Politics and Governance (ISSN: 2183–2463)
2020, Volume 8, Issue 4, Pages 421–431
DOI: 10.17645/pag.v8i4.3110

Article

In the Interest(s) of Many: Governing Data in Crises

Nathan Clark [1,*] and Kristoffer Albris [2,3]

[1] Department of Organization Sciences, Vrije University Amsterdam, 1081 HV Amsterdam, The Netherlands; E-Mail: n.e.clark@vu.nl
[2] Copenhagen Center for Social Data Science, University of Copenhagen, 1353 Copenhagen, Denmark; E-Mail: kristoffer.albris@sodas.ku.dk
[3] Department of Anthropology, University of Copenhagen, 1353 Copenhagen, Denmark

* Corresponding author

Submitted: 7 April 2020 | Accepted: 9 June 2020 | Published: 10 December 2020

Abstract
The use of digital technologies, social media platforms, and (big) data analytics is reshaping crisis management in the 21st century. In turn, the sharing, collecting, and monitoring of personal and potentially sensitive data during crises has become a central matter of interest and concern which governments, emergency management and humanitarian professionals, and researchers are increasingly addressing. This article asks if these rapidly advancing challenges can be governed in the same ways that data is governed in periods of normalcy. By applying a political realist perspective, we argue that governing data in crises is challenged by state interests and by the complexity of other actors with interests of their own. The article focuses on three key issues: 1) vital interests of the data subject vis-à-vis the right to privacy; 2) the possibilities and limits of an international or global policy on data protection vis-à-vis the interests of states; and 3) the complexity of actors involved in the protection of data. In doing so, we highlight a number of recent cases in which the problems of governing data in crises have become visible.

Keywords
big data; crisis management; data ethics; data governance; digital technologies; human rights; political realism

Issue
This article is part of the issue "The Politics of Disaster Governance" edited by Dorothea Hilhorst (Erasmus University Rotterdam, The Netherlands), Kees Boersma (Vrije Universiteit Amsterdam, The Netherlands) and Emmanuel Raju (University of Copenhagen, Denmark).

1. Introduction

The significance of digital technologies and data in crisis management is surging. Emergency and humanitarian organizations increasingly rely on information and communication technologies (ICTs), mobile data, social media platforms, geospatial information, and (big) data analytics to assess risks, provide early warnings, conduct relief efforts, and distribute aid (International Federation of Red Cross and Red Crescent Societies, 2013; Palen & Anderson, 2016; UN Office for the Coordination of Humanitarian Affairs [UNOCHA], 2012). These developments have also brought a range of new actors to the scene of crisis management, including private companies, academic institutions, and global online volunteer networks (Meier, 2015) who engage in crisis management processes by providing and/or processing data. Recent examples include private-sector partnerships (e.g., Flowminder and the International Organization for Migration [IOM], Parity Ethereum and the World Food Programme [WFP], Facebook and various humanitarian agencies; Meier, 2017), crowdsourcing initiatives (e.g., Humanitarian OpenStreetMap, CrisisMappers; Yates & Paquette, 2011), and even the unprompted efforts of researchers (Clark, 2019). It also includes cases of local citizens using social media plat-

forms to organize bottom-up response efforts (Reuter & Kaufhold, 2018), which can disrupt traditional emergency and crisis response mechanisms (Albris, 2018).

While these developments undoubtedly work to provide specific benefits within the sector that would not otherwise be possible, they are also creating new data-related challenges. This pertains not least to concerns around data protection and privacy. The General Data Protection Regulation (GDPR) in EU law and other regulatory frameworks have made data governance a key political issue, alongside emerging concerns over surveillance capitalism (Zuboff, 2019), the discriminatory politics of big data (O'Neil, 2016), and the power of Big Tech in shaping politics and society (Morozov, 2014). These concerns now translate into various potential risks associated with the use of personal data in crises, including relationships of trust between citizens and governments (Watson & Rodrigues, 2018, p. 92), as well as data being made available to third parties for whom it was not intended (McDonald, 2019). The use of personal behavioural data such as communications, location, and even health and demographic information can be useful in crises but is also highly sensitive and revealing. Indeed, the Covid-19 pandemic, which is ongoing at the time of writing this article, is emblematic of many of these concerns, as governments and companies are now attempting to track and contain the virus via apps and the mobile data of individuals (Kirchgaessner, 2020; Marrow & Soldatkin, 2020).

Concerns over data protection are also providing uncharted and complex dynamics for humanitarian organizations, emergency managers, and other actors to navigate. When mishandled, these entities may compromise their organization's integrity and relationships with traditional stakeholders such as donors, governments, and beneficiaries. Such was recently the case in Yemen, after the WFP pressed the Houthi Government to implementing a biometric identification system, as a precondition for receiving aid. Although the WFP's aim of using the biometrical system was allegedly to ensure fairness and transparency in the food and aid distribution, the utilization of such new data-driven technologies was not well received. As a result, the Yemeni Government opted for the "partial stoppage of aid, accusing the WFP of being a surveillance operation" (McDonald, 2019, p. 1).

To be certain, the concerns around data governance in crises are now many and have become a growing point of discussion around which governments, humanitarian organizations, academics, and individuals are contributing. While data governance issues in the context of humanitarian crises are not substantially different from general concerns over the application of data for the public good, in which there are necessary trade-offs, they do tend to be more complex for two reasons. First, urgent concerns over the protection of life and property permeating crises often render questions of data protection and privacy secondary. Second, the complexity of institutions crosscutting transnational relations and international agreements in the world of humanitarian work puts the question of national sovereignty to the test, in ways that differ from other domains of policy and governance.

In this article, we identify two dominant strands of literature on data governance in crises. The first consists of handbooks, guidelines, and very concrete attempts to apply principles of data protection to crisis management. The other is a highly critical literature, couched in academic discourse, attempting to mobilize a language that can make visible the power structures inherent in data governance in crises. While the inputs from both of these strands are important to further our understanding of the role of data protection in crisis management, in this article we propose to look at the issue from a perspective of political realism.

