http://doi.org/10.5038/1911-9933.11.1.1454

factors.[2] We suggest that the absence of a shared theory of harm and a corresponding framework for applying it to these new and evolving ethical challenges represents a key challenge. Third, to that end, we begin to articulate the core components of such theory of harm with respect to the use of ICT in mass atrocities. In our articulation, harm can arise from a wide array of technology-based practices, interactions and policy considerations in mass atrocity response. As a first step, we need to do the work of linking *data security* (privacy and data protection) and *cybersecurity* more comprehensively to *human security*. As a second step in our attempt to articulate a theory of harm, we put forward the view that DII requires its own category and science of identifiable data specific to itself. As a third step, we propose a closer focus on preparedness: We argue that mass atrocity and human security fields more broadly are characterized by missing conversations about tradeoffs before tech deployment. As a fourth step, we point to the need for greater reflexivity: we argue that it is necessary for response actors to take the differences between the ideologies, means, methods and objectives of humanitarian service provision and human rights truth provision-oriented communities seriously, and to more consciously reflect on the significance of this difference for one's own work. The fifth element of our theory of harm relates to ourselves as mass atrocity responders, and the ethical limits to *how far* we can go to digitally protect our operations.

The article proceeds as follows. We begin by briefly describing the rise of ICT technologies in mass atrocity response. We then argue that seen through the theoretical prism of technological utopianism, the arguments made on behalf of ICT technologies go beyond the notion of ICT as a force multiplier to claim that monitoring and information gathering may itself be equated to enhanced protection of civilians.[3] Next, we offer a four-pronged critique of the ICT progress narrative. We flesh out the components of the ambient protective or preventative effect; and describe the emergence of ICT as a site of ethical precariousness and as capable of causing actual harm to the response, to responders, and most importantly, to civilians who are the targets of mass atrocities. In the final part, we begin to lay out a theory of harm that can help us understand and address this issue. We conclude by arguing that our attempt at offering a theory of harm can assist in developing a means for logging and evaluating critical incidents, including standard definitions and procedures used by funders, governments, and local communities to evaluate past projects and prevent the infliction of harm from similar, future deployments.

The Rise of ICT in Mass Atrocity Response

These mass atrocity response specific uses of ICTs can include, but are not limited to, the following: Satellite imagery collection and analysis[4]; surveillance drones[5]; the use of crowd mapping and social media platforms[6]; and Big Data and algorithmic, machine-learning techniques to process large volumes of digital data from multiple sources. Increasingly, these individual tools and techniques

[2] Nathaniel A. 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 et al. (Cham: Switzerland, Springer International Publishing, 2017), 67-82.

[3] Christopher Tuckwood, "The State of the Field: Technology for Atrocity Response," *Genocide Studies and Prevention: An International Journal* 8, 3 (2014), 9. Our argument is concerned with different objectives than those articulated by Tuckwood, who argues that "recent years have seen a marked decline in the brand of 'cyber utopianism' that predicted the inevitable arrival of human rights and liberal democracy following rapidly on the heels of internet access in many of the world's dangerous places. Very few observers still believe that simply introducing an unspecified category of tools labeled 'technology' will be the panacea to defend human rights and save lives."

[4] Tanya Notley and Camellia Webb-Gannon, "FCJ-201 Visual Evidence from Above: Assessing the Value of Earth Observation Satellites for Supporting Human Rights," *The Fibreculture Journal* 27 (2016), accessed May 21, 2017, http://twentyseven.fibreculturejournal.org/2016/03/21/fcj-201-visual-evidence-from-above-assessing-the-value-of-earth-observation-satellites-for-supporting-human-rights/.

[5] Kristin Bergtora Sandvik and Kjersti Lohne, "The Rise of the Humanitarian Drone: Giving Content to an Emerging Concept," *Millennium-Journal of International Studies* 43, no.1 (2014), 145-164; Kristin Bergtora Sandvik and Maria Gabrielsen Jumbert, *The Good Drone* (New York: Routledge, 2016).

[6] Ryan Burns, "Rethinking Big Data in Digital Humanitarianism: Practices, Epistemologies, and Social Relations," *GeoJournal* 80, no. 4 (2015), 477-490.

are now being integrated together into combined applications that seek to fuse together several streams of data from different sources and formats into an amalgamated data product. While the deployment of each of these technologies takes place in discrete fields (humanitarianism, human rights, etc.) that are described and discussed by separate academic literatures, there is increasing recognition of responsible data management as *the* key crosscutting issue.[7]

The specific applications of these technologies and platforms are diverse and constantly evolving, but can be generally divided into two broad categories of prevention/response and justice/accountability: the uses that seek to create unique situational awareness for population protective purposes and informing response activities; and use cases aimed at detecting and/or documenting evidence of alleged crimes for judicial and/or advocacy purposes. In recent years, the intensifying adoption of the ICT technologies for mass atrocity response has commonly been presented as an expedient and substantive response to the gross human rights abuses arising from ongoing armed conflicts in non-permissive environments such as Syria, Iraq, South Sudan, Yemen, Libya and others. Additionally, the adoption of these technologies appears to be spurred, in large part, by a set of key factors, namely their comparatively low cost in comparison to other, analog interventions and their ability to be remotely deployed in highly lethal, non-permissive environments that preclude traditional, ground-based approaches.

"Hacking" Mass Atrocities: Technology Adoption as a Theory of Change

Thus, ICTs are now effectively treated as indispensable "force multipliers" that may either supplement or, in some cases, supplant mass atrocity responses that rely on humans physically making contact with other humans in the places where mass atrocity events are occurring. The adoption of an ever more technology-reliant and increasingly "remote" posture has encoded within it an implicit aspiration to literally predict, prevent and deter these crimes as a direct causal result of deploying these modalities. We propose that this increasingly publicly expressed vision that technology itself can fundamentally alter the calculus of whether and how mass atrocities occur demonstrates that civil society actors have done more than simply adopt tools and techniques: They have adopted a theory of change based on technological utopianism as well, a theory that posits technological change is inevitable, problem-free and progressive.

