Managing Risk Across Borders: ethical implications of engaging information technology for transboundary disaster collaboration

Katrina Petersen
Trilateral Research
katrina.petersen@trilateralresearch.com

ABSTRACT

Disaster management is increasingly becoming a project in managing diversity, from cross-organisational collaboration to inclusivity of voices. This is particularly prevalent when dealing with transboundary risks. New information technologies support these transboundary interactions by compiling diverse information and sources to build collaborative insight beyond what any individual organisation can know. This paper explores the ethical concerns that planners and responders face as they work with these collaborative information technologies to engage with data from other organisations, based in different data frameworks, socio-political priorities, goals, and cultures of risk. It draws on the ethical impact assessment of a cross-border collaborative crisis planning platform currently under development in the H2020 project IN-PREP to examine ethical tensions around equity, inclusion, diversity, solidarity, accountability and transparency. It discusses the consequences of such design foci for an agency's ability to notice ethical risks that emerge from working in diversity.

Keywords

Ethics, Transboundary, Responsibility, Collaboration, Information Technology

INTRODUCTION

This paper explores what ethical issues get foregrounded when borders become a focus in the design of collaborative information sharing technologies for disaster management. Specifically, it examines the tensions and concerns that emerge when actors are brought together from different cultures of risk assessment and preparedness through an interactive data framework and insight tool. As borders – national, jurisdictional, or institutional – increasingly play a role in how disaster risk information is organised and understood, questions arise around how these tools influence the ability of diverse decision-makers to address and take responsibility towards equity, inclusion, diversity, solidarity, accountability, and transparency. It proposes that articulation mechanisms to build awareness around diversity and difference, not just pathways to consensus, are necessary to build trust between responders, the tools they use, and the broader society.

By considering how having "transboundary" as a specific design goal for disaster information technology influences the attention of those using it towards ethics and the risks they assess, this paper adds to literature around digital ethics and improves understandings of how these tools lead to better societal resilience as a whole. It also offers insights, though broad and high-level, into how the design and use of these tools can be approached to develop a clearer understanding and responsibility towards how they affect the way disaster managers work, care for those they serve, and make their communities safer and stronger.

ETHICS AND TRANSBOUNDARY COLLABORATIVE DISASTER IT

Transboundary crises are considered a primary societal challenge facing Europe (Cabane and Lodge 2018). To support better cross-border cooperation and understanding for disaster planning, information technology systems

(IT) are regularly being designed and implemented. These IT systems combine data and insights to provide the broader views of a situation for more efficient coordination and more effective collaborative planning and decision-making (Pottebaum et al., 2016; Jasmontaite et al., 2015). But in combining data in ways that are mutually accessible to a broad network of actors, the IT raise ethical tensions in relation to what kind of impact on disaster management practice they make possible. These tensions go beyond semantic inconsistencies. They are accentuated by the transboundary intention of the systems and become a necessary design focal point (Bharosa et al, 2012; Panten et al., 2018). If left unaddressed, these tensions can lead to results ranging from the further marginalisation of communities to decreased solidarity between response agencies.

These IT work by collecting and translating into comparable forms different types and sources of data. These can include data from satellites, drone, CCTV, alarm sensors in buildings, and GPS worn by responders at the scenes. They can blend in historical data and the results of models, like estimated plume rates, fire spread patterns, and person movements in order to enrich situational awareness and the ability for responders to anticipate their next steps and future needs. This work with the data makes it possible for disaster responders to see across agencies and regions: they can identify resources held by different organisations, understand how their agents are positioned in the field in relation to others, and anticipate when a hazard might move beyond their capacities to know to ask for to help. They fundamentally shift the role of IT from horizon-scanning with the aim of collecting information in one place to providing analytics that enrich information to help transboundary responders detect risk, support collaborative decision-making, understand each other's strengths or resource gaps, and improve joint sense-making (Backman and Rhinard, 2018). Moreover, by structuring collaborative interactions through the sharing of data, these IT also have potential to act as forms of accountability and as professional safeguards against making bad choices (Princen et al., 2016).