From this point of departure, we ask if the rapidly advancing problems of data protection during crises can be regulated in ways following logically from the ways that data is regulated in periods of normalcy and non-urgency. By applying a political realist lens, we argue that data governance in crises is shaped by state interests and by the existence of a wide range of actors that hold competing interests. We do this by homing in on three key issues. First, the balancing of the protection of vital interests of the data subject vis-à-vis the right to privacy. Second, the possibilities and limits of an international or global policy on data protection in disaster management vis-à-vis the interests of states. Third, the complexity of actors involved in the governance and protection of data in times of crisis.

The article is structured in the following manner: In the next section, we provide a brief overview of the different themes emerging across disciplines and governance domains with respect to data governance in crises. In Section 3, we present our argument by way of examining the three-abovementioned issues. We then discuss how these three issues intersect, before offering our conclusions.

2. Data in Crises

Crises generally refer to high-impact events, which cause serious societal disruption. In this article, 'crises' is used as a broad overarching term to include emergencies and incidents, disasters originating from natural and man-made hazards, as well as other humanitarian scenarios such as those concerning pandemics and refugees. These scenarios may be short-term or ongoing, and will involve different actors depending on the context, phase, and needs of the crisis.

Within this broad framing, the mechanisms and ways by which ICTs, web-based platforms, and data are now involved in crisis management are many. In this regard, legal and ethical issues concerning data governance may also vary depending on, among other things, the context of a crisis, and on the types of data (e.g., personal or aggregate), and how they are generated, collected, and used. For instance, different rules and ethical considera-

tions may apply to actively and passively produced data relating to crowdsourcing initiatives in crises. The first category represents data that are actively generated and submitted by users through a mobile app or other service. In contrast, the second may involve the harvesting of public data from social networks and repositories, where end users may not by "directly involved in the process and possibly not even aware of the data collection in progress" (Dell'Acqua & De Vecchi, 2017, p. 1916).

While a growing corpus of research on the applicability of mobile phone data, social media platforms, microblogging, and geospatial information in crises has been published in recent years, there is a shortage of studies looking at data governance and data ethics in these contexts. In this section, we highlight the existing literature addressing questions in this domain. From the existing literature, we can deduce two distinct strands that each have their own objectives and genres. On the one hand, there is a body of documents that focus on crafting actionable guidelines and handbooks that address how humanitarian organizations and emergency response agencies should use data for crisis management. On the other, there is a body of research literature vested in and drawing from academic fields such as critical data studies and surveillance studies that seeks to point out the power relations and unintended consequences of the use of data in crises. In the following three subsections, we first present both strands of literature, and thereafter present a critical but constructive critique of the literature by proposing a third approach, namely a political realist lens.

2.1. Frameworks, Handbooks, and Guidelines

The 2010 Haitian earthquake triggered a new era for crisis management in which the uses and challenges around data and ICTs really emerged in the sector (Yates & Paquette, 2011). The application of drones, remote sensing data, and crowdsourcing initiatives via social media and text messages following the event became the focus of numerous reports and spurred innovative dynamics within the sector. A decade later, those developments have fed into a rapidly advancing digitalization of the crisis management sector, where the possibilities of using technologies such as AI and machine learning for big data analytics are now a reality. These advances hold much potential, but they have also resulted in a need to address issues of data governance and ethics in the humanitarian space, particularly from a governance perspective.

As a result, numerous frameworks, reports, guidelines, codes of conduct, and other documents are now being generated within the humanitarian sector addressing data protection and ethics. Many have emerged from international organizations and NGOs that have mandates or stakes in the management of international and national crises. There is thus a path dependency at work pertaining to organizational outlooks and priorities. McClure (2019) notes that many of these resources "broadly seek to provide some form of practical guidance for either a specific organization or subsector activity of humanitarian action, such as biometrics or mobile surveys" (p. 2). As one of the first international organizations to develop its own internal data protection policy and manual, the IOM provides a good example of data protection principles based on organizational priorities (i.e., protecting the right to privacy, human dignity, and well-being of migrants; IOM, 2010). Some attempts are also being made to provide more holistic frameworks, such as The Standby Task Force Code of Conduct (Standby Task Force, n.d.), the Signal Code (Greenwood, Howarth, Poole, Raymond, & Scarnecchia, 2017), the International Committee of the Red Cross (ICRC) Data Protection Handbook (Kuner & Marelli, 2017), and the more recent working draft of the OCHA Data Responsibility Guidelines (UNOCHA, 2019) from the UN's Centre for Humanitarian Data.

These functional (i.e., practical) documents have largely emerged to build on top of existing legal, human rights, and ethical resources and standards. Indeed, humanitarian data ethics cuts across multiple fields including (but not limited to) international law (e.g., international humanitarian law, refugee law, human rights law), international and domestic technical and legal standards for data protection, and ethics in areas ranging from big data and computer and information ethics to medical principles such as Do No Harm (McClure, 2019). Data protection issues have existed long before social media and big data saw the light of day, hence the starting positions for many of these documents is that "data protection and humanitarian action should be seen as compatible, complementary to, and supporting each other" (ICRC, 2017, p. 15). In this regard, some of the most important international instruments include the UN General Assembly Resolution 45/95 of 14 December 1990 adopting the Guidelines for the Regulation of Computerized Personal Data Files (UN General Assembly, 1990), the International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution) adopted by the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Madrid in 2009 (ICDPPC, 2009), the OECD Privacy Framework (OECD, 2013), and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention for the Protection of Individuals, 1981), including the Additional Protocol (Additional Protocol to the Convention, 2001; see ICRC, 2017; Kuner & Marelli, 2017, pp. 15–16).