Technological utopianism is a belief in technological progress as inevitable, and in technology as the vehicle for "achieving a 'perfect' society in the near future."8 This theory of change can be illuminated through Morozov's concept of "solutionism", described as "the idea that given the right code, algorithms and robots, technology can solve all of mankind's problems, effectively making life "frictionless" and trouble-free."[9] In the cybersecurity field, cyber-utopianism refers to "a naïve belief in the emancipatory nature of online communication," along with a refusal to acknowledge any negative impact of the Internet on society.[10] We argue that the emergence of ICTs as a perceived remote, force multiplication capability for civil society actors responding to alleged mass atrocities has, critically, dovetailed with the narrative that more information about a mass atrocity producing situation can intrinsically increase the chances of preventing or mitigating these scenarios. As Pryce writes in *How to Prevent a Mass Atrocity*,

[7] Nathaniel A. Raymond, Ziad Al Achkar, et al, "Building Data Responsibility into Humanitarian Action," *United Nations Office for the Coordination of Humanitarian Affairs,* (2016). Also, Nathaniel A. Raymond, Caitlin Howarth, and Jonathan Hutson, "Crisis Mapping Needs an Ethical Compass," *Global Brief* 6 (2012), accessed May 21, 2017, http://globalbrief.ca/blog/2012/02/06/crisis-mapping-needs-an-ethical-compass/.

[8] Howard P. Segal, "The Technological Utopians," in *Imagining Tomorrow: History, Technology and The American Future, ed. Joseph J. Corn, (Cambridge, MA: MIT Press, 1986).*

[9] Ian Tucker, "We are Abandoning All the Checks and Balances," *The Guardian*, March 9, 2013, accessed May 21, 2017, https://www.theguardian.com/technology/2013/mar/09/evgeny-morozov-technology-solutionism-interview.

[10] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011). Milton Mueller, *What is Evgeny Morozov Trying to Prove? A Review of the Net Delusion* (Internet Governance Project, 2011), accessed May 21, 2017, www.internetgovernance.org/2011/01/13/what-is-evgeny-morozov-trying-to-prove-a-review-of-the-net-delusion.

> Early warning networks in countries at risk are essential, whether they involve tapping into worldwide Diasporas for the wealth of knowledge and contacts they provide, or making use of cell phone technology for immediate access to unfolding events.[11]

It should be noted that this perception is supported and reinforced by similar developments in adjacent fields of human security-related rescue and response. Generally, with the rise of Big Data, data visualization has become central to the understanding of societal problems and their potential solutions.[12] In the field of humanitarian action, a key driver behind the rise of technology is the increasing conflation between information and protection: embedded within the embrace of extensive monitoring is the implicit promise of better performance.[13] More broadly this is connected to the widespread notion that "knowing about atrocities" through imagery and other data streams somehow mobilizes empathy and engenders political action.[14]

Herscher describes how the public viewing of images was understood to motivate public action, and how, with the *Eyes on Darfur* Campaign, the public viewing of satellite images was viewed as public action in itself.[15] In a different example, an October 2010 report from ICT4D Foundation expresses the decidedly solutionist aspiration that the deployment of these technologies themselves can realize a "dream of rescue" for imperiled populations succinctly, stating:

> Civil society is becoming increasingly involved in the search and design of digital innovations for addressing the challenges of genocide. A recent example is Project 10^100, a competition hosted by Google, where the idea of creating a genocide monitoring and alert system was one of the sixteen finalists. The ideas included reducing crimes against humanity by aggregating data, including pertinent statistics, the history and geography of specific conflicts, local cultures, geostrategic interests, by using e.g. updated dynamic web maps and hand-held GPS devices…Done well and over the long-term, initiatives like these can prevent recurrence of genocide and mass atrocity crimes.[16]

As a result, the goal of using technology in mass atrocity response has become more ambitious than simply how these tools and techniques can better help responders simply collect, make sense of, and act upon information derived from ICTs. Somehow the use of technology may fundamentally short-circuit how, whether, and to what degree these abuses actually occur.

Contesting the ICT Progress Narrative

Power and Political Economy

In this part, we offer four lines of critique of the ICT progress narrative. The first concerns power and political economy. We argue that an initial problematic aspect of this idea of "hacking" mass atrocities is the invisibilization of existing and emergent power relationships: hence, for us, it is not the (contestable) newness of ICT for mass atrocity response that must be investigated, but the

---

[11] Michael C. Pryce, "How to Prevent a Mass Atrocity," (n.d), accessed May 21, 2017, http://genocidewatch.net/genocide-2/articles-on-genocide/.

[12] Katharina Rall et al, "Data Visualization for Human Rights Advocacy," *Journal of Human Rights Practice* 8, no. 2 (2016), 171-197.

[13] Tina Comes, Kristin Bergtora Sandvik and Bartel De Walle, "Cold at Heart: A Critical Review of Technology for Keeping the Cool in Humanitarian Cold Chains." (Manuscript on file with authors). Also, Kristin Bergtora Sandvik and Katja Lindskov Jacobsen, *UNHCR and the Struggle for Accountability Technology, law and results-based managemen*t, (Abingdon, Oxon: Routledge Humanitarian Studies, 2016).

[14] Richard Ashby Wilson and Richard D. Brown, *Humanitarianism and Suffering: The Mobilization of Empathy* (Cambridge, UK: Cambridge University Press, 2009).

[15] Andrew Herscher, "Surveillant Witnessing: Satellite Imagery and the Visual Politics of Human Rights," *Public Culture* 26, no. 3, 74 (2014), 469-500.

[16] Caroline Hargreaves and Sanjana Hattotuwa, "ICTs for the Prevention of Mass Atrocity Crimes," *Report on the World Summit on the Information Society Stocktaking*, ICT for Peace Foundation (October 2010), 4, accessed May 21, 2017, http://ict4peace.org/wp-content/uploads/2010/11/ICTs-for-the-Prevention-of-Mass-Atrocity-Crimes1.pdf.

power it represents.[17] Technology is not neutral. Instead of society passively adopting technology, technology and society engage in a mutually constitutive relationship.[18] Nevertheless, we do believe that the diffusion of non-human objects generates new political settlements," which, in themselves, constitute a form of institutional power, rather than an elimination of it.[19]

Understanding the political economy of ICT mass atrocity practice is important for understanding power relations.[20] Essentially, ICTs can serve as a platform on which hegemony can be promoted and existing power imbalances be reinforced, shifting the balance towards powerful institutions if the latter are able to strategically use ICTs as legitimating tools.[21] This also links to a more instrumental rationale of technological utopianism, namely that confident, solutionist claims made on behalf of technology's ability to address mass atrocity are part of a moral economy whereby established industry actors and startups developing and promoting ICT solutions are trying to gain legitimacy, visibility and a leg up in the burgeoning business of global emergencies under the heading of "humanitarian innovation," "peace innovation", and so forth.[22] Commentators have noted that generally, in the Tech for Good sector, technology often appears as a solution in need of a problem. This is also the case in mass atrocity response where "the choice of technology used for prevention activities sometimes appears to be supply-driven as opposed to demand-driven."[23] Similarly, many utopian progress claims have been made in the name of the arrival of "digital humanitarians" in the crisis response field (such as the Standby Task Force, the Humanitarian Open Street Map and the Digital Humanitarian Network).[24]

In short, we suggest that the uses of ICTs by a diverse conglomerate of non-governmental, governmental, and private sector actors centrally contains within it an assumption that the present and future committal of mass atrocities can itself be somehow hacked; and that this assumption serves as a vehicle for accumulating legitimacy, resources and projects. Meanwhile, the potential negative consequences of hacking what is often the application of military means by state and non-state actors is subsumed by the potential, though unproven, benefits of these inherently experimental applications of technology.

