Kerasidou, X., Petersen, K., Büscher, M. (forthcoming 2017). Intersecting Intelligence: An Exploration of Big Data Disruptions, in Boersma, K. and Fonio, C. *Big Data, Surveillance and Crisis Management: The Dark Aide of Big Data*. Routledge: London and New York.

CHAPTER 9. Intersecting intelligence: exploring big data disruptions

Xaroula Kerasidou, Katrina Petersen and *Monika Büscher*

1. Introduction

In September 2015, Rana Novack, a Syrian American advocate for refugees and civilians in conflict and founder of the Refugee Admissions Network Alliance, wrote an article in *Wired* magazine entitled "We should have seen this refugee crisis coming". There, Novack berates the reactive approach taken to the escalating refugee crisis that first captured public attention when between January and March 2015 479 refugees drowned or went missing in the Mediterranean sea (UNHCR 2015). Novack calls upon the IT community to 'step up – big time' and use its ability to analyse 'incredible amounts of data' and build 'predictive models':

> *… we should be able to know when and where the next migration will occur. We should be able to predict how many people it will affect and the impact on surrounding areas. We have the technology—right here, right now—to create a new, agile, insightful model that will predict mass migrations and help us better serve displaced families even before they are displaced. We can do all this now. And we must.* (Novack 2015)

Such hopes that IT experts can construct machine or algorithmic 'intelligence' to analyse patterns, trends, anomalies within the vast amounts of data or 'intelligence about' people's and objects' everyday life, are widespread. They index complex intersections of different forms of intelligence and motivations for using them.

As big data meets crises, commercial forms of intelligence mix with humanitarian and security intelligence, as well as emerging forms of grassroots collective intelligence created and shared through social networking technologies. For example, president Obama called for Silicon Valley and other private industry actors to build new donation platforms that leverage access to consumers and users of social media platforms to increase awareness of the refugee crisis in the US (Mattingly and Svoboda 2015). In London, computer programmers, entrepreneurs and investors came together during a Tech City event in order to develop new ideas around data. Their 'Refugee Aid App' provides migrants with up-to-date information about where help might be found nearby, and it also enables charities to communicate with refugees based on their location (Silva 2015). Such support could be pivotal, as Markku Niskala, Secretary General of the International Federation of Red Cross and Red Crescent Societies (IFRC), suggests: disaster management is about "information as much as water, food and medicine or shelter" (as cited in Coyle and Meier 2009: 17). Indeed, technologies such as smartphones have become key tools that facilitate a less perilous journey for the refugees (Brunwasser 2015, Latonero 2016, Gillespie et al. 2016). A 'digital passage' (Latonero 2016) is formed and inhabited through the exchange of personal messages between refugees, friends and family. But at the same time as this digital passage enables mobility and a mobilisation of social collective intelligence that can help coordinate refugee journeys, it contributes to a 'datafication' of the persons and the physical and communicative mobilities involved. The

refugees', their traffickers' and their networks' everyday movements, communications and transactions become intelligence in their own right. Europol has started monitoring social media for human/refugee smugglers (Birnbaum 2015), and Frontex – the European Agency for the Management of Operational Cooperation at the External Borders – has put out a (controversial) call for the design of smartphone apps and databases to track and manage refugees arriving in Europe (Taylor and Graham-Harrison 2016).

There is an uneasy coming together of diverse computational and human intelligences in these intersections, and the ambiguous nature of intelligence – understood on the one hand as a capacity for perceiving, learning and understanding and, on the other, as information obtained for strategic purposes – marks complex relationships between 'good' and 'dark' aspects of big data, surveillance and crisis management.

As Kitchin (2014) observes, the use of machine 'intelligence' for big data analysis, including intelligence about mobile populations, constitutes disruptive innovation, an epistemological and political paradigm shift. There clearly are challenges, such as an erosion of privacy, freedom, equality and human rights (Lyon 2014, Graham and Marvin 2001, Büscher, Perng, and Liegl 2015). However, disruption also brings opportunity for hopeful transformations. New forms of digital humanitarianism (Meier 2015) and the social collective intelligence of self-organised refugee networks and community support groups are examples (Gillespie et al. 2016). For formal crisis management, too, there are many positive outcomes, including richer and faster situation awareness, increased agility, interoperability and capacity for anticipation and prediction. Yet, such humanitarian and community innovations and improvements to crisis management can also be seen as enacting problematic reconfigurations of global power and understandings of resilience that contribute to a hollowing out of societal structures in line with neoliberal ideologies (Burns 2015). Overall, the effects of big data in crisis management are ambiguous.

These ambiguities are at the heart of our analysis in this chapter. Our discussion is structured around three themes emerging from an analysis of discourses on big data in crisis, including media reports, documentation of data processing procedures and a review of academic and popular literature on big data in crises. We begin by examining how big data is produced and how this constitutes a 'datafication' of life on the move for refugees. Here, we explore the effects of visibility/invisibility through datafication and frictions that arise between identification and subjectification. Our second focus draws attention to how the refugee crisis manifests a deepening of the transition from societies of discipline to societies of control through data. A key aspect of this are capabilities for anticipation and prediction of crises. A third focus on dataveillance allows us to discuss how democratising forms of producing and using big data come into conflict with an amplification of 'institutionalised individualism' (Beck 1999) through neoliberal interpretations of freedom and responsibility in crisis. We conclude with a critical evaluation of the relationship between crisis and preparedness as seen through the lens of big data, crisis management and surveillance as constitutive rather than merely reflective of subject positions and realities.