2.2. Critical Studies of Data in Crises

Researchers coming from disaster studies (Alexander, 2014), as well as from mixed-methods fields such as crisis informatics (Palen & Anderson, 2016; Reuter & Kaufhold, 2018) and social data science (Albris,

2018), have approached questions about data in crises from pragmatic and adaptable perspectives (Nagendra, Narayanamurthy, & Moser, 2020; Watson & Rodrigues, 2018). The effective incorporation and wielding of 'big data' formats, for example, is widely seen by scholars as the most pressing frontier for crisis management. Data in crises is not collected for the sake of collection itself, but to make it actionable, with the aim of having some form of utility for the response or recovery activities during emergencies (Boersma, Wagenaar, & Wolbers, 2012; Wolbers & Boersma, 2013).

However, a more prominent research agenda has emerged which is concerned with the inherent challenges and risks, which accompany the rampant growth of data and information during crises. These works largely stem from critically oriented concepts in disciplines such as media and communication studies on critical infrastructure (Parks & Starosielski, 2015), research in critical data studies (boyd & Crawford, 2012; Dalton & Thatcher, 2014) and critical geography (Burns, 2015b; Turk, 2017) and work in science and technology studies and surveillance studies (Boersma & Fonio, 2018). All of these, to a certain extent, share an underlying assumption that "there is no such thing as raw data, and that our technologies are always shaped by, and serve, some interests over others" (Soden & Palen, 2018, p. 4; see also Gitelman, 2013). Each of these disciplines have amassed a rich canon of work concerned with how the lack of accountability to local stakeholders and inequalities in the access to technical infrastructures and data in crises are merely extensions of larger political and material interests in these processes.

Along similar lines, recent discussions have focused on linkages between digital humanitarian networks and what has been termed philanthropic capitalism, which sees the involvement of private-sector actors in the crisis sector (Burns, 2015a; Klein, 2007). The highly technical nature of modern-day crisis management has resulted in a complexity of new actors arriving into the sector such as Big Tech corporations (i.e., Facebook and Google). These actors hold interests which are sometimes seen to clash with traditional humanitarian principles. Research in this area has focused on the marketing of ideas by these actors that technical expertise and "for-profit motivations lead to larger volumes of high-quality data and reliable data curation in crisis contexts" (Burns, 2015a, p. 62). Not only do these developments have the potential to undercut humanitarian principles during crises, but they may also jeopardize the rights, privacy, and security of affected populations. From this viewpoint, technology and data are indirectly becoming 'agents of chaos' in crises, rather than assets for reducing risks.

2.3. A Realist Lens

In this section, we will discuss some of the arguments made by researchers related to the two abovementioned strands of literature by way of outlining what we here term a political realist lens, which serves as a third position. In doing so, our aim is to lay the foundation for the subsequent sections of the article, in which we analyze three key issues around data governance in crises.

The first aforementioned strand of literature, we believe, is to some extent not addressing the deeper and most important questions, namely whether data protection in crises can (or should) be governed through global and universal policy frameworks. Let us illustrate through a recent example from the existing literature. In an editorial for the journal *International Data Privacy Law*, Kuner, Svantesson, Cate, Lynskey, and Millard (2017) discuss a range of issues pertaining to data protection and humanitarian emergencies, based on the publication of the *Handbook on Data Protection in Humanitarian Action*. Humanitarian organizations face a dual challenge: They have to rely on personal data for expedient and efficient humanitarian response, while at the same time having to protect vulnerable people's data. As Kuner et al. (2017, p. 147) note, "In the context of humanitarian action, data protection can literally be a matter of life and death." While they seem to recognize the inherent tensions we outline here, they also state: "While there may be occasional instances of friction between the two areas, data protection and humanitarian action in emergency situations should be viewed as complementary rather than contradictory" Kuner et al. (2017, p. 148). In many concrete instances, this might indeed be the case, and we should indeed hope that it is. Yet although Kuner et al. are correct in pointing out that, for instance, the GDPR does allow for flexible interpretation of the lawful basis upon which data is processed with reference to vital interests, there are deeper questions with respect to this issue that remain unaddressed, which we will return to.

In contrast, the second body of literature seems to be addressing questions that are of great importance, but in a manner that is not providing relevant critiques. While much of this literature is indeed looking at some of the problems and violations of potential breaches of data protection principles and laws, there is lack of recognition in this literature of the *real politik* at work, and too much focus on social constructions of identities, categories, and the imaginaries of progress and control invoked by a reliance on data for crisis management. Such a focus indeed mirrors much of the general literature in critical data studies (e.g., boyd & Crawford, 2012). That is, that data is always imbricated in power relations, and is part and parcel of state practices in surveilling its population.

In seeking to carve out a space for a third position, we employ a political realist lens to the question of whether and how personal data can and/or should be governed in crises. This is not meant to be in opposition to the two strands of literature outlined above, but rather to complement them. The political realist approach rests on the notion that states have legitimate interests or reasons of state—*raison d'états*—which guide and undergird their actions and priorities (Morgenthau, 1978). One

such reason in the era of late modernity and in our highly advanced information societies is to collect data about the state's population, and to apply it to useful ends in public governance. This reliance on data is of course part of a larger history and development about the rise of the welfare state and the surveillance society in tandem with a trust in numbers and expertise (Porter, 1996) and the biopolitical interests of states (Foucault, 1990).

While political realism is central to the study of politics and international relations, it is by no means, as Wohlforth (2008) argues, one coherent theory. It is rather a family of ideas and lenses through which political and power relations are viewed. Furthermore, we do not wholesale buy into political realism as a theoretical dogma. Nor do we disregard the role of non-state and international actors (see Section 3.3). We recognize the complexity of humanitarian governance, as a field of multiple competing national, regional, and international interests (Barnett, 2013). We do however argue that discussions around data governance need to be more *realistic*. By this we mean that state interests inevitably shape the implementation and development of different political and policy arrangements regarding data laws and data ethical codes. Such interests seek to preserve the narrow self-interests of states and governments for the sake of the groups they purport to represent. Moreover, given the lack of a clear governing authority in the world of international data governance, different instantiations of politics of power, often referenced to securitization and the vital interests of the population, will inevitably ensue. The following sections of the article will discuss the politics of data governance in crises from this vantage point.