The Myth of the Ambient Protective or Preventative Effect

Our second line of critique concerns what we call the myth of the protective or preventative effect. Despite the broad adoption of ICT, and the broad claims made on behalf of its abilities to provide change, we argue that there is no extant base of scientific evidence that in any way suggests, let alone proves, the existence of what in our conceptualization can be referred to as a causal Protective or Preventative Effect (PPE) from the use of ICTs in mass atrocity producing environments. We put forward the idea that the Ambient Protective Effect (APE) is based on the assumption that increased volumes of unique otherwise unobtainable data over large-scale geographic areas and/or non-permissive environments may cause one, some, or all of the following four outcomes to occur:

1. Deterrent APE: Perpetrators are less likely to act because of threat of having action documented.

[17] See Tuckwood, *The State of the Field*.

[18] Donald MacKenzie and Judy Wajcman, *The Social Shaping of Technology* (Buckingham: Open University Press, 1999).

[19] Daniel R. McCarthy, "Technology and 'the International' or: How I Learned to Stop Worrying and Love Determinism," *Millennium-Journal of International Studies* 41, no.3 (2013), 471, 489.

[20] Ella McPherson, *ICTs and Human Rights Practice, A report prepared for the UN Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions,* (2015), accessed May 21, 2017, https://www.repository.cam.ac.uk/handle/1810/251346.

[21] Ioannis Tellidis and Stefanie Kappler, "Information and Communication Technologies in Peacebuilding: Implications, Opportunities and Challenges," *Cooperation and Conflict* 51, no.1 (2016), 75-93.

[22] Kristin Bergtora Sandvik, "Humanitarian Innovation, Humanitarian Renewal?" *Forced Migration Review* (2014), 25-27.

[23] Francesco Mancini and Marie O'reilly, "New Technology and the Prevention of Violence and Conflict," *Stability: International Journal of Security and Development* 2, no. 3 (2013).

[24] Burns, *Rethinking Big Data*.

2. Public Outcry APE: Citizens in nations that have capability to interdict become more activated to push for interventions/protective actions because of immediacy/undeniability/uniqueness of ICT derived/transmitted evidence.
3. Actionable intelligence APE: Governments are given new intelligence that they otherwise would not have, due to focus of NGOs on poorly monitored/lower politically valued locations, which causes them to act.
4. Early warning APE: Targeted communities have early warning that enables them to make better, quicker, more informed decisions that are potentially lifesaving.

Underlying these strands is a common conflation of how we intend technology to work and how we predict and measure its effect. Hence, we argue that these aspirations for the effects of technology use, effects that have frequently been seen as objectively resulting from its mere application, have no objective foundation.

The Potential for Harm

Our third line of critique concerns the awareness and acknowledgment of the possible direct and indirect negative effects of ICT. There are longstanding and well-articulated concerns about the use of data for example in the human rights field: data is non-existent or of poor quality due to collection problems or digital shadows; data suffers from bias; effective data analysis is hampered by low levels of data literacy in the practitioner community and so forth. The concern is that these weaknesses affect levels of credibility and accuracy, which is "the currency of human rights advocacy."[25] However, over the last five years, the domain of mass atrocity ICT has in itself emerged as a site of ethical precariousness.

As noted by Latonero and Gold, the "problem is that we simply do not know all the positive and negative impacts these new technologies will bring, which makes it difficult to make informed decisions in the present."[26] The problem is not only that well-intentioned data driven interventions may fail to assist (through bad strategic planning, insufficient resources or inattentiveness to context) but that they may even harm beneficiaries.[27] An important aspect of this development is what appears to be a very weak community-wide interest so far in the ethical dimensions of ICT use for mass atrocity-producing contexts.[28] Concerns have been emerging both with respect to the practices of the volunteer and tech community, and the information practices of the "walled garden" of human security professionals in the UN and INGO system.[29]

While many heavily promoted initiatives around cell phones proclaim that SMS codes can save lives, these detection and documentation focused initiatives seem to be generally unconnected to the response side of operations. Commenting on the celebrated crowd-seeded program Voix des Kivus, Pham and Vinck note that "there were no known efforts to respond to or address incidents or issues raised by cell phone holders."[30] Other times, information collection practices have lacked transparency and accountability, leading to suspicion by individuals and communities providing information.[31]

---

[25] Rall, et al, *Data Visualization.*

[26] Mark Latonero and Zachary Gold, "Data, Human Rights & Human Security," *Human Rights & Human Security* (2015), 1-16.

[27] Ibid.

[28] 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 (2015), 491-502.

[29] Megan Finn and Elisa Oreglia, "A Fundamentally Confused Document: Situation Reports and the Work of Producing Humanitarian Information," *Proceedings of the 19th ACM (Association for Computing Machinery) Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 2016.

[30] Phuong N Pham and Patrick Vinck, "Technology, Conflict Early Warning Systems, Public Health, and Human Rights," *Health and Human Rights* 14, no. 2 (2012), 106-117, accessed May 21, 2017, https://www.hhrjournal.org/2013/08/technology-conflict-early-warning-systems-public-health-and-human-rights/. See also Alexander Austin, "Early Warning and the Field: A Cargo Cult Science?" *Transforming Ethnopolitical Conflict* (Wiesbaden: VS Verlag für Sozialwissenschaften, 2004), 129-150.

[31] Finn, et al, *A Fundamentally Confused Document*.