2. Datafication

The infrastructures for communication and information exchange that Latonero (2016) describes have engendered a pervasive transformation of almost all

dimensions of human experience. Thrift shows how populations 'increasingly function as a set of human pantographs, measuring out the world and themselves both at once' as they go about their everyday life in 'Lifeworld.Inc' (2011:9). In crisis situations, another dimension of what Mayer-Schönberger and Cukier (2013) call 'datafication', takes hold. Datafication refers to the fact that 'we can now capture and calculate at a much more comprehensive scale the physical and intangible aspects of existence and act on them' (Mayer-Schönberger and Cukier 2013, 97). In crisis management this has prompted experts to argue that 'technology that provides the right information, at the right time, and in the right place has the potential to reduce disaster impacts' (Koua et al. 2010: 255) and more recent arguments that finding the 'needles' in the big data 'haystack' can provide 'life-saving information for humanitarian organisations and disaster-affected communities' (Meier 2015: 62). Although there is some critical engagement, seeing data as a key to understanding and saving the world has become common sense, an epistemology-ideology and politics driven by a deep belief in data as actionable knowledge.

Datafication utilises meta-data, that is, information about information, such as the author's language, location, communication patterns, preferences. Edward Snowden exposed how analysis of such meta-data can undermine privacy and civil liberties (Harding 2014). Although Snowden's revelations shocked the world and prompted calls for a public debate on issues of privacy and transparency, regulatory decisions have since been taken that allow continuation of such surveillance trends, such as that of the UK's investigatory powers tribunal (IPT) which deals with complaints about surveillance and the intelligence services, rendering legal the hacking of computers, networks and smartphones in the UK or abroad by the Government Communications Headquarters (GCHC) (Bowcott 2016). The power of a data centred epistemology-ideology seemingly trumps concerns over imbalances between security, privacy and liberty. The refugee crisis and its recent escalation in Europe sheds an interesting light on this issue as debates on the importance of the control of external borders, the protection of "fortress Europe", along with efforts to prevent future terrorist attacks have intensified calls for more and more security measures, security measures that rely on increased data. There are three aspects in particular that are revealing.

First, there is a double dynamic to the generation of data in the refugee crisis. On the one hand, the two key agencies involved - Frontex and the European Asylum Support Office (EASO) – depend on data for their very activation. The founding regulations for these agencies explicitly stipulate that their provision of increased technical and operational support is to be given to Member States whose border management or asylum systems are confronted with specific and disproportionate pressure. Without data to capture the 'disproportionate' nature of the situation, these provisions cannot be mobilised. On the other hand, refugees themselves are said to benefit. As the Deputy High Commissioner Wendy Chamberlin suggested, "You have no protection if you are invisible. To get this kind of documentation is a basic form of protection, and services flow from that" (Microsoft Corporation 2011: 1). Thus, refugees, too, have a need to be registered. The UNHRC, for example, which provides humanitarian aid to refugees has based many of their data strategies upon making sure the refugees are known to those with the power to distribute aid. Refugees claiming asylum have their bio-data and other personal information gathered through interviews entered into the UN's *ProGres* database and another database for biometric data, a necessary step for the provision of food, medicine, and other humanitarian services. Depending on

the national authorities, refugees may also have to register with local authorities and the UNHCR may be obliged to share personal data with them (Trilateral 2015).

Secondly, this tracking and tracing of refugees has become a deeply ambiguous process in a world riven by political conflict, where 'migration' increasingly comes to be discussed in co-location with terrorism. For example, the first two themes discussed in the 17-18 December 2015 European Council's meetings, were 'Migration' and the 'Fight Against Terrorism'. A drive towards datafication is visible in both, with the conclusions on migration calling for measures that 'ensure systematic and complete identification, registration and fingerprinting, … to tackle refusal of registration and stem irregular secondary flows'; whilst the conclusions regarding the fight against terrorism state that there is an 'urgency of enhancing relevant information sharing, notably as regards … ensuring the interoperability of the relevant databases with regard to security checks' (European Council 2015). Within the meetings there were also calls for 'systematic security checks' to 'address deficiencies in the functioning of hotspots … and further supporting Frontex and EASO'[1] , as well as proposals for a new European Border and Coast Guard, which is controversial, as it can override member state's powers (Peter 2016).

Thirdly, at this juncture, control and security is being equated with visibility; and visibility with personal security. But how these individuals are made visible matters for both privacy and security, let alone the politics of conflating refugees, migration and terrorism. Working with specific data framing mechanisms affects how the causes and effects of disasters are identified and what elements and people are considered (Frickel 2008). For example, the different structuring frames for data processing presented by specific organisations involved in the 1984 Bhopal disaster[2] determine whether it is seen as an Indian only disaster to be dealt with internally or as an international disaster with responsible parties spread as far as the United States. Changing the classification framing mechanism can change whether disaster recovery is considered complete or still on-going or whether what is relevant to consider are immediate chemical spills or future health problems (Fortun 2000). With the narrower national frame, it is an issue of individual health care, for the other it is a matter of national security.

How we engage with data thus also produces, rather than merely describes, histories and futures (Fritzsche 2005), and data thus cannot be treated simply as intelligence about a situation. This is too often forgotten when data is equated with intelligence and seen to suffice to define solutions. The methods and decisions inherent in data production are made invisible. But datafication clearly is not just a matter of identification and intelligence, it is also a matter of subjectification.

3. Societies of Control

Information technology to manage, engage, and analyse big data are posited as

[1] The European Commission developed a '"Hotspot" approach where the European Asylum Support Office, Frontex and Europol will work on the ground with frontline Member States to swiftly identify, register and fingerprint incoming migrants" (EU Commission 2015:6)

[2] In December 1984, a Union Carbide India Limited (UCIL) pesticide manufacturing plant in Bhopal leaked a mixture of toxic gases, killing between 2-4000 people in the immediate aftermath and significant long term health effects for hundreds of thousands (Fortun, 2000), classed as one of the worst industrial disasters in the world's history.

carriers of innovations and solutions that can provide a clearer common operational picture for command and control in disasters, as well as help build resilient communities. As Coyle and Meier (2009) argue, disasters are often seen as crises of information, where it is vital to make sure that people know where to find potable water, how to ask for help, where their relatives are, or if their home is at risk; as well as providing emergency response and humanitarian agencies with information about affected populations. Such a quest for information for "security", in turn, provides more than fertile ground for a quest for technological solutions, such as big data, which provide opportunities for the extended surveillance of everyday life. The assumption is that if only enough information could be gathered and exchanged, preparedness, resilience, and control would follow. This is particularly pertinent with regard to mobile populations (Adey and Kirby 2016).