However, to work, these IT must bring together overlapping, but not identical, practices of risk assessment, perspectives and voices (Muhren and van de Walle, 2010). Interests may overlap, conform or conflict, differing in how they are translated and interpreted depending on the scale of activity (Williams et al., 2019). Combined with the complexity of the existing technological ecosystems, the diverse nature of the stakeholders they support, the potential needs of communities being served, what a good result should look like becomes more difficult to assess. While in some cases these are semantic (e.g. I define vulnerability in socio-economic terms, you define it in geographic terms), more consequentially they are about translating different valences, functions and expectations of that data that (Fiore-Gartland and Neff, 2015). In doing so, the IT piece together more than just information, but different conceptions of care and of what it means to take responsibility for the well-being of others (Baker and Karasti, 2018). As these combine, ethical tensions emerge.

In the most general sense, ethics around such collaborative IT asks questions about if a tool should be used, what acceptable results are of that use, and who is responsible for such use. For some scholars, this is a debate about what satisfactory results are for society, when the tools might be wrong, or to whom are designers and users accountable to and about what (Ananny, 2016). For others it is about considering the oughts and ought nots to determine what should and should not be designed and implemented (Floridi, 2018). Identifying ethical concerns is often approached by looking at different units of analysis, including examining the technology and the rules upon which it is constructed itself, looking at the processes and ends being sought, and addressing the responsibilities and liabilities of the persons or organisations doing the actions (Brey 2012; Ananny 2016; Floridi and Taddeo 2018). These framing questions and units of ethical analysis have the potential to act as a form of societal accountability, building into the tools forms of responsibility, and integrating societal concerns into the practices with these tools (Hijmans and Raab, 2018).

However, these frames rely on a basis of commonality to start with, and do not always anticipate the collaboration or necessary ad-hoc negotiations that make working over and through a border a benefit for all involved. They approach data and the digital in a way that assumes (even if just local to a given assessment) stability and lack of contestation about what the understandings of the world are, what is a good association, and what the hopes for making a world better are (Neff et al., 2017). Putting a border as a centre of focus complicates *shoulds* and *oughts* and *betters*, as the answers to these questions and what ethical concerns they evoke are not universally normative but culturally grounded and unstable over time and scale, and thus cannot be remedied via relativism or consensus (Leonelli, 2016; Fiore-Gartland and Neff, 2015). Approach these questions in a transboundary way requires taking into account how the tools can be used by end-users in the future and their potential human rights implications for the communities on either side of the line (Stahl, 2013). Ethics becomes about elaborating and encouraging dialogue around the tensions that arise in answers to the questions about if a tool should be used and if the results of this use are acceptable.

METHODS

This work is based upon an initial ethical impact assessment for a large-scale, 3-year long, ongoing EC funded research project to design a transboundary disaster planning and training platform, IN-PREP. This project team is made up of over twenty international and interdisciplinary partners (academia, industry, emergency management practioners and trainers, SMEs) from across the EU. This project intends to create an IT structure to connect a large quantity of complex and diverse data from disparate sources, from modeling of potential hazard outcomes and impacts (e.g. smoke plumes and infrastructural damage assessment) to the local resources available and deployed by collaborating agencies. It provides data analytics and data management frameworks to help process that data and provide realistic scenarios and insights to support all actors in improving their ability to coordinate and work together.

The ethical impact assessment is a process of critical scrutiny that aims to make it easier for designers and end-users to become more aware of the features and interactions that have ethical, moral, and societal implications (Brey 2000; Wright, 2015). In the process, they each learn more about the problem domain and potential of the technology, reflecting upon the potential impacts of different design moves, diverse user practices, and the ambiguities of real-world knowledge and experience (Carroll 2000). In doing so, it contributes towards the protection of societal values and the design of effective risk management strategy (Kloza et al. 2017).