Additionally, and crucially, emerging, though limited, evidence is beginning to suggest that the opposite of the intended PPE may, in fact, be occurring. A growing body of scholarship indicates that the attempt to project a PPE through technology may be, in some cases, both exposing affected civilian populations to new, rapidly evolving risks to their human security and negatively mutating the behavior of alleged mass atrocity perpetrators. Technology can have unpredictable or unpredicted knock-on effects: For example, crowd-sourced data is neutral in the sense that it can also be used to foment violence, for example by creating a riot, instead of preventing it.[32] In one available example, there is qualitative evidence that the presence of ICTs may cause governments to restrict a population's ability to communicate, as well as facilitate actions that further violence and make conflict dynamics more complex. Mancini and O'Reilly, discussing the use of ICTs during violent crisis in Kyrgyzstan in 2010, write:

> In a context where the government restricted the use of new technology, ICTs appeared to do little to facilitate a response from local authorities or international actors. On the contrary, the government elected to shut down some mobile networks. At the community level, actors using mobile phones and Internet websites did foster group action, but these technologies were predominantly used to help mobilize violent mobs, issue threats to the opposing community, and propagate conflict narratives.[33]

Another, primarily quantitative example indicates that ICTs may have, in at least one case, directly increased violence against the very vulnerable populations that the deployment of these tools and techniques was originally intended to protect. Gordon's study of Amnesty International's 2007-2008 *Eyes on Darfur* project, that monitored villages in the Darfur region of Sudan at risk for attack, provides some of the first evidence of a potential causal relationship between ICT use and direct harm on populations. Gordon argues that:

> …Amnesty's intervention increased violence in monitored villages and neighboring villages during the program as well as in subsequent years. Coupled with qualitative data, results suggest that the Government of Sudan increased violence to retaliate against Amnesty's advocacy efforts. This study highlights the potential for well-intentioned advocacy efforts to generate perverse effects.[34]

It should be reasonably assumed, sadly, that the incidents described above are likely not the only critical incidents that have occurred so far.

Lack of preparedness

Our fourth line of critique concerns the lack of collective consciousness and preparedness regarding these emergent risks. Despite these concerns being raised by multiple voices over the course of years, there has been no concerted, successful effort to date by the various sectors using ICTs in human security crises to develop common ethical, technical, and rights-based standards for their safe and responsible use.[35] Several reasons likely exist for the failure of the human rights and humanitarian sector to either proactively or responsively address the clear and present dangers that these new modalities and methods present for the vulnerable populations these groups seek to protect. We suggest that these factors may include concerns amongst practitioners that documenting and releasing evidence of critical incidents having occurred during their ICT-based projects could cause reputational damage and jeopardize current or future funding. Also of vital importance is a

[32] Joseph G. Bock, "Firmer Footing for a Policy of Early Intervention: Conflict Early Warning and Early Response Comes of Age," *Journal of Information Technology & Politics, 12, no. 1 (2015), 103-111*.

[33] Mancini, *New Technology*.

[34] Grant Gordon, "Monitoring Conflict to Reduce Violence: Evidence from a Satellite Intervention in Darfur," (2016), accessed May 21, 2017, http://www.grantmgordon.com/wordpress/wp-content/uploads/2010/06/GG-EoD.pdf.

[35] See also Joseph G. Bock, "Technology and Vulnerability in Early Warning: Ethical Use of IT in Dangerous Places," *Information Technology for Development*, 22, no.4 (2016), 696-702.

lack of technical and ethical fluency amongst funding and supporting organizations about how to evaluate the potential harm these projects may inadvertently cause. Most critical, however, is the absence of a shared theory of harm and corresponding framework for applying it to these new and evolving ethical challenges.

Towards a Shared Theory of Harm

Regardless of the actual reasons for the lack of intentional and comprehensive action on these issues, it is the last point – the absence of a shared theory of harm and a corresponding framework for applying it – that represents the logical starting point for course correction by the sectors and actors engaged in this work. As noted by Latonero and Gold, "Harms from data revelations range from physical violence, to retribution, to shaming. Yet a more precise taxonomy of data related harms is needed."[36] An accepted, evidence-based theory of harm specific to the potential deleterious impacts resulting from current technical realities of the applications of ICTs in the mass atrocity response context is the first step for the development of any ethical framework for guiding this area of work.

In this article, we seek to articulate this initial theory of harm for ICT and digital data use in the mass atrocity response context. Our goal of doing so is to hopefully initiate a discussion within the fields of both research and practice that is grounded in reality, rather than in aspirations and assumptions, about how to move beyond the "dream of rescue" and the unproven solutionist myth of the PPE towards a rights-based ethical framework for these activities. With rights-based we do not refer to the kind of impossible-to-articulate-and-to-meaningfully-implement rights-based buzzword of the previous decade: our understanding is of rights-based as applying the rule of law and existing data protection and privacy guarantees fully and responsibly to the human insecurity/crisis response field, as well as the concerted effort to identify and develop legal protection mechanisms for new threats posted by ICT use in the human security field.

Failure to develop an accepted theory of harm may mean that civil society will continue to accept the current status quo indefinitely under the auspices of innovating mass atrocity response. At the heart of the current context resulting from the absence of a shared theory of harm is a perceived imperative by civil society to continue to test and deploy largely untested and non-consented interventions in a host of worst-case scenarios because trying anything is seen as better than doing nothing.

Evidence of the dangers of this perceived worst-case scenario innovation imperative can be found in a recent case of the 2014-2015 West Africa Ebola Outbreak. During that crisis, Call Detail Records (CDRs) were collected from mobile phone networks for the ostensible purpose of tracing the spread of the disease. McDonald, in his paper *Ebola: A Big Data Disaster* describes this phenomenon in the context of Ebola as "disaster experimentation", writing:

> The chaos of humanitarian disaster often creates an implied social license for experimentation with new approaches, under the assumption of better outcomes. Vested interests dominate the public discussion of humanitarian data modeling, downplaying the dangers of what is essentially a public experiment to combine mobile network data and social engineering algorithms. In the case of using mobile network data to track or respond to Ebola, the approaches are so new–and generally so illegal– that most advocacy focuses on securing basic access to data. Advocates for the release of CDRs often paint an optimistic picture of its potential benefits, without applying the same rigor to the risks or likelihood of harm. This trades on the social license created by disaster to experiment with the lives of those affected, under the implicit assumption that it can't make the situation worse.[37]

The presiding paradigm can be seen as fundamentally treating highly vulnerable populations affected by extreme crisis events as experimental subjects of largely untested, non-consented,

[36] Latonero, et al, *Data, Human Rights & Human Security.*

[37] Sean. M. McDonald, "Ebola: A Big Data Disaster. *Privacy, Property, and the Law of Disaster Experimentation,*" CIS Papers (2016).

and remotely applied technological interventions.38 We are however concerned that as the scale and depth of global connectivity increases, the scale and nature of cyber-insecurity is being transformed from representing a nuisance or economic loss to encompass fundamental threats to human security that may themselves contribute to mass atrocity targeting and committal.39 ICT interventions in mass atrocity responses are often designed and deployed by actors often existing outside the affected communities themselves. What's more, the severity of the crisis event appears to serve as justification by human rights, humanitarian, and private sector actors for routinely abrogating certain categories of rights – i.e. privacy and human subject research protections - in the stated service of an unproven theoretical protective effect. This approach to the use of ICTs in mass atrocity producing contexts has inherently injected, however unintentionally, a utilitarian ethic of greater goods and trade-offs into this work at the expense of the do no harm ethics traditionally espoused by actors in this space. The phenomena of ad hoc prioritization of one set of rights over another by outside actors utilizing technology creates implicit hierarchies of rights and operational objectives that the subjects of these interventions have little to no consent as to whether, when, and how they are imposed.