3. Issues in the Governance of Crisis Data

In the following subsections, we will outline three different arguments for why we believe that data governance in crises cannot be modelled on the notions underlying data governance and data ethics in periods of normality. These are vital interests, state interests, and actor complexity.

3.1. Vital Interests

The concept of vital interests is precisely the conundrum which lies at the heart of our concern, since personal data protection collides with crisis management priorities: States have a presumable preference for saving lives or minimizing economic costs over protecting personal data principles. The mechanisms of vital and public interests, as for instance stipulated in the GDPR, ensure that possibility for states and other entities acting as data controllers in crises.

The term 'vital interests' in relation to data protection is used in legal and policy contexts to refer to situations in which there is a legitimate purpose to collect personal data due to matters of life and death. Vital interests are, on the one hand, inserted into the GDPR to enable the collection and processing of data in health emergencies in case a patient is unable to give his or her informed consent due to illness or unconsciousness; on the other hand, as recital 46 of the GDPR makes explicit, vital interests also refer to large-scale emergency scenarios, such as epidemics or disasters. As one of the six legal bases upon which personal data can be collected and processed, vital interests have however been seen as a last way out in case no other legal basis can be used. As recital 46 states:

> Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters. (European Parliament & Council of European Union, 2016)

Yet while the legal basis of vital interests provides a legitimate reason to collect and process personal data under extraordinary circumstances, it is not specified precisely what the baselines for vital interests are, nor when the circumstances are special enough to warrant talk of vital interests. The problem with mechanisms such as vital or public interests is that they are flexible for interpretation. Thus, states or other actors might invoke the need to collect and process data about data subjects by reference to vital or public interests regardless of whether the data could be collected via other means (e.g., informed consent).

While the GDPR is but one legal framework, and so does not influence all of the cases of data governance in crises, it does reflect general ideas about what is at stake in how states and other actors are able to collect and process data in crises. Other legal bases for collecting and processing data—such as informed consent or the performance of a contract—might not be as effective in situations of great urgency, where lives and livelihoods are at stake.

Parallel to the notion of vital interest, we also find the principle of public interest in frameworks such as GDPR. While vital interest designates the interest of the data subject or the legal person(s) in question, public interest might refer to multiple things, including the interest of society in general, or the public sector or the state itself. From a realist perspective, states and other actors will seek to maximize their power and influence in any given situation, including in crises. The governance of an emergency or crisis will to a large extent rest on the ability of the state or other actors to have both quantitatively (a large amount of data) and qualitatively (the right kind of data) about the human groups who are the target

of governance measures. This can, in turn, be framed as data being processed and collected without the consent of data subjects, because it serves some public interest.

3.2. State Interests

The second issue follows directly from the first, namely that states, from a political realist perspective, have clear and often legitimate interests in collecting and processing data about subjects because this will likely increase the successful management and control of the crisis. We cannot presume that states would follow the same kind of rules regarding data protection in crises to the same degree that they would regarding data protection writ large, which in itself is lacking widespread standardization. Expecting a global ratification of the same principles and guidelines is laudable, but highly unrealistic. This is central, because data in emergencies and crises are matters of national or regional security. States have thus extraordinary interests in protecting and governing data. From a political realist perspective, states will always see the necessity of controlling a possible or materialized state of emergency over citizens' rights to data protection and privacy. Many states already have such mechanisms in place in their information and data management laws, and again the vital interest or public interest articles in the GDPR encompass that possibility for states to derogate from the rights of data subjects in extraordinary times.

These measures by the state can also be viewed through a broader legal lens, specifically concerning international human rights law and disaster risk reduction. It is widely accepted that the political obligations contained in many disaster risk reduction instruments, such as the Sendai Framework and International Law Commission Draft Articles on the Protection of Persons in the Event of Disasters, are underlined by the legal obligations imposed on states by human rights instruments (Sommario & Venier, 2018). Indeed, under international law, states may have positive obligations to guarantee fundamental human rights of individuals and groups affected by crises under their jurisdiction. This includes, among other rights, rights related to life, physical security, integrity, and dignity, as well as the right to privacy in a digital context (UN General Assembly, 1966a; UN Human Rights Committee, 1988). And yet, as Sommario (2012) points out, it is also "widely accepted that when facing serious public emergencies states can temporarily suspend their obligations under certain human rights treaties and adopt exceptional measures aimed at overcoming the crisis" (UN General Assembly, 2016, p. 43; Sommario, 2012). For instance, the European Convention of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights are instruments which allow for derogations as lawful responses to emergencies (Council of Europe, 1950; UN General Assembly, 1966a; UN General Assembly, 1966b). Article 15 of the European Convention of Human Rights (Council of Europe, 1950) states:

> In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under [the] Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.

To place this within the context of this article: In a state of emergency, states may derogate from international law and fundamental human rights related to data protections of individuals for the sake of national interests. In fact, in some circumstances states may need to impose limitations to certain human rights, such as those dealing with privacy, in order to uphold others (i.e., right to health), especially those which are non-derogable (i.e., the right to life).

Of course, there are also certain conditions that must be met in order for states to legitimately derogate from human rights, which in time of crisis should be assessed via the balancing of interests and rights through the legitimate limitation clauses found in many provisions (e.g., privacy vs. public interest, or two individuals' competing rights). In this regard, the considerations to be made are not so dissimilar from those previously discussed in the section on vital and public interests and GDPR. These discussions also bring up more delicate political questions, as to the extent to which human rights law (or international law in general) should interfere with the prioritization of states' resources and approaches to safeguarding the life of the nation in crisis (Lauta, 2016). While these questions are outside the scope of this article, they are in line with realist thinking harking back to Schmitt's (2005) notion of the sovereign's power vested in the ability to determine the state of emergency.