The assessment is iterative throughout the project. This paper is drawn from the first stage, produced with the project's outset before design commitments have been made. The intention of this phase of the assessment is to identify what ethical concerns might arise at various scales of analysis, including technological, processual, and application (Brey 2012; Ananny 2016; Floridi and Taddeo 2018). It makes visible, early on, the potential dilemmas and tensions faced by end-users and stakeholders in the uptake of the new technology so that risks can be mitigated to the greatest extent possible and to support ethically aware future use. The results at this stage are thus more abstract and conceptual, describing little in concrete solutions.

The process began by developing an understanding of the IN-PREP technology by interviews with the technology partners and working with them to map high-level information flows, such as what information is collected and shared, how it will be used, and how quality is assessed. It proceeded with desk studies and participation in user requirements workshops to identify key ethical risks and related harms. It ended with stakeholder consultation, via an end-user workshop to validate these initial findings and to begin to identify mitigation measures and solutions that would be relevant to system design and organisational practice. The workshop included twenty-one participants, a mix of external stakeholder experts and IN-PREP's technology and end-user partners. The end-users included experts in Civil Protection, Fire & Rescue, Police, Crisis and Disaster Risk Management, Disaster Relief, and Public Crisis Management from eight different EU Member States. In addition, six technology partners participated to incorporate technical potential to better anticipate outcomes where tools and practices meet.

What follows are some of the initial tensions identified in the literature and these interactions around the mundane decisions that are necessary to make diverse data talk across borders and around making data mean when managing different cultures of risk.

MAKING DATA TALK ACROSS BORDERS

When building this IT, designers are able to combine a variety of data, manage their translations from one format to another, and map them together onto a common operating picture. These mundane design decisions about which data format to use or which terminology to adopt when describing data, decisions that are often made for practical and efficacy reasons, have the ability to both empower and disempower actors and communities as different data and practices with data are included and excluded from consideration (Leonelli, 2016). Choosing one classification scheme over another risks power struggles and exclusion (e.g. missing a race or ethnicity category). Choosing all schema for the sake of inclusion risks bringing communication between organisations into discord and confusion (e.g. so many different interpretations it is impossible to know which one is intended). Data needs structure, and coordination acts needs common reference points, but the answers are not to be found in the ability to share data itself.

When working with such IT, the end-users want to ask complex question of the data that go beyond layering and comparisons. Tensions starts to emerge around what they want to do with the data as they move from questions like 'what data might they need to know?' and 'what situations they might encounter?' towards questions like 'who could be the most vulnerable?' and 'what socio-economic elements could exacerbate a crisis?'. It is already well acknowledged among disaster practioners that what risk means is not the same on two sides of a border, and thus what data they use and how they use similar data to answer these questions differ (Abad et al., 2018). As a

result, for the data to talk together, design and use has to be able to navigate these ethical tensions in how they can be put to use towards answering these different questions in different risk contexts.

At the most basic level, for example: in Germany, responders will first attend to those in need of aid, then they will attend to the safety of the scene: the greater risk is the immediate lives lost. In France, it is the other way around, first the scene is secured, then those that are in need of aid: the greater risk is to the ability to provide service, if the first responders are injured, then no one will be helped. In England, the aim is to remove all victims from the scene so both scene and person can be treated separately. Differences in what is required of data can be similarly exacerbated by different organisational and role-based approaches to disaster management. While most European countries work with a command and control model that has three levels, strategic, operational, and tactical, the responsibilities at each level are not consistent. For examples, decisions taken by a tactical team in the Netherlands can be taken by an operational team in Italy. What keeps coming out when responders from different places engage with each other is the basic question "why are you doing it that way?". Each practice of risk management has different data that is immediately relevant and highest priority: data about the scene, context, broader picture; data about who is where and in what condition; data about who has the capacity to take victims. Each require the data to be able to be focused and organised depending on the goal of the actor. This does not imply that these goals are by their nature conflicting (they are not), but the different aims ask for different IT work with the data beyond the ability for them to be comparable. When responders engage with such a system, they need to know, for example, if relating their understanding of social vulnerability to another organisation's data on infrastructural instability is an accurate and relevant association to make and to understand how that association might need to be made differently in one locale to the next.