In this article, we argue that as a community, we are causing harm through the current paradigm of deployment that will cause irreparable damage to populations in crisis and those who work with them. As a critical community, we need to do a better job of articulating the components of this claim. Without an accepted theory of harm grounded in the operational and technical realities of this work, this utilitarian ethic of disaster experimentation will likely persist and continue to evolve in unpredictable and dangerous ways. In our attempt to begin to articulate a theory of harm, we include five lines of argument.

Cyber Insecurity as Human Insecurity

As a first step, while the case that legal rights are being violated is increasingly made[40], we need to do the work of linking *data security* (privacy and data protection) and *cybersecurity* more comprehensively to *human security*.[41] The protection of social identity has been considered a key component of human security. We suggest that as social identity is increasingly constituted through information technology, threats to data protection and privacy can usefully be understood to now exist as core threats to human security. In 1994, the UN Human Development Report challenged the state-centered conception of security as pertaining to geopolitical issues, exploring the "new frontiers of human security in the daily lives of the people" by arguing that "[h]uman security is not a concern with weapons - it is a concern with human life and dignity."[42] Human vulnerabilities were therefore to be found across a range of issues, broadly categorized into security matters in the community, the economy, and the environment, as well as people's food security, and their health, political and personal security. Since then, contestations over human security's substance, its definitions of threats and vulnerabilities have been thoroughly examined.[43] We suggest that the concept of *human* security deepens the understanding of threats to both privacy and data protection by repositioning the physical individual at the center of the privacy and data protection discourse.

---

[38] Katja Lindskov Jacobsen, "Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation," *Citizenship Studies*, 14, no.1 (2010), 89-103. As noted by Katja Lindskov Jacobsen, experimentation on subjects in the human security field is nothing new; this was part and parcel of the colonial enterprise. She explains that humanitarianism's history cannot be understood apart from a history of experimentation, including experimental colonial and postcolonial endeavors in foreign territories and on foreign bodies to test new technologies and to make them safe for use by more valued citizens often located in metropolitan states.

[39] Kristin Bergtora Sandvik, "The Humanitarian Cyberspace: Shrinking Space or an Expanding Frontier?" *Third World Quarterly* 37, no.1 (2016), 17-32.

[40] McDonald, *Ebola.*

[41] This section draws on Kristin Bergtora Sandvik, Mareile Kaufmann and Kjersti Lohne, "Terror Threats, Data Protection and Human Security: A Shifting Interface in Norwegian Law," 2011, on file with authors.

[42] United Nations Development Program, *Human Development Report 1994* (New York and Oxford: Oxford University Press 1994), 3.

[43] Taylor Owen, "Human Security- Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-based Definition," *Security Dialogue* 35, 3 (2004), 373-387.

Emphasizing the universality of the concept, and in contrast to the use of human security as a foreign policy tool to look at "other" societies, we adopt Burgess and Tadjbakhsh's inward-looking perspective appraising personal integrity through data protection as an asset of value which belongs to the vital core of mass atrocity response. Our ambition here is to set the stage for a harm matrix by emphasizing the utility of human security as an analytic tool in order to comprehend the globalization of the erosion of "personal liberties as trade-offs to national security" where the individual moves to center stage; and to emphasize the way in which global civil society has become engaged in the capture, storage and distribution of personal data in a way that alters its compact with the populations it purports to act on behalf of.[44] The concept of human security is useful not only for the definition and identification of human in/securities, but also for evaluation and critique of those practices which make people insecure.[45] Considering the detachment of personal data from the individual as a process of dehumanization, we argue that the human security perspective, informed by stringent empirical analysis, can provide a theoretical starting point from which scholarship may help to bring back the human and reconnect the individual with its body of data now being generated in technologically driven mass atrocity responses.

What is the Risk: Ignoring Demographically Identifiable Information (DII)

A failure to understand the linkage between cyber security and human security; poor cyber security approaches or even blatant mistakes of such as losing, dumping or inadvertently releasing data can result in harm. Harm may also arise from a failure to calibrate the sensitive nature of the information one is releasing or sharing with third-parties with substandard cyber security practices or partners with commercial or political priorities that puts shared data at risk. Generally, there has been an increasing, if insufficient, acceptance across the sector of the problems related to collecting personal identifiable information (PII) from individuals in crisis; the challenges of obtaining informed individual consent; and the issues raised by resorting to implied or "good enough" consent.

However, we argue that DII is increasingly becoming a critical issue. It is critical in part because DII is being *explicitly subordinated to PII* in standards used by crisis responders.[46] While there is some mention of demographic information, it is often presented as a subset of personal identifiable information, such as name, age, ethnicity, etc. DII can include, though is not limited to PII, online data, geographic and geospatial data, environmental data, survey data, census data, and/or any other data set that can - either in isolation or in combination - enable the classification, identification, and/or tracking of a specific demographic categorization constructed by those collecting, aggregating, and/or cross-corroborating the data. [47]

Hence, as a second step in our attempt to articulate a theory of harm, we put forward the view that DII requires its own category and science of identifiable data specific to itself. This absence of a clearly articulated concept of DII is striking given its critical role in now common digital, networked data collection approaches, such as smartphone apps, social media, and any crowd-sourced platform offered by the private sector. The lack of a standard definition of this term is itself evidence of the enormity of the technical and doctrinal challenge that this type of data presents for all fields of data science, not only humanitarian and human rights applications of ICTs and the data derived from them. The importance of DII in civil society applications of ICTs and the data derived from them cannot be overstated. It may be argued that most, if not all civil society applications of ICTs and the data derived from them fundamentally aim to collect, analyze, and create actionable products either initially based upon and/or seeking to result in DII.[48]

---

[44] Peter J. Burgess and Shahrbanou Tadjbakhsh, "The Human Security Tale of Two Europes," *Global Society* 24, no.4 (2010), 447-465.

[45] Alex J. Bellamy and Matt McDonald, "The Utility of Human Security: Which Humans? What Security? A reply to Thomas & Tow," *Security Dialogue* 33, no. 3 (2002), 373-377, 376.

[46] Raymond, *Beyond 'Do No Harm'*.

[47] Ibid.

[48] Ibid.

DII can be seen as, at first glance, ethically neutral by itself in many cases, without a seemingly obvious ethical imperative for a practitioner to immediately act upon. For example, the 2013 Red Cross Professional Standards for Protection Work, comparing the risks of aggregated data to sensitive individually identifiable data, seems to underplay the risks of these aggregated data sets, stating:

> Protection actors working with aggregated information, such as trend analysis, do not face the same challenges as the information they handle is less sensitive. They may feel less concerned by the standards and guidelines of this chapter. They should nevertheless be aware of the constraints of managing data on individuals and events, in order to understand how the information they are handling has been obtained.