In the refugee crisis current at the time of writing, states and aid organisations are looking for a big data solutions, precisely because they are mobile. Surveillance studies have tracked a shift from *discipline* to *control* (Deleuze 1992; Haggerty and Ericson 2000; Lyon 2014) exemplified by the shift from monitoring confined populations (through technologies such as the panopticon) to using new technologies to keep track of mobile populations. Snowden's revelations about data retention and sharing pursued by the UK Government Communications Headquarters (GCHQ) and the US National Security Agency (NSA) dwarf these concerns. Revealing the ultimate ambition of this collaboration during a visit to a joint communications monitoring station in the UK in 2008, Lt Gen Keith Alexander, head of the NSA, asked 'Why Can't We Collect All the Signals, All the Time?' (MacAskill et al. 2013). A 'collect-all' policy could create a live imprint of 'the haystack', that is, all ICT supported communications (in the world), to find 'needles' – terrorists and organised criminals with malicious intent, whose communication patterns are exceptional enough to 'trigger' scrutiny. This is deemed necessary because terrorists may hide as 'one in a million' in amongst ordinary people (Crang and Graham 2007; Crampton 2015). There is a benign impetus to 'collect all', 'just in case'. The city of Amsterdam, for example, is experimenting with techniques to use data to track people's mobile phones within the impact area of a chemical accident to support incident management (Steenbruggen et al. 2013). But big data further escalates mobilities of control and control of mobilities, not only at the level of monitoring the discrete movements of individuals.

Andrejevic and Gates (2014: 190) suggest that 'the target becomes the hidden patterns in the data, rather than particular individuals or events.' National and local authorities are not seeking to monitor individuals and discipline their behaviour but to see how many people will reach the country and when, so that they can accommodate them, secure borders, and identify long term social outlooks such as education, civil services, and impacts upon host community (Pham et al. 2015). Moreover, there is a search for patterns, as highlighted by Edward Snowden's whistleblowing revelations. Analytic tools such as *XKeyscore* make analysis of volumes of data of unprecedented magnitude possible (Gallagher 2013). The technology enables live capture of up to 75% of internet data for certain 'trigger' criteria, such as 'one end foreign' connections between people in the home country and abroad. But the capabilities of these systems are limited, undermining claims to be able to clinically focus only on 'needles'. To analyze the 'haystack', search has to 'go shallow', that is, it has to apply broad rules for selection, which means the 'probability that information is being collected that is unrelated to people the NSA is really interested in (and who the

agency has FISA warrants and National Intelligence case files for) is fairly high' (Gallagher 2013).

Yet even if capacities to analyze the 'haystack' for 'needles' more adequately were available, there would be questions about the quality of the haystack, and the meaning of analysis. For 'Big Data is not self-explanatory' (Bollier 2010: 13 in boyd and Crawford 2012). Neither is big data necessarily good data in terms of quality or relevance (Lesk 2013: 87) or complete data (boyd and Crawford 2012). These concerns apply not only to the analysis of big data for state surveillance or commercial purposes. There are claims that we have reached 'the end of theory', because big data analytics are said to be able to reveal patterns more effectively than theory (Anderson, 2008), but apart from misconceiving the nature of scientific reasoning, such assumptions are undermined by uncertainties about the completeness and accuracy of data. When analysing social media data, for example, most researchers do not have access to the 'firehose', which contains all public tweets ever posted, but only to a 'gardenhose' (roughly 10 percent of public tweets) or a 'spritzer' (roughly one percent of public tweets), and boyd and Crawford argue that 'Without taking into account the sample of a data set, the size of the data set is meaningless' (boyd and Crawford 2012: 669). Furthermore, many techniques used by the state and corporations in big data analysis are based on probabilistic prediction, which brings 'profound ethical dilemmas' (Mayer-Schönberger, in Heaven 2013: 35). Some experts are now 'less worried about privacy and more worried about the abuse of probabilistic prediction' [ibid.], because probabilistic techniques of triggering scrutiny are based on processes that are alien to human reasoning.

Networked electronic technologies and companies such as Google and Facebook best exemplify this shift towards what Baumann might call 'liquid control', as users of such services voluntarily generate through their social activities the data that can then be 'sucked up …, quantified and classified, making possible real-time tracking and monitoring' (Lyon 2014: 4). In the context of the refugee crisis, technologies such as smartphones have become key tools that facilitate a less perilous journey for the refugees (Gillespie et al. 2016). As Latonero (2016) writes:

> *Social media, mobile apps, online maps, instant messaging, translation websites, wire money transfers, cell phone charging stations, and Wi-Fi hotspots have created a new infrastructure for movement as critical as roads or railways. Together, these technologies make up a digital passage that is accelerating the massive flow of people from places like Syria, Iraq, and Afghanistan to Greece, Germany, and Norway.* (Latonero 2016)

Moreover, most aid agencies do mobile data collection which are increasingly connected to interagency sharing portals where partner agencies can access and update the data (Favell 2015). At the same time, these technologies produce new spaces of governing.

The border agency Frontex has put out a recent call for designs for smartphone apps and databases to track and manage refugees arriving in Europe (Taylor and Graham-Harrison 2016). This call sought ideas for how to address the concerns over a lack of situational control expressed by EU nations. Ideas include apps, biometrics and smart cards to track and control people both before they cross into Europe and once they arrive and continue to move around the Schengen countries. Smart-card based vouchers have been used in past refugee situations to provide financial aid in a way that does not require them to continually return to a base-camp to restock supplies (as

happens when physical goods are provided) but allows them to purchase what they need where they need it. At present in the Middle East with the current Syrian crisis, these vouchers and cards are encoded with digital identifiers so that their use can be tracked. The reasoning given is that this allows analysis of the underlying trends behind the movement of people and thus demand for resources can be monitored and forecast (Favell 2015; Marr 2015). The aim is to better target and deliver assistance to those in greatest need through community-based approaches (Trilateral Research and Consulting 2015).