3.3. Actor Complexity

The third issue is that, in crises, there is a great complexity of actors with different mandates, interests, and competencies. This is particularly evident in the technical space of crises, where it is often necessary to merge the expertise and resources from various entities, which can clash along epistemological, strategic, and institutional lines (Albris, Lauta, & Raju, 2020). While states—per the two previous issues—may be the primary actors when it comes to data governance, non-state actors are important. Acknowledging this does not inhibit the political realist lens we base our argument on. Rather, the fact that non-state actors do have a role to play in shaping ongoing debates and frameworks for data governance is an empirical and realist fact. Increasingly, we do see humanitarian organizations, research institutions, and private companies putting forth recommendations and

guidelines that call for global data governance standards that (intentionally or not) align with their own specific needs and/or *interests* in crises. Others seem to take the opposite approach, acknowledging that their guidelines are domain specific and not intended to contribute to a broader set of standards, while simultaneously building from and/or referencing established norms. In both instances, by referencing international humanitarian law, human rights law, GDPR, and other international technical and legal standards for data protection, actors legitimize their own additions and subsequently their interests and perceived beliefs about the standards needed across the crisis management sector.

This is a rational strategy to pursue. Just as crises are complex and context specific, so too must be the mandates and interests of different actors. IOM, for instance, may be more concerned with the monitoring of locational data than the World Health Organization, which sees the protection of information related to personal health indicators as a greater priority. Similarly, humanitarian organizations will certainly have more applied, timely concerns than those of critical scientific researchers who conceptualize potential risks based on their observations of diverse variables across a broader landscape. In addition, private and technical actors must strike a balance between revenue models and business objectives on the one hand, and responsible data collection, use, and management on the other. At the end of the day, data governance will inevitably reflect the deep-seated goals of those calling for and implementing it—in whatever format.

This, of course, also assumes that different actors actually know what effective data protection and governance should look like (Parker, 2018). In reality, the complexity and ambiguity among the growing number of rules and policies for data management has left nearly every sector struggling to keep up in order to be legally compliant (or at least appear to be) to instill trust in their target audiences and of course to avoid liability issues down the road (e.g., the ongoing implementation of GDPR). We believe these developments may result in at least three negative trends in the crisis management sector: 1) the implementation of overly restrictive blanket policies to "cover all bases" in the absence of knowledge on appropriate measures; 2) the implementation of policies which mimic the practices of others but are not context specific enough or applied in a way to provide robust, targeted data protection measures for business/organizations or individuals whose data is meant to be protected (Van der Merwe, 2020); and 3) the loose coupling of humanitarian-related initiatives to the existing data policies of organizations.

This has been a particularly interesting dynamic to watch unfold with regards to the relationships of private corporate actors with states and the broader humanitarian sector. Private entities have emerged as crucial actors in crisis management (particularly in the response phase) owing to their efficiency in technological developments and uses, and their access to vast amounts of data. However, this has also meant that these actors are increasingly being pressured to balance their own corporate interests with the interests of the public as well as with general humanitarian principles. Companies must gain public trust while simultaneously achieving objectives which may be linked directly or indirectly to other private interests unrelated to humanitarian causes. The Global Systems for Mobile Communications (GSMA), for instance, is an industry organization representing over 750 mobile operators and hundreds of companies worldwide. They link their Mobile for Humanitarian Innovation programme and Big Data for Social Good initiative, to the organizational principles on data privacy and security, as well as the more recent Digital Declaration (GSMA, 2020a, 2020b). Indeed, the Declaration provides companies within the industry with a symbolic badge of commitment to upholding digital principles in terms of handling personal data.

Of course, evolving power dynamics which take place between private actors and states may also influence the development of rules and measures around data protection over time. There is considerable research devoted to the incursion of private tech actors in humanitarian and state affairs (Saetnan, Schneider, & Green, 2018), and this has certainly been accelerated during Covid-19 via the use of track-and-trace apps (Scott, Braun, Delcker, & Manancourt, 2020). In this regard, humanitarian data governance also reflects larger discussions taking place around data governance in general, where states and supranational actors are seen to be increasingly disempowered through the corporate empowerment of Big Tech companies.

Finally, there is another category of actors whose interests in crises are often overlooked. We are referring to the data subjects themselves. In the wake of the Cambridge Analytica data scandal and the growing monetization of personal data, individuals are increasingly using online social media platforms and media outlets to express their concerns over personal data privacy and to advocate for more transparent data protection processes (Arcila, 2020). Similar discussions are emerging around data protection in crisis management, specifically within societies with greater digital and online connectivity. Those opposed to surveillance powers and the unauthorized use of personal data in crises fear the potential misuse (and abuse) of data by governments, private industry, and other actors. In this paradigm, the concept of vital interests may be interpreted as an invasive, backdoor policy allowing different actors to access and use personal data at their own discretion.

4. Discussion

What emerges from the arguments made in the previous sections is that there are two core issues at stake: interests and governance. These two components are fundamental for creating effective data protection in crises. However, we believe that as the crisis man-

agement sector has become more technically complex, these core issues are being increasingly diverted towards the domain and discipline-specific objectives of different actors. Whether highlighting the practices, promises, or perils of data use and governance in crisis management processes, practitioners and academics are generating volumes of context-specific guidelines and hypotheses. At the same time, many of these actors are calling for standardizations for data protection within the sector.