The more, seemingly subtle ethical implications of DII are in stark contrast to many common types of PII encountered in the civil society context, such as raw, de-identified individual health records or refugee registration documents. DII's ethical implications largely results situationally from when, how, why, and from what combinations of initial sources it is derived and applied, rather than the more easily ethically categorized data that comprises PII. In other words, 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 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.

Missing Conversations About Tradeoffs Before Tech Deployment Shape Outcomes

With new ways of seeing come new, correspondent ways of being blind. For example, with new means of mitigating one potential harm or risk (i.e. remote sensing mitigating threat to staff from deployment in dangerous environments) comes an increase in the potential willingness by organizations to act in ways that might harm vulnerable populations in exchange for enhanced staff protection through increased situational awareness. Another example concerns the application of ICT in early warning approaches, and the tradeoff between speed and accuracy, which affects the quality and reliability of the information collected.[49] The most important category of examples, however, concerns the uses of aggregate population data and personally identified data. These tradeoffs are dynamic by nature: As noted by Latonero and Gold, in an acute crisis, concerns over data privacy and data protection mechanisms may be low, but as the threat to life diminishes, the equation changes. They note that "such tradeoffs require measured assessments which are often unclear and ambiguous when data is readily available, easy to collect or simple to share." [50]

As a third step, we propose a closer focus on preparedness: We argue that mass atrocity and human security fields more broadly are characterized by missing conversations about tradeoffs before tech deployment: at its most general, this concerns the question of whether to deploy a particular technology or not; the choice between technological modalities and eventually costs and benefits in particular deployments. What's missing is both a structured process for having such conversations and a generalized perception that these conversations are *intrinsic* both to preparedness and accountability efforts. This also involves a consideration of the kind of tradeoffs taking place, but also the scope and nature of permissible tradeoffs: when does a particular class of tradeoffs become unethical? At present, this evolving economy of largely undocumented tradeoffs related to technology are creating new power disparities and dichotomies that fundamentally

[49] Pham, et al, *Technology, Conflict Early Warning Systems.*

[50] Latonero, et al, *Data, Human Rights & Human Security.*

favor the interests and operational needs of northern NGO, government, and corporate actors over the rights and needs of the subjects of these deployments, in many cases. These trade-offs are happening in often unacknowledged, sublimated ways that are left unsurfaced due to the sometimes pervasive presumption that somehow tech application for situational awareness is somehow separate and hermetically sealed off from risks incurred from ground interventions. Ironically, it may be argued that in fact the scale and scope of ICT related harm may, in some cases, potentially outstrip the harms incurred through ground action precisely because its remote nature somehow removes the perception that it can be harmful.

Taking Difference Seriously: Understanding the Incongruity between Data for Humanitarian Service Provision and Human Rights Truth Provision

This article focuses on mass atrocity response as part of the broader field of human security response. While this broad and very common categorization is helpful to articulate general problems, it also obscures fundamental differences in the objectives, practices, cultures and toolboxes of the various communities of practice that aim to protect or rescue civilians. In our view, in particular, this categorization obfuscates the growing split between human rights and humanitarians as crisis responding communities. This includes how this split shapes and is shaped by each group's use of data and the impact the use has on crisis affected individuals and communities. It also includes increasingly divergent perceptions of what responsible approaches to data collection, maintenance, storage and sharing of data look like. Here, as a fourth step, we point to the need for greater reflexivity: we argue that it is necessary for response actors to take the differences between the ideologies, means, methods and objectives of these communities seriously, and to more consciously reflect on the significance of this difference for one's own work.

At the outset, the moral underpinnings of these two communities are different: Humanitarianism is ideologically framed around the two imperatives of doing no harm and providing assistance according to need; as well as around adherence to core humanitarian principles of humanity, neutrality, impartiality and universality. The humanitarian field has a curious relationship to law and legal regulation: there is an erstwhile and enduring implicit relationship with the IHL modality of trade-offs; proportionality and acceptance of collateral damage if necessary for military gain. At the same time, the law of humanitarian action is fragmented and consists in large part of soft law initiatives surrounding service provision and the conduct of the service providers themselves in contexts of mass atrocities, crisis and other operational scenarios.

The human rights crisis response community is heavily regulated by international human rights law and core principles of non-discrimination. Human rights are also shaped by the regularity of states of exception and suspension of rights in times of crisis. Where humanitarianism has a problem with "politicization" of human security at the expense of responding to human need, the human rights framework conjures up panoply of possible tradeoffs in the interest of securing formal rights protection. As noted above, the product of the human rights community is accurate and credible information about human suffering and rights violations. In short, this community produces and provides "truth" in response to mass atrocities as the product of its operations.

These differences are highly relevant because they problematize the protection perspective: whether you approach data as a means to service provision or as a means to the provision of truth. These differences need to be taken into account as the mass atrocity community engages more comprehensively in exploring how problem definitions shape and are shaped by technology use. As noted above, a power perspective is required for making sense of how the interests of the larger industrial, corporate humanitarian and human rights complexes shape idiosyncratic notions of the harm matrix and where one's own work is situated. We suggest that through the insistence that one's own work has no possibility for physical impact (only providing truth) or is apolitical (only aiding the needy) members of each community not only wrongly attempt to exclude themselves from the harm matrix in the individual instance, but contribute to systemic abdication of responsibility for the potential harms caused by their data-driven interventions.

The Transformational Capacity of Cyber-Insecurity: Human Security Protection as Counter Intelligence?

The final element of our theory of harm relates to ourselves as mass atrocity responders. Some

concern has been directed at the potential damage arising from "bad apples" intent on causing harm by destroying or disrupting data flows. However, a more important and realistic danger is posed by the widespread and near-permanent state of cyber-insecurity in which human security responders find themselves, which may render them as vehicles for attacks by hostile actors. To put it bluntly, when we worry about human rights actors as spies, that is quaint – the critical concern is how what *we* are doing now provides capacities and capabilities for other people's spies. When civil society is cyber-attacked or cyber-exploited, it is not necessarily because attackers want to stop our activities but because we are a surfboard to accessing additional sources and methods in the control of civil society actors. Attackers are often mostly parasitic. This reality calls for a greater understanding of the very utilitarian nature of cyber-attacks, not as targeted acts of aggression violating rights to free speech or to organize, but as a business strategy – civil society is fast becoming an access point to a smörgåsbord of data, devices and institutions. In short –we are now an intelligence asset.