However, with these big data collections, the focus becomes not the individual's behaviour but social and economic insecurities, vulnerabilities, and resilience in relation to the movement of such people. The shift acknowledges that what is surveilled is more complex than an individual person's movements, communications, actions over time. The questions start to become: *how* are they doing what they are doing, what are the patterns, and how does that relate to larger social infrastructures, such as the prediction of needs for movement of resources to support the refugees or to identify aspects of vulnerability (such as single female lead households, their financial situation, water security, health, and education). This demands surveillance of a matrix of mobilities: of communities/populations, goods, money, services, and needs, among others.

This also comes with a switch in humanitarian practices, from bringing aid of specified and assumed types to the victims instead to providing them with the ability to purchase goods specific to their needs on their own. Ironically, resilience, as an effect of this form of community tracing, becomes about making it possible for individuals to self-provide. It is a form of embedded neoliberalism (Joseph 2013). While seemingly avoiding the traps of exerting top-down power over people, the state does not yet have formal control over, and simultaneously providing support for self-determination and choice to empower individuals for self-sufficiency rather than defining them as vulnerable and passive recipients of top-down protection (Meier 2013), tying individual aid to mobile tracking puts refugees in a situation where their security is dependent upon individual choice and the private sector. Apart from disrupting traditional dynamics of responsibility for aid and protection, public-private sharing of intelligence brings new forms of dataveillance as we will discuss below.

Before we turn to this, the fact that tracking also becomes a question of analysing data about the environment and its impact on people's movements is worth noting. For instance, the UNHCR has tried to make sense of refugee mobility by examining wave height versus registered arrivals to Lesvos. By mapping on top of each other the average wave heights around Lesvos and the number of refugees registered upon arrival, they found a clear negative correlation: the choppier the sea, the lower the number of people arriving, and vice versa. Consequently, by looking at the state of the sea they can predict refugee mobilities (UNHCR 2016). We will return to this in our discussion.

4. Power through data: From dataveillance to democratisation?

Public-private collaborations in the sharing of intelligence generate questions regarding the role of private companies in facilitating and enabling dataveillance (Raley 2013). As we have seen above, sharing information with private companies is proposed as a key move to enhance security for refugees, but it also frequently comes to be framed as part of international concerns with security, as 'migration' is

discussed in co-location with terrorism. The 17-18 December 2015 European Council's discusses the two in close proximity, implying links between everyday life, displacement, migration and terrorism. This is a false framing that is nevertheless frequently made, and one that draws commercial communications service providers into the frame. Mortera-Martinez, of Wall Street Journal, for example, almost threatens that:

> *The EU also needs to share more classified information with the U.S., and vice versa. America's Internet giants can help. Think of all the data Facebook or Google has. The EU needs to take a less adversarial position if it wants to establish a constructive relationship with both the U.S. government and U.S. companies.* (Mortera-Martinez 2015)

Since the data is already being collected on a regular basis by ubiquitous private firms, it is thought to contain information that will increase opportunities for intelligence gathering and control and thereby security. This marks a shift from surveillance to 'dataveillance' (van Dijck 2014), where the impetus for data processing is no longer motivated by specific purposes or suspicions, but 'opportunistic' discovery of anomalies that can be investigated. Benefits expected for crisis management include richer situation awareness, increased capacity for risk assessment, anticipation and prediction, as well as more agile response.

However, such changes also reconfigure power relations between state, commercial operators, citizens and non-citizens, through transformations of privacy and accountability. The Snowden revelations made clear that the leading technology companies, Apple, Facebook, Google, Microsoft, Skype, etc. were subject to the NSA and GCHC's data demands, circumventing encryption and privacy controls of unwitting users (Gellman and Poitras 2013). Such practices create an imbalance of power, whereby data subjects do not know who holds how much data about them and for what purposes. For instance, Kennedy and Moss (2015) note that "the analysis of social media data is seen as a powerful new way of knowing publics and capturing what they say and do" (3). But they also note that these analytics tend to be dominated by private and state elites who have access to the necessary tools. In addition to the power relations being fostered, the result is often less privacy, increased social discrimination, and decreased trust as data is being shared beyond the original collecting agency (Andrejevic and Gates 2014; van Dijck 2014). In addition, the integration of multiple databases brings together disparate and fragmented data which, when integrated, can come to be seen as a 'complete picture', which is, however, inevitably and always incomplete (Amoore and de Goede 2008).

There is always a 'prism' (van Dijck 2014: 202) in big data analytics. For instance, as illustrated by Rana Novack's call at the beginning of this Chapter, in relation to crises, the presumption is often that knowledge about future risks is present in the data, that if only data had been consulted sooner, if only ''the dots [had] been connected, the events could have been exposed and stopped' (Amoore and de Goede 2008:174). Infrastructure, both physical and logical, matters to the power and use of big data (Andrejevic and Gates 2014). Big data, even if it is constantly growing and changing shape, is a set of elements assembled for a reason, based in infrastructure, where the work of recording an (on-going or past) event makes "meaning by choosing and placing and pasting" elements together in relation to one another (Smith 2004: 7). Meaning is circumscribed and delimited through these relationships, with ethical

implications for how events becomes knowable, especially in relation to inclusiveness and neutrality.

Yet, at the same time as power is exercised by the state and commerce, power is gathering from the bottom up in new ways. In disaster response, a dynamic interplay between publics and experts is captured by the concept of social collective intelligence; a disruptive innovative force that is challenging the social, economic, political, and organisational practices that shape disaster response.