The manner in which data can be approached to answer these questions matters because, as previous studies have demonstrated, decisions taken during disasters can "reinforce, intensify and produce new and uneven stratifications" (Adey 2016: 42). But, as Mark Latonero notes, "the very introduction of data-centered technologies can both reveal and exacerbate power relations on the ground."[1] If a responder or a model they use assumes specific identifiers for vulnerability – such as poverty, lack of robust utility services, dense housing – but in a specific context vulnerability is exacerbated by disability and unique religious tensions, then the inequalities that already existed in these less well represented features start to have greater weight and impact on those living in that context. Yet, it is not always possible to see the details in even the most well-structured big data from across the border. Nor are actors always aware of their interests when they decide on how they structure and categorise data (Ackerman et al., 2013). Both the end-users and technology designers often have a "less-than-complete understanding of the assumptions and values shaping the data they are working with" (Neff et al., 2017: p. 88). And, users of the designed technologies will often have different expertise and priorities when handling the data. It does not help that it is also very hard to predict what information will be available and relevant at what time for which organisation (Ley et al., 2014).

When working at the intersection of multiple risk practices, the challenge becomes one of choosing what kind of knowledge gets included in a system of classification and standards to be able to support and enhance successful collaborative decision-making, without erasing all diversity and ambiguities for the sake of making things common enough for all. Thus, the ability to assign value to the data is not determined by the data itself but by ever-shifting contexts and situations of use (Leonelli, 2016). Identifying these perspectives and accommodating what various actors need to know versus what is nice to know, what tools they must have versus may have, requires careful and considered design (Radianti et al., 2018). Meta-data is a start but cannot provide for all these uncertainties nor can it anticipate the informational needs of other organisations in advance.

The reach of these technologies across socio-political, cultural, and organisational divides demands articulation mechanisms by which actors are able to be aware of others, express difference, and align activities (Doherty, 2012). This awareness can in part be achieved by including a diversity of data and localised sources in the design process to ensure the work done with the data (through algorithms, translations, layering) is generalisable in ways that produce collaborative environments (GFDRR, 2018). But reconciling this diversity, particularly in the face of unpredictability, sets out new forms of responsibilities. Understanding the diversity involved is a vital step in supporting equity and inclusion but does not in and of itself build solidarity or an understanding of responsibility within the collaborations being pursued through the system. Care fundamentally involves critical commitments not just in the acts with the data but the processes of curating the data for multiple audiences and situations of use and involves a unique responsibility to produce and maintain the awareness of where one stands in relations to others. It is necessary to understand how one's data and one's acts with data fit into the broader picture and how specific engagements with that data build trust (Baker and Karasti, 2018).

[1] https://responsibledata.io/2015/06/22/emerging-responsible-data-questions-for-human-rights-and-human-security/

MAKING DATA MEAN ACROSS BORDERS

In order for the data to be technologically combined together, there needs to be an underlying ontology, grounded in some form of shared standards and classification system. But standards and classification systems for data sharing carry with them value systems, systems that guide behaviour, preferences, and implicit bias within a given society (Bowker et al., 2010). Data bias is not an ethical challenge unique to border situations. In fact, it is increasingly being accepted as inevitable and necessary; data systems and the categories upon which they function are just approximations of the world, helping those looking to pay attention in specific ways (GFDRR, 2018). All humans work with some form of implicit biases as ordering mechanisms to make sense of the world around them. And, not all bias or disparate impacts are bad. But putting borders between different entrenched cultures of bias together create new urgencies, such as avoiding mission creep or discrimination. It also presents new opportunities, through comparison, to make visible the otherwise tacit and implicit for interrogation.