The flexibility of data governance approaches among different actors is understandable. However, it also means that the alignment of standards or governance approaches in any universal sense seems highly unrealistic. In fact, in the absence of common, targeted objectives among actors, the growing number of interests will work to soften their influence and impact as a whole. Furthermore, without some form of coercive, normative, and/or mimetic international pressures, states and other actors will simply defer to their preferred approaches and practices for the treatment of data in crises. And when viewed through the realist lens, even those pressures may have very minimal influence on state behaviors. This is important—especially if we accept the notion that for better or worse it is the state which is ultimately responsible for the vital interests of the public and individuals. In this paradigm, the attempts to establish and/or align humanitarian principles, organizational mandates and interests, and data governance by different actors may actually cause more harm than good. Because it is quantitatively distracting, yes, but also because in the search for exclusive or universal solutions, the vital interests of states, and subsequently individuals, are overlooked.

The question of vital interests is again central, because it points to the state's responsibility and authority to protect the interests of its citizens in crises. At times it seems this authority is acknowledged and simultaneously disregarded by humanitarian professionals when they create frameworks and guidelines (e.g., Kuner & Marelli, 2017, p. 58). From a realist perspective, state interests, including data about its population, are the main driver for the allocation of values in society and the positioning of actors. Thus, in order to align effective data governance and interests, actors should think outside of their own domains, principles, and standards, and work directly with policy makers. That is, if data protection in crises is to be more than just about good intentions.

Of course, whether or not the state possesses the absolute authority to respond and manage data in crises does not exclude skepticism around the state's ability to do so in an appropriate manner. Never has this been more apparent than with Covid-19. At the time of writing this article, governments around the globe are struggling to manage the outbreak while large swaths of the global population are under some form of mandatory isolation measures. In order to track the spread of the virus, various technical initiatives have been launched by governments and private companies, which rely on the collection and use of personal data—with or without the consent of the targeted communities (Google, 2020; Government of Singapore, 2020). From the perspective of the state, this has meant attempts to allow for limitations to privacy rights in order to protect individual and public rights to health, namely in ways that can adequately account for what would otherwise be infringements of the right to privacy without needing to resort to the more drastic measure of derogations. However, the influence of Big Tech actors in these processes has been substantial and has not gone unnoticed (Scott et al., 2020). Indeed, these developments have spurred various media reports and online protests over the nonconsensual use of personal data by states in an effort to track and contain the spread of the virus. A signal to both the increasing utility of personal data in crises and a growing unease around its use by many. For now, the extent to which the opinions of companies or of the everyday citizens will affect data governance is difficult to say, but collectively these voices could have a normative influence on policy decisions over time.

Where does this leave us? If the efforts around data protection by actors in the humanitarian space are somewhat ancillary (even problematic) to those of states, then how do crisis management professionals ensure that the people's rights to anonymity, privacy, and security are guaranteed in situations where both authorities and people themselves might be more eager to share data for the potential benefit of others? Here they may face both technical and legal obstacles regarding data management, for instance when and if international legal frameworks and national legislations are in conflict with one another. Moreover, as McClure (2019) rightly asks, how should the ethical obligations of emergency and humanitarian professionals be protected and delineated from the interests of other actors when engaging in data-related partnerships and services? We would argue that the core aspect of the issue does not revolve around the question of whether data protection and humanitarian action are either complementary or contradictory. Rather, the issue pertains to the fact that actors do have competing and sometimes overlapping interests at the interface between data protection and humanitarian action, which they should have an *interest* in aligning for the greater benefit of the many. This entails working together in a pragmatic manner as events unfold, rather than conforming to arbitrary, ill-suited, or organization-specific rules and standards.

5. Conclusion

To what extent is the question of data protection different in a humanitarian context from other situations and domains? In this article, we have argued that personal data cannot be governed in the traditional sense for three main reasons: vital interests, the interests of states, and the complexity of actors. Gathering and processing personal data about people might be necessary to respond to or mitigate harmful events. But given the

urgency underlying crises, ethical principles and even laws might be bypassed or disregarded, which puts data subjects in harm's way in a different sense. This presents an obvious conundrum: We should do as much as we can to minimize harm to people in disasters, but that might sometimes mean ethically or legally limiting (or violating) the rights of data subjects.

By employing a political realist approach as we have done in this article, we do not intend to dismiss the relevance and utility of international handbooks and guidelines on data protection in crises, nor what we have termed as critical studies in data governance. Rather, we hope to provide a constructive provocation to the existing literature and to the growing literature in both domains. We do so because we believe that current discussions do not address some of the fundamental issues at stake, which could hinder a wider adoption of both legal codes and ethical principles. Thus, our aim is ultimately also one of ensuring that both personal data is not missed or violated, while also making sure that crises are managed and prevented in the best way possible.

While it is certainly true that data is vital to the governance of crises, the increasing reliance on large data-sets raises the persistent and pernicious issue that data protection, as both a legal obligation and ethical principle, will be forfeited when weighed up against the survival of those in risk of dangerous events, or the state's interests in suffering losses as a result of the risks incurred in crises.

Acknowledgments

The authors wish to thank Ana Stella Ebbersmeyer for her assistance with the editing of this article. Kristoffer Albris was supported by the project DISTRACT—The Political Economy of Distraction in Digitized Denmark, funded by an Advanced Grant from the European Research Council (ERC), project No. 834540.

Conflict of Interests

The authors declare no conflict of interests.

References

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flow, ETS No. 181. (2001).

Albris, K. (2018). The switchboard mechanism: How social media connected citizens during the 2013 floods in Dresden. *Journal of Contingencies and Crisis Management*, *26*(3), 350–357.

Albris, K., Lauta, K., & Raju, E. (2020). Disaster knowledge gaps: Exploring the interface between science and policy for disaster risk reduction in Europe. *International Journal of Disaster Risk Science*, *11*(1), 1–12.

Alexander, D. (2014). Social media in disaster risk reduction and crisis management. *Science Engineering Ethics*, *20*, 717–733.