General policy trends point towards the need for community involvement, recognising the public as important and expert stakeholders in the coordination of response efforts and in the development of community resilience and adaptation. The humanitarian field has for some time now adopted this democratic approach. Many voices within the humanitarian sector welcome the new tools and innovative solutions that information technology, industry, and big data can offer (UN Global Pulse 2012; UN OCHA 2013; Meier 2015). Doing so switches the discourse from vulnerability, where there is a need for external protection mobilised from above to come in and rescue the refugees, to one of resilience, where self-sufficiency and autonomy are part of the equation (Meier 2013).

While similar proposals from the EU were met with controversy (Taylor and Graham-Harrison 2016), biometric technologies and other digital ways of delivering aid, like voucher cards, are already being used for Syrian refugees in countries such as Egypt and Lebanon, being thought of as data aggregation devices that enable effects and capacities, including a more dignified existence, greater choice, and support for local economies (Betts 2013). The UNHCR has even called for the refugees themselves to also develop their own data solutions and ideas (see Palmer 2014) as a way to help build their ideologies into the data infrastructures and thus bring their prisms into view. This could create a richer situational awareness and a better ability to understand and deal with unfolding and future crises by supporting resilient communities through giving them the means of data sharing.

But Burns (2015) finds that humanitarian staff often describe the "local communities" and "crowds" as the eyes, ears and sensors of UN staff, which does not index a genuine collaborative relationship. He states: 'In all these cases, the discourse talks of putting local people "in the driving seat" when in reality the direction of the journey has already been decided' (p. 48). Burns (2015: 42) also notes that this leads to a transformation of social responsibility into individual responsibility.

> *Neoliberalism's promotion of free market norms is therefore much more than the simple ideology of free market economics. It is a specific form of social rule that institutionalises a rationality of competition, enterprise individualised responsibility. Although the state 'steps back' and encourages the free conduct of individuals, this is achieved through active intervention into civil society and the opening up of new areas to the logic of private enterprise and individual initiative. This is the logic behind the rise of resilience.*

In some ways this constitutes the production of 'liquid resilience' – a deflection of risk to the individuals and communities affected. But there is an imbalance of power, with data locally produced, but produced in ways designed to fit into systems and structures already in place, where local individuals and communities have very little

say as to what matters or how data should be collected. So while they may be local sensors, the sensors are pre-programmed to see within a specific spectrum.

Ruppert argues that: 'Rather than an all-knowing state, what we have instead is a plethora of partial projects and initiatives that are seeking to harness ICTs in the service of better knowing and governing individuals and populations' (2012: 118). However, as Chandler (2015: 9) argues, crowdsourcing of big data does not equate to a democratisation of risk assessment or risk governance:

> *the 'power' which big data promises local communities, in terms of capacity-building, relational awareness and resilience, is not the same type of power which governments claimed for themselves in the modernist era of linear cause-and-effect understandings. … does not empower people to change their circumstances but merely to be more aware of them in order to adapt to them. … while disasters were traditionally perceived as sudden and short lived events, there is now a tendency to look upon disasters as continuous processes of gradual deterioration and growing vulnerability. … the role of Big Data is not that of understanding and predicting disasters so as to prevent them but to enable communities to cope with them, through a better understanding of themselves.*

Moreover, any understanding that might be supported is of a strange kind, because ' helps answer what, not why' (Cukier and Mayer-Schönberger 2013). They state that 'often that's good enough'. But is it? The basis of debates about the nature of big data is the onto-epistemological claim reified in 'the needle in the haystack' metaphor. It assumes a reality that exists out there, independent and external, which we are trying one way or another to unveil. Understandings like this limit critiques of big data and such technological advancements to issues of privacy with calls for transparency over data processing practices, of more unveiling, of better knowledge and understanding as the answer to such problems. Yet such an approach leaves us to question the very relationship between crisis and preparedness, crisis and response. This is not a rational, but a political relationship. Otherwise, why, even if there are predictable events (such as a refugee crisis) do people not prepare?

Novack's statement that 'We have the technology—right here, right now—to create a new, agile, insightful model that will predict mass migrations and help us better serve displaced families even before they are displaced. We can do all this now' sounds hollow when seen in the light of the fact that 'we' did know. OCHA and other humanitarian agencies routinely monitor the movement of people. In 2014 the number of people displaced by conflict and persecution increased by 8.3 million, reaching a total of 59.5 million worldwide (UNHCR 2015). Similarly, the use of big data analytics to establish a correlation between turbulent weather, rough seas and numbers of refugees embarking on a journey by boat seems, at best, naïve. Crises are often *not* a crisis of information. It is often not a lack of data or capacity to analyse it that prevents 'us' from preventing disasters or responding effectively. Risk management fails because there is a lack of a relational sense of responsibility. In her work on 'technologies of humility', or technologies that are designed to support collaboration, Jasanoff (2007) explores how we might find ways of framing data and correlations differently and elicit a greater sense of relational responsibility and commitment.

Moreover, technologies designed to support collaboration (and contestation of data!) can support acknowledgement of the subjectifying impetus of data. Ruppert (2011: 2) draws our attention to the performativity of data and devices:

> *subjects are not already and always there waiting to be identified. It is often argued that individuals are subjected to identification processes rather than subjectified by them. There is an assumption, especially in debates about privacy, that a true or authentic self is revealed or 'made public' by identification practices (Sewell and Barker, 2001). The subject is conceived of as either a passive recipient of practices or one who is engaged in active resistance. However, practices do not simply reveal subjects as already formed and unchanging but produce them and the particular capacities and agencies required for the technology to operate.*

Burns (2015) builds on this to investigates how within digital humanitarianism discourses, big data produce and perform subjects 'in need' (individuals or communities affected by crises) and a humanitarian 'saviour' community that, in turn, seek answers through big data. Big data should therefore

> *be conceptualized as a framing of what can be known about a humanitarian crisis, and how one is able to grasp that knowledge; in short, it is an epistemology. This epistemology privileges knowledges and knowledge- based practices originating in remote geographies and de-emphasizes the connections between multiple knowledges. … Put another way, this configuration obscures the funding, resource, and skills constraints causing imperfect humanitarian response, instead positing volunteered labor as ''the solution.'' This subjectivity formation carves a space in which digital humanitarians are necessary for effective humanitarian activities (9-10)."*