In practice, some human rights actors are taking the consequences of cyber vulnerability seriously, actively developing offensive counter-strategies. These activities can involve wiping context or providing malware to trace attackers. The result is, however, that we are becoming a surveillance actor. For practitioners, intelligence capability produces a unique situational awareness that is highly beneficial for advocacy. However, this capability also gives actors intending to commit atrocities the ability to make otherwise unavailable real time decisions. This paradox raises an important but little discussed issue: is it ethical for us to think about the fact that in the digital age, to protect mass atrocity operations, we have to engage in counter intelligence, to prepare and counter armed actors' attempts to exploit us; to study their perceptions and capabilities? Are we allowed to engage in deception and kinetic cyber counter-attacks against direct denial of service (DDS) attacks, for example? What would engaging in counter measures mean for the core obligations of human rights and humanitarian actors to protect civilians and respect human rights? Moreover, in the short to medium term, another issue will arise that adds increasing complexity to the do no harm imperative, namely the paradox of ICT counter intelligence activities becoming inextricably linked to the notion of responsible and ethical use of ICT technologies in mass atrocity contexts, resulting in the possibility that ethical ICT use can only happen with built-in counter intelligence components. This potential paradigm fundamentally challenges the do no harm approach and the sources of tradition and doctrine that have defined both humanitarian and human rights civil society sectors.

Conclusion

In this article, we have attempted to begin to articulate the components of a shared theory of harm. Our concluding observations concern ethics and evidence. Developing ethical frameworks to guide emergent technologies is a complex endeavor, and such frameworks have a temporary nature. We are not advocating the adoption of a permanent convention or similar instruments. What we are asking, is that the human security community broadly speaking—particularly mass atrocity responders, such as humanitarians, human rights advocates and peace builders—come to terms with the fact that there is a difference between knowing about alleged atrocities and doing something about them; monitoring a mass atrocity crime is different and distinct from preventing it or protecting against its effects. We are also asking that the members of this broad and diverse community to begin to take seriously the fact that ICT use can cause real harm to civilians.

We argue that there is a need to talk about critical incidents stemming from these interventions openly and transparently— not as urban rumors, not as scandal but in the structured form of after action processes. If we can't collect evidence about failure, we are not a scientific evidence based profession— we are not learning and we cannot become ethical in our approach to ICT. Instead, we will become, however unintentionally, a post-ethical and extra-legal field. Civil society requires a means for logging and evaluating critical incidents, including standard definitions and procedures used by funders, governments, and local communities, etc., to evaluate the impact of these projects. In this regard, the imperative to consider ethics must be emphasized as a prerequisite for fulfilling the obligation to do no harm.

It should be emphasized that in itself, the absence of empirical evidence of impact and risk fundamentally makes this project of ICT use problematic. The ethics and evidence of technical opportunities, limitations, and liabilities are intrinsically entwined into the development of each other. If we don't have ethics in our science, we can't responsibly collect results from evidence. Conversely, if we don't have scientifically obtained results from evidence, we can't shape our ethics to be inclusive of the likely modalities of our potential activities and manage their intended and unintended outcomes. Ethics without evidence is impossible. Valid evidence without ethics is also impossible.

This enterprise also entails renegotiating the ethical compact of the human rights and humanitarian fields for the digital age: Current ethical doctrine is based on operational and contextual assumptions from a bygone era (i.e. the 20th century). These "unitary" ethical and protection doctrines were based on direct information collection of PII from individuals, thus the ethical compact between providers and advocates with the populations they encountered is based on a technical reality and value proposition rooted in conceptions of data technologies and expectations of data control that no longer fully apply. The continued use of outmoded ethics in the age of ICTs is, in itself, an unethical act. For even the patina of "ethicality" to be restored to these fields that now more and more rely on ICTs for basic workflows, this "compact" must be reexamined and ultimately renegotiated.

Finally, in a post-Snowden era when global military surveillance is occurring, it is now a key part of the humanitarian imperative to be able to demonstrate why using digital data and platforms in operations *does not* affect the ethical commitment to do no harm to beneficiaries. Our task as academics and researchers is to establish empirical evidence and pedagogic narrative of impact—both positive and negative alike—with clarity and honesty about the current context, which, increasingly, is defined by cyber-insecurity and cyber-warfare.

Bibliography

Austin, Alexander. "Early Warning and the Field: A Cargo Cult Science?" *Transforming Ethnopolitical Conflict*. Wiesbaded VS Verlag für Sozialwissenschaften, 2004. 129-150.

Bellamy, Alex J. and Matt McDonald. "The Utility of Human Security: Which humans? What Security? A Reply to Thomas & Tow." *Security Dialogue* 33, no. 3 (2002): 373-377. https://doi.org/10.1177/0967010602033003010

Bock, Joseph G. "Firmer Footing for a Policy of Early Intervention: Conflict Early Warning and Early Response Comes of Age." *Journal of Information Technology & Politics*, 12, no. 1 (2015): 103-111. https://doi.org/10.1080/19331681.2014.982265

--------. "Technology and Vulnerability in Early Warning: Ethical Use of IT in Dangerous Places." *Information Technology for Development*, 22, no. 4 (2016): 696-702. https://doi.org/10.1080/02681102.2014.903894

Burgess, J. Peter and Shahrbanou Tadjbakhsh. "The Human Security Tale of Two Europes." *Global Society* 24, no.4 (2010): 447-465. https://doi.org/10.1080/13600826.2010.508334

Burns, Ryan. "Rethinking Big Data in Digital Humanitarianism: Practices, Epistemologies, and Social Relations." *GeoJournal* 80, no. 4 (2015): 477-490. https://doi.org/10.1007/s10708-014-9599-x

Comes, Tina, Kristin Bergtora Sandvik, and Bartel De Walle. "Cold at Heart: A Critical Review of Technology for Keeping the Cool in Humanitarian Cold Chains." (On file with authors.)

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 (2015): 491-502. https://doi.org/10.1007/s10708-014-9597-z

Finn, Megan and Elisa Oreglia. "A Fundamentally Confused Document: Situation Reports and the Work of Producing Humanitarian Information." *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM (Association for Computing Machinery), 2016. https://doi.org/10.1145/2818048.2820031

Gordon, Grant. "Monitoring Conflict to Reduce Violence: Evidence from a Satellite Intervention in Darfur." (2016). Accessed May 21, 2017.http://www.grantmgordon.com/wordpress/wp-content/uploads/2010/06/GG-EoD.pdf.

Hargreaves, Caroline and Sanjana Hattotuwa. "ICTs for the Prevention of Mass Atrocity Crimes." *ICT for Peace Foundation (October 2010)*. Accessed May 21, 2017. http://ict4peace.org/wp-content/uploads/2010/11/ICTs-for-the-Prevention-of-Mass-Atrocity-Crimes1. pdf."Report on the World Summit on the Information Society Stocktaking.