The biases can be amplified in how community data, like the demographics of crime or who engages with specific public services, are known to often over- and under-represents communities. For example, low-income communities tend to be surveilled to a greater extent than high-income neighbourhoods, leading to disproportionate representation (Narayanan and MacDonald, 2019). While none of this data is inaccurate in and of themselves, inequalities emerge in how data becomes actionable information for specific actors, with the potential to make some segments of society better off or magnifying injustice for others (Powles and Nissembaum, 2018; Vallor et al., 2018). An added challenge with these transboundary tools is that there are so many actions being done with data and to the data in order to get different answers for different questions in different situations, that to design a system that can address these will be so complex that transparency becomes unrealistic for the users.

Yet, many disaster response agencies lack the technological and data skills and comparative capacities to ensure data and insights are accurate, credible, and not misleading for those they are sharing it with (Campo et al., 2018). When the quantity of data is so great that it is impossible for a person to process, actors need greater support in determining the proportionality and legitimacy of their actions with the data. To know if these systems are meeting specific needs and if their acts are accountable, actors need transparency: an understanding of what is being done with the data and why they received specific results with that data. But this is easier said than done, as exemplified in an exchange during one of the workshops:

> Responder: So when what we do changes, how do we make the models match?
> Designer: New rules would have to be able to be added to the system.
> Responder: How? Who would do that?
> Designer: You could tell us the new rules so we can add it in.
> Responder: But we don't understand what rules are there. How do we know how to make a rule?

The more accurate the algorithm is to transboundary interactions, the more complex it is and thus less able to be made transparent or intelligible by those making decisions with the systems. A lack of understanding in how the systems works means a greater reliance on this 'designed' foundation of action. It risks users being unaware of the limits of their view and experience of the data (House of Lords Select Committee on Artificial Intelligence 2018). Use of such systems require a level of data preparedness, technological knowledge, and knowledge on how to incorporate local and remote data activities into current practices (Baker and Karasti, 2018; Haak et al., 2018). This also magnifies bias discrimination and inequality, particularly in respect to underprivileged communities who have less access to such training and education (European Political Strategy Centre, 2018).

This puts actors in a difficult position of managing, without full information, the tension between using algorithms to make decisions more accurate in solidarity with others and ensuring fair treatment of those being served by making decisions that are locally relevant but potentially inaccurate for others (Whittlestone et al., 2019). With incomplete transparency or transparency that is full but too complex to be understood by a human, it is hard for users to understand when a model is insufficient for the required decisions or for the public to understand why certain groups get aid and others do not (GFDRR, 2018). This also makes trust problematic (Buscher et al., 2013). These are not simple decisions that can be tick-boxed away, but fundamentally part of understanding what is at stake in a collaboration, in a joint response, and when faced with simultaneously transboundary and local responsibilities.

Addressing bias is a social problem and not just a computational problem (Powles and Nissembaum, 2018). It involves envisioning the technical ecosystem, the full context, social forces, and purpose to which a technology is put to use (Vallor et al., 2018). While meta-data can help, it is difficult to produce the kind of background information useful to explain the data to help alleviate bias in advance of the information being exchanged. When

a responder learns how to engage with information, they learn it in a specific context -- national, cultural, institutional. This interpretive context helps people notice, determine, and improve the relevance, quality, timeliness, appropriateness, and compatibility of the data provided in the system (Bertelsen and Bødker, 2001). Understanding how categories were arrived at could help end-users see that a specific segment of the population would go unrepresented. It helps actors understand the 'how' and 'why' of information they are working with and avoid translating data inconsistencies into societal vulnerabilities (Dawes and Gharawi, 2018).