Having the information, does not linearly translate into knowing, and acting upon this knowledge. Strathern (2000) reminds us that visibility also conceals and writes about 'the tyranny of transparency' (2000). To study what can become hidden by making the information visible, is a case of attending to the asymmetries of who can predict/know and who can actually act/move/prepare, and how. Big data is caught in confusions over the nature of reality, responsibility and power. It has fallen into a common sense call for more 'transparency', where

> *transparency has been politically and morally juxtaposed against secrecy, [when actually] there is a symbiotic relation between the two, for example, when decisions are made about what to disclose or when transparent data gets buried under volumes of data thus rendering it opaque (Birchall 2011). A politics of transparency must thus be understood in relation to a politics of secrecy, a relation that is also suggested in Strathern's formulation of transparency. An answer thus does not reside in extending the boundaries of the explicit as this will not lead to greater transparency or trust in the state. Indeed, such a strategy would only legitimise the technology of power through which the state has constituted transparency and through which it seeks redemption. Indeed, calls for more disclosure of the same reinforces the virtue and moral rightness of the TA (Transparency Agenda) and its authority and effectivity (Harvey et al). Rather, a politics of transparency needs to include contestation of the knowledge practices and the kinds of realities that are both promoted and eclipsed by the TA …"* (Ruppert 2015:13)

So big data is not just about knowing more. It could be, and should be, about knowing better, or about changing what knowing means, it's an ethico-episteme-ontological-political matter. The 'needle in the haystack' metaphor conceals the fact that there is no such thing as a reality that can be revealed. But realities are made through mediations and human and technological assemblages. Refugees' realities of intersecting intelligences are shaped by the ethico-episteme-ontological politics of big data.

5. Discussion

This chapter explores ambiguous forms of emergent practices around big data use for crises in order to produce a set of questions and uncover a range of issues that might enable "better" ways of working with big data. Crisis response and management, especially in its convergence with big data analytics, is a particularly important site for such investigations, because it is here that exceptional transformations of security, privacy and liberty are driven with extraordinary energy. Specifically, ICT enhanced disaster management can enable data sharing and more efficient and flexible response, including more richly and dynamically informed communication, collaboration and coordination. Such effects are almost unethical to not pursue. However, it can also extend capabilities for intentionally or unintentionally unjust subjectification, data retention, disclosure of personal data in the interest of security, sharing data for the purpose of promoting certain public interests. This risks an extended, ethically dubious and even counter-productive securitisation of emergency response as it engenders a shift from concerns with all hazards and safety (a general concern with risk) to concerns of security (focused on dangers arising from the illegal actions of others).

We discuss various ways in which the emergent practices around big data are amplified and transformed through current trends in IT innovation in crisis response and management. Combining big data with crisis situations frames complex socio-political problems such as the refugee crisis that is current at the time of writing as problems of intelligence and information/data. By focusing on crisis it becomes possible to see how questions around data use need to shift from asking what is in the data to include discussion of how the data is structured and how this structure codifies value systems and social practices, subject positions and forms of visibility and invisibility – and thus forms of surveillance, and the very ideas of crisis, risk governance and preparedness. Practices around big data produce and perpetuate specific forms of social engagement as well as understandings of the areas affected and people being served.

Big data could be a technology for collaboration in relation to the complex causes and consequences of disasters, heightening awareness of vulnerabilities and capacities for response, and fostering consideration of the distribution of risks. Moreover, by highlighting fault lines of injustice before disaster strikes, risk governance augmented by big data could raise hopes for the development of communities of risk (Beck, 1999) and a more relational ethics of risk (Büscher et al. 2017), where 'it would not take a hurricane to make visible the plight of the poor' (Jasanoff 2007, 33) or a refugee crisis to highlight a need for integrated European and global responses to displacement, enabling planning for futures where risks are addressed in more richly informed and - if not more just - more richly and broadly understood and contested ways.

Acknowledgements

The research is part of research funded by the European Union 7th Framework Programme in the SecInCoRe project (Grant no: 261817) and BRIDGE project (Grant no.: 261817). We thank the editors Kees Boersma and Chiara Fonio, and the anonymous reviewers of this chapter for their thoughtful comments, and our colleagues in the SecInCoRe and BRIDGE projects for inspiring debates about big data.

References

Adey, P. and Kirby, P. 2016. The Digital Evacuee. In I. van der Ploeg & J. Pridmore (Eds.), *Digitizing Identities: Doing Identity in a Networked World*. London: Routledge, 221-241.

Amoore, L. and de Goede, M. 2008. Transactions after 9/11: The Banal Face of the Preemptive Strike. *Transactions of the Institute of British Geographers*, 33(2): 173-185.

Anderson, C. 2008. The End of Theory. Will the Data Deluge Make the Scientific Method Obsolete? *Edge* [Online] Available at: http://www.edge.org/3rd_culture/anderson08/anderson08_index.html [Accessed 25 February 2014].

Andrejevic, M. and Gates, K. 2014. Big Data Surveillance: Introduction. *Surveillance and Society*, 12(2): 185–196.

Beck, U. 1999. *World Risk Society*. Cambridge: Polity.

Betts, A. J. 2013. Put Innovation at the Heart of Refugee Protection Work - The Guardian http://www.theguardian.com/global-development-professionals-network/2013/jan/04/refugees-camp-innovation-creativity [Accessed 15th June 2016]

Birnbaum, M. Sep. 2015. Smuggling Refugees into Europe is a New Growth Industry - Washington Post. https://www.washingtonpost.com/world/europe/smuggling-refugees-into-europe-is-a-new-growth-industry/2015/09/03/398c72c4-517f-11e5-b225-90edbd49f362_story.html [Accessed 15th June 2016]

boyd, D. and Crawford, K. 2012. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication & Society*, 15(5): 662–679.