Herscher, Andrew. "Surveillant Witnessing: Satellite Imagery and the Visual Politics of Human Rights." *Public Culture* 26, no. 3, 74 (2014): 469-500.

Latonero, Mark and Zachary Gold. "Data, Human Rights & Human Security." (2015): 1-16. Accessed May 21, 2017. https://ssrn.com/abstract=2643728.

Jacobsen, Katja Lindskov. "Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation." *Citizenship Studies* 14, no.1 (2010): 89-103. https://doi.org/10.1080/13621020903466399

Mancini, Francesco and Marie O'reilly. "New Technology and the Prevention of Violence and Conflict." *Stability: International Journal of Security and Development* 2, no. 3 (2013).

McCarthy, Daniel R. "Technology and 'the International' or: How I Learned to Stop Worrying and Love Determinism." *Millennium-Journal of International Studies* 41, no.3 (2013): 470-490. https://doi.org/10.1177/0305829813484636

McDonald, Sean. M. "Ebola: A Big Data Disaster. *Privacy, Property, and the Law of Disaster Experimentation.*" *CIS Papers* (2016).

MacKenzie, Donald and Judy Wajcman. *The Social Shaping of Technology*. Buckingham: Open University Press, 1999.

McPherson, Ella. *ICTs and Human Rights Practice: A Report Prepared for the UN Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions*. (2015). Accessed May 21, 2017. https://www.repository.cam.ac.uk/handle/1810/251346.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs, 2011.

Mueller, Milton. *What is Evgeny Morozov Trying to Prove? A Review of the Net Delusion*. (Internet Governance Project, 2011). Accessed May 21, 2017. www.internetgovernance.org/ 2011/01/13/ what- is- evgeny- morozov- trying- to- prove- a- review- of- the- net- delusion.

Notley, Tanya and Camellia Webb-Gannon. "FCJ-201 Visual Evidence from Above: Assessing the Value of Earth Observation Satellites for Supporting Human Rights." *The Fibreculture Journal* 27 (2016). Accessed May 21, 2017. http://twentyseven.fibreculturejournal.org/2016/03/21/fcj-201-visual-evidence-from-above-assessing-the-value-of-earth-observation-satellites-for-supporting-human-rights/.

Owen, Taylor. "Human Security-Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-based Definition." *Security Dialogue* 35, no. 3 (2004): 373-387. https://doi.org/10.1177/0967010604047555

Pham, Phuong N. and Patrick Vinck. "Technology, Conflict Early Warning Systems, Public Health, and Human Rights." *Health and Human Rights* 14, no. 2 (2012): 106-117. Accessed May 21, 2017. https://www.hhrjournal.org/2013/08/technology-conflict-early-warning-systems-public-health-and-human-rights/.

Pryce, Michael C. "How to Prevent a Mass Atrocity" (n.d.). Accessed May 21, 2017. http://genocidewatch.net/genocide-2/articles-on-genocide/.

Rall, Katharina, et al. "Data Visualization for Human Rights Advocacy." *Journal of Human Rights Practice* 8, no. 2 (2016): 171-197. https://doi.org/10.1093/jhuman/huw011

Raymond, Nathaniel A., Ziad Al Achkar, et al. "Building Data Responsibility into Humanitarian Action." *United Nations Office for the Coordination of Humanitarian Affairs,* (2016).

Raymond, Nathaniel A., Caitlin Howarth, and Jonathan Hutson. "Crisis Mapping Needs an Ethical Compass." *Global Brief* 6 (2012). Accessed May 21, 2017. http://globalbrief.ca/blog/2012/02/06/crisis-mapping-needs-an-ethical-compass/.

Raymond, Nathaniel A. "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 L. Taylor, L. Floridi, & B. van der Sloot, 67-82. Cham, Switzerland: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-46608-8_4

Sandvik, Kristin Bergtora and Kjersti Lohne. "The Rise of the Humanitarian Drone: Giving Content to an Emerging Concept." *Millennium-Journal of International Studies* 43, 1 (2014): 145-164. https://doi.org/10.1177/0305829814529470

Sandvik, Kristin Bergtora, Mareile Kaufmann, and Kjersti Lohne. "Terror Threats, Data Protection and Human Security: A Shifting Interface in Norwegian Law." 2011. (On file with authors.)

Sandvik, Kristin Bergtora and Maria Gabrielsen Jumbert. *The Good Drone*. New York: Routledge, 2016.

Sandvik, Kristin Bergtora and Katja Lindskov Jacobsen. *UNHCR and the Struggle for Accountability Technology, law and results-based management*. Abingdon, Oxon: Routledge Humanitarian Studies, 2016.

Sandvik, Kristin Bergtora, et al. "Humanitarian Technology: A Critical Research Agenda." *International Review of the Red Cross* 96.893 (2014): 219-242. https://doi.org/10.1017/S1816383114000344

Sandvik, Kristin Bergtora. "Humanitarian Innovation, Humanitarian Renewal?" *Forced Migration Review* (2014): 25-27.

--------. "The Humanitarian Cyberspace: Shrinking Space or an Expanding Frontier?" *Third World Quarterly* 37, 1 (2016): 17-32. https://doi.org/10.1080/01436597.2015.1043992

Segal, Howard. P. "The Technological Utopians." In *Imagining Tomorrow: History, Technology and The American Future*, edited by Joseph J. Corn, 119-136. Cambridge, MA: MIT Press, 1986.

Straus, Scott. "Identifying Genocide and Related Forms of Mass Atrocity." *United States Holocaust Memorial Museum* 7 (2011). Accessed May 21, 2017. https://www.ushmm.org/m/pdfs/20111219-identifying-genocide-and-mass-atrocity-strauss.pdf.

Tellidis, Ioannis and Stefanie Kappler. "Information and Communication Technologies in Peacebuilding: Implications, Opportunities and Challenges." *Cooperation and Conflict* 51, no.1 (2016): 75-93. https://doi.org/10.1177/0010836715603752

Tucker, Ian. "We are Abandoning All the Checks and Balances" (2013). Accessed May 21, 2017. https://www.theguardian.com/technology/2013/mar/09/evgeny-morozov-technology-solutionism-interview.

Tuckwood, Christopher. "The State of the Field: Technology for Atrocity Response." *Genocide Studies and Prevention: An International Journal* 8, 3 (2014): 9.

United Nations Development Program. *Human Development Report 1994.* New York and Oxford: Oxford University Press.

Wilson, Richard Ashby and Richard D. Brown. *Humanitarianism and Suffering: The Mobilization of Empathy*. Cambridge, UK: Cambridge University Press, 2009.