CONCLUSION

A focus on transboundary in disaster IT shows that for such systems to really work and support ethical decision-making and actions, they have to find ways to put that boundary forward. The IT becomes a starting point for a whole host of political engagements with ethical ramifications. Actors involved in the design and use need to learn how to be data allies, not just data sharers. Ethical standards are contextual and thus what is "good" in one context might not be in another and, as such, standards are not code-able or pre-definable in transboundary situations. As a result, the data, the structure of the systems it passes through, and the goals for its use need to become sites for deliberation (Neff et al., 2017). It might not be possible to take apart all the different classification systems to make sure they are ontologically representative (though they should still be, as much as possible). Nor it is possible to provide transparency of category, code, and algorithm. But, putting boundaries at the centre opens up opportunities to design for contextual awareness and articulation mechanisms that support actors in weighing local benefit with collaborative solidarity. It also makes visible new ethical responsibilities, not just about managing one's own data for the sake of liabilities, but about caring about its reuse by others.

The meaning and impact of codes and practices can only be understood in full in their relationship to others (Ananny, 2015). However, consistency and stability of meaning is exceedingly difficult in transboundary disaster management. Thus, ethics here is not about deciding right from wrong, but about providing the tools that enable actors engaged with these IT to produce the necessary descriptive context and interactional practices for an actor to understand where they stand in relation to others and how their actions affect diverse, and sometimes not well known, communities around them. Looking at ethical obligations with a sensitivity towards their context specificity can show that some data uses that may not be acceptable within one context may be permissible in another or to another purpose (Vayena et al., 2015). It is not enough to rely on context encoded as metadata or to open up code for inspection; while these steps are necessary, they are not enough to produce accountability towards the broader societal experience (Ananny, 2015). This kind of broader awareness is made in active and interactive the use of the system, as actors constantly renegotiate the distinctions between responder data and societal data (Neff et al., 2017). It is made through a better understanding of technological capabilities and limitations in different ethical contexts (Whittlestone et al., 2019).

Trust in the designers is not enough for trust in a system. Trust in a system is not enough for "good" collaborations that benefit society at all scales. Rather, mutual trust is built on shared context and coordination (Doherty, 2012). This comes from proactive engagement with the broader stakeholder and societal context, including activities to incorporate different kinds of knowledge, perspectives, and goals to inform innovation trajectories. In some respects, to understand the importance of different forms of interpretability in different situations, engagement with the system needs to reflect the interactive perspective and active participation often taken on by Liaisons or, as Princen et al. (2016) term it, Reginauts.

What is needed in the meantime is the ability to identify and see places where differences exist. Instead of aiming for an unreal transboundary ideal of no-bias and complete consensus in the abstract, the aim is then to use the diversity and discrepancies to make bias open for interrogation, in context. Maybe, then, though hopelessly idealistic, this kind of socio-technical work can become a starting point for understanding how to better address larger human rights challenges that increase societal resilience rather than merely act as amplifiers of bias and inequalities.

ACKNOWLEDGMENTS

The research presented here is part of the IN-PREP projects, funded by Horizon 2020 (H2020/2014-2020), the European Union's Programme for Research and Innovation under grant agreement n° 740627. I am grateful to my colleagues in this project for many inspiring conversations.

REFERENCES

Abad, J., Booth, L., Marx, S., Ettinger, S. and Gérard, F. (2018) Comparison of national strategies in France,

Germany and Switzerland for DRR and cross-border crisis management. *Procedia engineering*, 212, 879-886.

Ackerman, M. S., Dachtera, J., Pipek, V., and Wulf, V. (2013) Sharing knowledge and expertise: The CSCW view of knowledge management. *Computer Supported Cooperative Work,* 22, 4-6, 531-573.

Adey, P. (2016) Emergency Mobilities, *Mobilities*, 11, 1, 32-48, doi: 10.1080/17450101.2015.1103533

Ananny, M. (2016) Toward an ethics of algorithms: Convening, observation, probability, and timeliness. *Science, Technology, & Human Values*, 41, 1, 93-117.

Backman, S. and Rhinard, M. (2018). The European Union's capacities for managing crises. *Journal of contingencies and crisis management*, *26*(2), 261-271.

Baker, K. S. and Karasti, H. (2018) Data care and its politics: designing for local collective data management as a neglected thing. In *Proceedings of the 15th Participatory Design Conference: Full Papers-Volume 1*, ACM.