Bowcott, O. Feb, 2016. GCHQ Hacking does not Breach Human Rights, Security Tribunal Rules - The Guardian. https://www.theguardian.com/uk-news/2016/feb/12/gchq-hacking-does-not-breach-human-rights-investigatory-powers-tribunal [Accessed 15th June 2016].

Brunwasser, M. 2015. Migrant Essentials Extend to Smartphone'. International New York Times, August 27, p. 1. https://i.nfil.es/lyl0Iu.pdf [Accessed 31 August 2016].

Burns, R. 2015. Rethinking Big Data in Digital Humanitarianism: Practices, Epistemologies, and Social Relations. *GeoJournal*, 80(4): 477-490.

Büscher, M., Perng, S-Y., Liegl, M. 2015. Privacy, Security, Liberty: ICT in Crises. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, 6(4): 72-92.

Büscher, M., Kerasidou, X., Petersen, K. and R. Oliphant (2017, in press). Networked Urbanism and Disaster. In Freudendal-Petersen, M. and Kesselring, S. (Eds). *Networked Urban Mobilities*. Springer.

Chandler, D. 2015. A World without Causation: Big Data and the Coming of Age of

Posthumanism. *Millennium-Journal of International Studies*, 43(3): 833-851.
Couldry, N. and Powell, A. 2014. Big Data from the Bottom Up. *Big Data & Society*, 1(2): 1-5.
Coyle, D. and Meier, P. 2009. *New Technologies in Emergencies and Conflicts: The Role of Information and Social Networks*. United Nations Foundation; Vodafone Foundation. http://www.alnap.org/resource/6572 [Accessed 11 May 2017]
Crampton, J.W. 2015. Collect it All: National Security, Big Data and Governance. *GeoJournal*, 80(4): 519-531.
Crang, M. and Graham, S. 2007. Sentient Cities: Ambient Intelligence and the Politics of Urban Space. *Information Communication Society*, *10*(6): 789–817.
Cukier, K., and Viktor Mayer-Schönberger. 2013. Rise of Big Data: How it's Changing the Way We Think About the World. *Foreign Affairs*, 92: 28.
Deleuze G. 1992. Postscript on the Societies of Control. *October*, 59: 3–7.
European Commission. 2015. *A European Agenda on Migration*. Brussels. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/background-information/docs/communication_on_the_european_agenda_on_migration_en.pdf [Accessed 31 August 2016]
European Council. 2015. European Council Meeting (17 and 18 December 2015) – Conclusions. http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-euco-conclusions/ [Accessed 6 June 2016].
Favell, A. 2015. How Technology is Helping Deliver Aid to Syrian Refugees in the Middle East. *Computer Weekly*. October 2015. http://www.computerweekly.com/feature/How-technology-is-helping-deliver-aid-to-Syrian-refugees-in-the-Middle-East [Accessed 11 May 2017]
Fortun, K. 2000. Remebering Bhopal, Re-figuring Liability. *Interventions*, 2(2): 187-198.
Frickel, S. 2008. On missing New Orleans: Lost knowledge and knowledge gaps in an urban hazardscape. *Environmental History*, 13(4): 643-650.
Fritzsche, P. 2005. The archive. *History & Memory*, 17(1): 15-44.
Gallagher, S. 2013. Building a Panopticon: The Evolution of the NSA's XKeyscore. How the NSA Went From Off-the-shelf to a Homegrown "Google for packets." *Ars Technica*, August 2013. http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/ [Accessed 15 August 2013]
Gellman, B. and Poitras, L. June, 2013. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program - The Washington Post. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [Accessed 15th June 2016]
Gillespie, M., Ampofo, L., Cheesman, M., Faith, B., Iliadou, E., Issa, A., Skleparis, D. 2016. Mapping Refugee Media Journeys: Smartphones and Social Media Networks Research Report. http://www.open.ac.uk/ccig/sites/www.open.ac.uk.ccig/files/Mapping%20Refugee%20Media%20Journeys%2016%20May%20FIN%20MG_0.pdf [Accessed 11 May 2017]
Graham, S. and Marvin, S. 2001. *Splintering Urbanism*. London: Routledge.
Haggerty K. and Ericson R. 2000. The Surveillant Assemblage. *The British Journal of Sociology*, 51(4): 605–622.
Harding, L. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted*

Man. London: Guardian Faber Publishing.
Heaven, D. 2013. Not like Us: Artificial Minds We Can't Understand. *New Scientist* August: 33–35.
Jasanoff, S. 2007. Technologies of humility. *Nature*, 450(7166): 33.
Joseph, J. 2013. Resilience as Embedded Neoliberalism: A Governmentality Approach. *Resilience*, 1(1): 38-52.
Kennedy, H. and Moss, G. 2015. Known or Knowing Publics? Social Media Data Mining and the Question of Public Agency. *Big Data & Society*, 2(2): 1-11.
Kitchin, R. 2014. Big Data, New Epistemologies and Paradigm Shifts. *Big Data & Society*, 1(1): 1-12.
Koua, E.L.; MacEachren, A.M.; Turtun, I.; Pezanowski, S.; Tomaszewski, B. and Frazier, T. 2010. Conceptualizing a User-Support Task Structure for Geocollaborative Disaster Management Environments. In B. van de Walle, M. Turoff and S. Hiltz (Eds.), *Information Systems for Emergency Management*. New York: Sharpe, 254-278.
Latonero, M. 2016. For Refugees, a Digital Passage to Europe – Responsible Data Forum https://responsibledata.io/for-refugees-a-digital-passage-to-europe/ [Accessed 15th June 2016]
Lesk, M. 2013. Big Data, Big Brother, Big Money. *IEEE Security & Privacy*, 11(4): 85–89.
UN Global Pulse, May 2012. Big Data for development: challenges & opportunities.. http://www.unglobalpulse.org/projects/BigDataforDevelopment. [Accessed 10 June 2014].
Lyon, D. 2014. Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society*, 1(2): 1-13.
MacAskill, E., Borger, J., Hopkins, N., Davies, N. and Ball, J. 2013, June 21. GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications. *The Guardian*. http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [Accessed 11 May 2017]
Marr, B. 2015. Big Data, Technology and The Middle East Refugee Crisis - *Forbes*. http://www.forbes.com/sites/bernardmarr/2015/10/15/big-data-technology-and-the-middle-east-refugee-crisis/#7489ca8430c9 [Accessed 15th June 2016].
Mattingly, P. and Svoboda, S. 2015. How the White House Got Silicon Valley to Take On the Refugee Crisis - Bloomberg Politics, October 2015 www.bloomberg.com/politics/articles/2015-10-16/how-the-white-house-got-silicon-valley-to-take-on-the-refugee-crisis [Accessed 15 June 2016].
Mayer-Schönberger, V. and Cukier, K. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston, MA: Houghton Mifflin Harcourt.
Meier, P. 2013. How to Create Resilience Through Big Data, *iRevolutions* (11 Jan) https://irevolutions.org/2013/01/11/disaster-resilience-2-0/ [Accessed 15th June 2016].
Meier, P. 2015. *Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response*. Boca Raton, Florida: CRC Press.
Microsoft Corporation. 2011. UNHCR – Microsoft Partnership: Applying ICT to Support Refugees. Partnership Profile.
Mortera-Martinez. Dec. 2015. Taking Security Seriously in the Age of Global Terror - The Wall Street Journal. http://www.wsj.com/articles/taking-security-seriously-in-the-age-of-global-terror-1450817139 [Accessed 15th June 2016].
Novack, R. 2015. We Should Have Seen This Refugee Crisis Coming. *Wired 22*