Arcila, B. B. (2020, March 18). We need privacy and data laws to tackle this global pandemic. *MEDIUM*. Retrieved from https://medium.com/berkman-klein-center/the-world-well-wake-up-to-1-7bbd8460b200

Barnett, M. N. (2013). Humanitarian governance. *Annual Review of Political Science*, *16*(1), 379–398.

Boersma, K., & Fonio, C. (2018). Big data, surveillance and crisis management. In K. Boersma & C. Fonio (Eds.), *Big data, surveillance and crisis management* (pp. 1–16). Abingdon: Routledge.

Boersma, K., Wagenaar, P., & Wolbers, J. (2012). Negotiating the 'trading zone.' Creating a shared information infrastructure in the Dutch public safety sector. *Journal of Homeland Security and Emergency Management*, *9*(2), 1–25.

boyd, d., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, *15*(5), 662–679.

Burns, R. (2015a). *Digital humanitarianism and the geospatial web: Emerging modes of mapping and the transformation of humanitarian practices* (Unpublished Doctoral dissertation). University of Washington, Seattle, WA, USA. Retrieved from http://burnsr77.github.io/assets/uploads/burns_dissertation.pdf

Burns, R. (2015b). Rethinking big data in digital humanitarianism: Practices, epistemologies, and social relation. *GeoJournal*, *80*, 477–490.

Clark, N. (2019). Blurred lines: Multi-use dynamics for satellite remote sensing. *Journal of International Humanitarian Legal Studies*, *10*(1), 171–183.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 (1981).

Council of Europe. (1950). *European convention on human rights* (Art. 15). Strasbourg: Council of Europe.

Dalton, C., & Thatcher, J. (2014, May 12). What does a critical data studies look like, and why do we care? *Society + Space*. Retrieved from https://www.societyandspace.org/articles/what-does-a-critical-data-studies-look-like-and-why-do-we-care

Dell'Acqua, F., & De Vecchi, D. (2017). Potentials of active and passive geospatial crowdsourcing in complementing sentinel data and supporting Copernicus service portfolio. *Proceedings of the IEEE*, *105*(10), 1913–1925.

European Parliament, & Council of European Union. (2016). *Regulation 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)* (Regulation (EU) 2016/679). Brussels: European Parliament and Council of European Union. Retrieved from https://eur-lex.europa.eu/legal-

content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Foucault, M. (1990). *The will to knowledge: The history of sexuality* (Vol. 1). London: Penguin Books.

Gitelman, L. (Ed.). (2013). Raw data is an oxymoron. Cambridge, MA: MIT Press.

Google. (2020). See how your community is moving around differently due to Covid-19. *Google*. Retrieved from https://www.google.com/covid19/mobility

Government of Singapore. (2020). Help speed up contact tracing with TraceTogether. *Government of Singapore*. Retrieved from https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether

Greenwood, F., Howarth, C., Poole, D. E., Raymond, N. A., & Scarnecchia, D. P. (2017). *The signal code: A human rights approach to information during crisis.* Cambridge, MA: Harvard Humanitarian Initiative. Retrieved from https://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf

GSMA. (2020a). Mobile for humanitarian innovation. *GSMA*. Retrieved from https://www.gsma.com/mobilefordevelopment/mobile-for-humanitarian-innovation

GSMA. (2020b). Digital declaration overview. *GSMA*. Retrieved from https://www.gsma.com/betterfuture/resources/digital-declaration-overview

ICDPPC. (2009). *International standards on the protection of personal data and privacy (The Madrid resolution)*. Madrid: Spanish Data Protection Agency. Retrieved from https://www.gpdp.gov.mo/uploadfile/others/Madrid_Resolution-en.pdf

ICRC. (2017). Annual report 2017. *ICRC*. Retrieved from https://www.icrc.org/en/document/annual-report-2017

International Federation of Red Cross and Red Crescent Societies. (2013). *World disaster report: Focus on technology and the future of humanitarian action*. Geneva: International Federation of Red Cross and Red Crescent Societies. Retrieved from http://www.ifrc.org/PageFiles/134658/WDR%202013%20complete.pdf

IOM. (2010). *IOM data protection manual*. Geneva: IOM. Retrieved from https://publications.iom.int/books/iom-data-protection-manual

Kirchgaessner, S. (2020, March 25). Mobile phone industry explores worldwide tracking of users. *The Guardian*. Retrieved from https://www.theguardian.com/world/2020/mar/25/mobile-phone-industry-explores-worldwide-tracking-of-users-coronavirus

Klein, N. (2007). *The shock doctrine: The rise of disaster capitalism*. New York, NY: Metropolitan Books and Henry Holt.

Kuner, C., & Marelli, M. (2017). *Handbook on data protection in humanitarian action*. Geneva: ICRC. Retrieved from https://www.privacy-web.nl/cms/files/2017-07/handbook-data-protection-and-humanitarian-action-2-.pdf

Kuner, C., Svantesson, D. J. B., Cate, F. H., Lynskey, O., & Millard, C. (2017). Data protection and humanitarian emergencies. *International Data Privacy Law*, *7*(3), 147–148.

Lauta, K. C. (2016). Human rights and natural disasters. In S. C. Breau & K. L. Samuel (Eds.), *Research handbook on disasters and international law* (pp. 91–110). Cheltenham: Edward Elgar Publishing.

Marrow, A., & Soldatkin, V. (2020, April 1). Putin takes coronavirus precautions as Moscow unveils tracking app. *Reuters*. Retrieved from https://www.reuters.com/article/us-health-coronavirus-russia/putin-takes-coronavirus-precautions-as-moscow-unveils-tracking-app-idUSKBN21J4W8?feedType=RSS&feedName=technologyNews

McClure, D. (2019). *Humanitarian data governance frameworks: Guide and literature review*. Global Alliance for Humanitarian Innovation. Retrieved from https://reliefweb.int/sites/reliefweb.int/files/resources/GAHI-Best-Practice-DOCUMENT.pdf

McDonald, S. (2019). *From space to supply chain: Humanitarian data governance*. Unpublished manuscript. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436179

Meier, P. (2015). *Digital humanitarians: How big data is changing the face of humanitarian response*. Boca Raton, FL: CRC Press.