Bertelsen, O. W., and Bødker, S. (2001) Cooperation in massively distributed information spaces. In ECSCW01 Proceedings of the seventh conference on European Conference on Computer Supported Cooperative Work. Kluwer Academic Publishers. 1–17. Retrieved from http://portal.acm.org/citation.cfm?id=1241868

Bharosa, N., Lee, J., Janssen, M. and Rao, H. R. (2012) An activity theory analysis of boundary objects in cross-border information systems development for disaster management. *Security Informatics*, 1, 1, 15.

Bowker, G. C., Baker, K., Millerand, F., and Ribes, D. (2010) Toward information infrastructure studies: Ways of knowing in a networked environment. In International handbook of internet research, 97-117. Springer: Netherlands.

Brey, P. (2000) Disclosive Computer Ethics. *Computers and Society*, 30, 4, 10-16.

Brey, P. (2012). Anticipating Ethical Issues in Emerging IT. *Ethics and Information Technology,* 14, 305-317.

Buscher, M., Perng, S., and Wood, L. (2013). Privacy, Security, Liberty: Informing the Design of EMIS. In T. Comes, F. Fiedrich, S. Fortier, J. Geldermann, & L. Yang (Eds.), *Proceedings of the 10th International ISCRAM Conference – Baden- Baden, Germany* http://eprints.lancs.ac.uk/62141/1/ELSI_FP_Privacy_pre_final.pdf

Cabane, L. and Lodge, M. (2018) Dealing with transboundary crises in the European Union: options for enhancing effective and legitimate transboundary crisis management capacities. TransCrisis, London, UK.

Campo, S. R., Howarth, C. N., Raymond, N. A. and Scarnecchia, D.P. (2018) The Signal Code: Ethical Obligations for Humanitarian Information Activities. Signal Program on Human Security and Technology, Standards and Ethics Series: 03. Harvard Humanitarian Initiative: Cambridge.

Dawes, S. and Gharawi, M. (2018) Transnational public sector knowledge networks: A comparative study of contextual distances. Government Information Quarterly, 35, 2, 184-194. https://doi.org/10.1016/j.giq.2018.02.002.

Doherty, G., Karamanis, N., and Luz, S. (2012) Collaboration in translation: The impact of increased reach on cross-organisational work. *Computer Supported Cooperative Work (CSCW)*, *21*(6), 525-554.

European Political Strategy Centre. (2018) Report from the High-Level Hearing 'A European Union Strategy for Artificial Intelligence'. https://ec.europa.eu/epsc/sites/epsc/files/epsc_-_report_-_hearing_-_a_european_union_strategy_for_artificial_intelligence.pdf

Fiore-Gartland, B. and Neff, G. (2015) Communication, mediation, and the expectations of data: Data valences across health and wellness communities. *International Journal of Communication*, 9, 19.

Floridi, L. and Taddeo, M. (2018) What is data ethics?, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374, 2083.

Floridi, L. (2018) Soft Ethics and the Governance of the Digital, *Philosophy & Technology,* 31, 1, 1–8.

GFDRR. (2018) Machine Learning for Disaster Risk Management. Washington, DC: GFDRR.

Hijmans, H. and Raab, C. (2018) Ethical Dimensions of the GDPR. in: Mark Cole and Franziska Boehm (eds.) *Commentary on the General Data Protection Regulation.* Cheltenham: Edward Elgar.

Haak, E., Ubacht, J., Van den Homberg, M., Cunningham, S., and Van den Walle, B. (2018) A framework for strengthening data ecosystems to serve humanitarian purposes. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, ACM: New York. DOI: https://doi.org/10.1145/3209281.3209326

House of Lords Select Committee on Artificial Intelligence. (2018) AI in the UK: ready, willing and able?