September 2015 https://www.wired.com/2015/09/able-predict-refugee-crisis/ [Accessed 15 June 2016].

Palmer, D. Mar, 2014. How IT and Collaboration Tools Help UNHCR Improve the Lives of Refugees - Computing http://www.computing.co.uk/ctg/interview/2337179/how-it-and-collaboration-tools-help-unhcr-improve-the-lives-of-refugees [Accessed 15th June 2016].

Peter, L. 2016. Migrant Crisis: EU Border Security Becomes New Mantra - BBC News. http://www.bbc.co.uk/news/world-europe-35140794 [Accessed 5th June 2016].

Pham, P.N., Comes, M., Van de Walle, B., Wagner, A., Arkwright, C., Gibbons, N. and Vinck, P. 2015. European Refugee Crisis: Data, Technology & Coordination Briefing Note. Dec 17. Harvard Humanitarian Institute. http://atha.se/blog/european-refugee-crisis-data-technology-coordination-briefing-note [Accessed 11 May 2017].

Raley R. 2013. Dataveillance and countervailance. In: Gitelman L (ed.) *Raw Data Is an Oxymoron*. Cambridge, MA: MIT Press, pp. 121–145

Ruppert, E. 2011. Population Objects: Interpassive Subjects. *Sociology*, 45(2): 218–233.

Ruppert, E. 2012. The Governmental Topologies of Database Devices. *Theory, Culture & Society*, 29(4-5): 116-136.

Ruppert, E. 2015. Doing the Transparent State: Open Government Data as Performance Indicators. In: R. Rottenburg; S. E. Merry; S-J Park and J Mugler, eds. *A World of Indicators: The making of governmental knowledge through quantification*. Cambridge: Cambridge University Press, pp. 127-150.

Silva, R. Oct, 2015. Tech City's Response to the Refugee Crisis Shows Real Innovation - Evening Standard. http://www.standard.co.uk/comment/comment/rohan-silva-tech-city-s-response-to-the-refugee-crisis-shows-real-innovation-a3082841.html [Accessed 15th June 2016].

Smith, S. M. 2004. *Photography on the Color Line*. Durham, NC: Duke University Press.

Steenbruggen, J., Borzacchiello, M. T., Nijkampa, P. and Scholten, H. 2013. Data from Telecommunication Networks for Incident Management: An Exploratory Review on Transport Safety and Security. *Transport Policy*, 28: 86–102.

Strathern, M. 2000. The tyranny of transparency. *British Educational Research Journal*, 26(3): 309-321.

Taylor, D. and Graham-Harrison, E. 2016. EU Asks Tech Firms to Pitch Refugee-tracking Systems - The Guardian. https://www.theguardian.com/world/2016/feb/18/eu-asks-tech-firms-to-pitch-refugee-tracking-systems [Accessed 15th June 2016].

Thrift, N. 2011. Lifeworld Inc—and What to Do About It. *Environment and Planning: Society and Space*, 29: 5–26.

Trilateral Research and Consulting. 2015. Privacy Impact Assessment of UNHCR Cash Based Interventions. Improving Cash-Based Interventions Multipurpose Cash Grants and Protection Enhanced Response Capacity Project 2014–2015. Office of the United Nations High Commissioner for Refugees. http://www.globalprotectioncluster.org/_assets/files/tools_and_guidance/cash-based-interventions/erc-privacy-impact-assessment-of-unhcr-cbi_en.pdf [Accessed 31 August 2016]

UN OCHA. 2013. United Nations Office for the Coordination of Humanitarian

Affairs. 2013. Humanitarianism in the Network Age. UN Office for the Coordination of Humanitarian Affairs. https://ochanet.unocha.org/p/Documents/WEBHumanitarianismintheNetworkAgevFsingle.pdf [Accessed 15 Apr 2013].

UNHCR. 2015. The sea route to Europe: The Mediterranean passage in the age of refugees. 1 July 2015. https://s3.amazonaws.com/unhcrsharedmedia/2015/sea-routes-to-europe/The_Sea_Route_to_Europe.pdf [Accessed 15 July 2016].

UNHCR. 2016. Intelligence Analysis Unit: Daily Report for Greece. March 24. http://reliefeb.int/sites/reliefweb.int/files/resources/20160324OperationsCellDailyReport.pdf [Accessed 31 August 2016].

van Dijck, J. 2014. Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology, *Surveillance & Society*, 12: 197-208.