Meier, P. (2017). The future of crisis mapping is finally here. *iRevolutions*. Retrieved from https://irevolutions.org/2017/06/07/crisis-mapping-future

Morgenthau, H. J. (1978). *Politics among nations: The struggle for power and peace* (5th ed., revised). New York, NY: Alfred A. Knopf.

Morozov, E. (2014). *To save everything, click here: The folly of technological solutionism*. New York, NY: Public Affairs.

Nagendra, N. P., Narayanamurthy, G., & Moser, R. (2020). Management of humanitarian relief operations using satellite big data analytics: The case of Kerala floods. *Annals of Operations Research*, *2020*, 1–26. https://doi.org/10.1007/s10479-020-03593-w

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York, NY: Crown Publishing Group.

OECD. (2013). *The OECD privacy framework*. Paris: OECD. Retrieved from https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Palen, L., & Anderson, K. M. (2016). Crisis informatics: New data for extraordinary times. *Science*, *353*(6296), 224–225.

Parker, B. (2018, January 18). Aid agencies rethink personal data as new EU rules loom. *The New Humanitarian*. Retrieved from https://www.thenewhumanitarian.org/analysis/2018/01/18/aid-agencies-rethink-personal-data-new-eu-rules-loom

Parks, L., & Starosielski, N. (Eds.). (2015). *Signal traffic: Critical studies of media infrastructures*. Champaign, IL: University of Illinois Press.

Porter, T. (1996). *Trust in numbers: The pursuit of objec-*

tivity in science and public life. Princeton, NJ: Princeton University Press.

Reuter, C., & Kaufhold, M. A. (2018). Fifteen years of social media in emergencies: A retrospective review and future directions for crisis informatics. *Journal of Contingencies and Crisis Management*, *26*(1), 41–57.

Saetnan, A. R., Schneider, I., & Green, N. (2018). *The politics and policies of big data: Big data, big brother?* Abingdon and New York, NY: Routledge.

Schmitt, C. (2005). *Political theology: Four chapters on the concept of sovereignty*. Chicago, IL: Chicago University Press.

Scott, M., Braun, E., Delcker, J., & Manancourt, V. (2020, May 15). How Google and Apple outflanked governments in the race to build coronavirus apps. *Politico*. Retrieved from https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany

Soden, R., & Palen, L. (2018). Expanding critical perspectives in crisis informatics. *Proceedings of the ACM on Human-Computer Interaction*, *2*, 1–22.

Sommario, E. (2012). Derogation from human rights treaties in situations of natural or man-made disasters. In A. de Grutty, M. Gestri, & G. Venturini (Eds.), *International disaster response law* (pp. 323–352). The Hague: TMC Asser Press.

Sommario, E., & Venier, S. (2018). Human rights law and disaster risk reduction. *Questions of International Law*, *1*, 29–47.

Standby Task Force. (n.d.). Code of conduct. *Standby Task Force*. Retrieved from https://standbytaskforce.wordpress.com/our-model/code-of-conduct

Turk, C. (2017). Cartographica incognita: 'Dijital jedis,' satellite salvation and the mysteries of the 'missing maps.' *The Cartographic Journal*, *54*(1), 14–23.

UN General Assembly. (1966a). International covenant on civil and political rights. In *Treaty series* (Vol. 999, p. 171). New York, NY: UN General Assembly.

UN General Assembly. (1966b). International covenant on economic, social and cultural rights. In *Treaty series* (Vol. 993, p. 3). New York, NY: UN General Assembly.

UN General Assembly. (1990). *Resolution 45/95 of 14 December 1990 adopting the Guidelines for the Regulation of Computerized Personal Data Files*.

UN General Assembly. (2016). *Report of the international law commission: Sixty-eight session (2 May–10 June and 4 July–12 August 2016)* (UN Doc A/71/10). New York, NY: UN General Assembly.

UN Human Rights Committee. (1988). *General comment No. 16: Article 17 (the right to respect of privacy, family, home and correspondence, and protection of honour and reputation)* (HRI/GEN/1/Rev.9, Vol. I). Geneva: UN Human Rights Committee.

UNOCHA. (2012). *Humanitarianism in the network age*. New York, NY: UNOCHA. Retrieved from https://www.unocha.org/sites/unocha/files/HINA_0.pdf

UNOCHA. (2019). *Data responsibility guidelines: Working draft*. New York, NY: UNOCHA. Retrieved from https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf

Van der Merwe, J. (2020). Data responsibility: An approach to protecting the people behind the data. *Data & Policy*. Retrieved from https://medium.com/data-policy/data-responsibility-an-approach-to-protecting-the-people-behind-the-data-d6470e4a5fad

Watson, H., & Rodrigues, R. (2018). Bringing privacy into the fold: Considerations for the use of social media in crisis management. *Journal of Contingencies and Crisis Management*, *26*(1), 89–98.

Wohlforth, W. C. (2008). Realism. In C. Reus-Smit & D. S. Web (Eds.), *The Oxford handbook of international relations* (pp. 132–149). Oxford: Oxford University Press.

Wolbers, J., & Boersma, K. (2013). The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management*, *21*(4), 186–199.

Yates, D., & Paquette, S. (2011). Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake. *International Journal of Information Management*, *31*(1), 6–13.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Public Affairs.

About the Authors

Nathan Clark is a Postdoc at the Vrije University Amsterdam, Department of Organization Sciences, and former Director of the Copenhagen Center for Disaster Research (COPE). His areas of research included crisis governance and space law.

Kristoffer Albris is Assistant Professor in Social Data Science and Anthropology at the University of Copenhagen. His research focuses on social media, crisis response, and disaster culture.