Report of Session 2017–19: HL Paper 100. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiHnZDp1t3bAhXDcsAKHVe8CgUQFggpMAA&url=https%3A%2F%2Fpublications.parliament.uk%2Fpa%2Fld201719%2Fldselect%2Fldai%2F100%2F100.pdf&usg=AOvVaw1ORsnbqvCmu_cetDlwpjLU

Jasmontaite, L., Delprato, U., Jager, B., and Neubauer, G. (2015) Challenges for the Use of Information Technology and Standards in International Disaster Management. *Proceedings of Future Security 2015*, 129-136.

Kloza, D., Van Dijk, N., Gellert, R., Böröcz, I., Tanas, A., Mantovani, E. and Quinn, P. (2017) Data Protection Impact Assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals. d*.pia.lab Policy Brief*, 1/2017.

Leonelli S. (2016) Locating ethics in data science: responsibility and accountability in global and distributed knowledge production systems. *Phil. Trans. R. Soc. A,* 374, 1-12. http://dx.doi.org/10.1098/rsta.2016.0122

Ley, B., Ludwig, T., Pipek, V., Randall, D., Reuter, C., and Wiedenhoefer, T. (2014) Information and expertise sharing in inter-organizational crisis management. *Computer Supported Cooperative Work (CSCW)*, 23, 4-6, 347-387.

Muhren, W. J., and van de Walle, B. A. (2010) Sense-making and information management in emergency response, *Bulletin of the American Society for Information Science and Technology*, 36, 5, 30-33.

Narayanan, A. and MacDonald, G. (2019). Toward an Open Data Bias Assessment Tool: Measuring Bias in Open Spatial Data. *Urban Institute working paper. https://www.urban.org/research/publication/toward-open-data-bias-assessment-tool/view/full_report*

Neff, G., Tanweer, A., Fiore-Gartland, B., and Osburn, L. (2017) Critique and contribute: A practice-based framework for improving critical data studies and data science. *Big Data*, 5, 2, 85-97.

Panten, K., van Heel, B. F., Fliervoet, J. M., and van den Born, R. J. (2018) Cross-Border Collaboration in River Management: Views on Participation in a Dutch-German Case Study. *Water resources management*, 32, 12, 4063-4078.

Powles, J. and Nissenbaum, H. (2018) The Seductive Diversion of 'Solving' Bias in Artificial Intelligence. *Medium*. https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53

Pottebaum, J., Schäfer, C., Kuhnert, M., Behnke, D., Wietfeld, C., Büscher, M., and Petersen, K. (2016) Common information space for collaborative emergency management. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, 1-6.

Princen, S., Geuijen, K., Candel, J., Folgerts, O., and Hooijer, R. (2016) Establishing cross-border co-operation between professional organizations: Police, fire brigades and emergency health services in Dutch border regions. *European Urban and Regional Studies*, 23, 3, 497-512.

Radianti, J., Martinez, S., Munkvold, B. E., and Konnestad, M. (2018) Co-designing a virtual training tool for emergency management. In *The 15tn International Conference on Information Systems for Crisis Response and Management*.

Stahl, Bernd Carsten (2013) Responsible research and innovation: The role of privacy in an emerging framework, Science and Public Policy 40, pp. 708–716.

Vallor, S., Green, B. and Raicu, I. (2018). Ethics in Technology Practice. The Markkula Center for Applied Ethics at Santa Clara University. https://www.scu.edu/ethics/

Vayena E, Salathé M, Madoff LC, Brownstein JS (2015) Ethical Challenges of Big Data in Public Health. PLoS Comput Biol 11(2): e1003904. https://doi.org/10.1371/journal.pcbi.1003904

Whittlestone, J. Nyrup, R. Alexandrova, A. Dihal, K. and Cave, S. (2019) Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research. London: Nuffield Foundation.

Williams, S., Hardy, C., and Nitschke, P. (2019) Configuring the Internet of Things (IoT): A Review and Implications for Big Data Analytics. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Wright, D. (2015) Ethical Impact Assessment. in J. Holbrook & C. Mitcham (eds.), *Ethics, Science, Technology and Engineering: A Global Resource*, 2nd edition, Macmillan Reference: MI.