

[**https://www.routledge.com/Big-Data-Surveillance-and-Crisis-Management/Boersma-Fonio/p/book/9781138195431**](https://www.routledge.com/Big-Data-Surveillance-and-Crisis-Management/Boersma-Fonio/p/book/9781138195431)

**Contents**

1. Big Data, Surveillance and Crisis Management, by *Kees Boersma and Chiara Fonio*

**Part I Social media and crisis management**

1. The use of social media for crisis management: a privacy by design approach, by *Muhammad Imran, Patrick Meier* and *Kees Boersma*
2. Mining social media for effective crisis response: machine learning and disaster response, by *Rachel Finn, Hayley Watson* and *Kush Wadhwa*
3. Between the promise and reality of using social media in crisis management: lies, rumours and vigilantism, by *Gemma Galdon Clavell*

**Part II Big Data and health surveillance**

1. Biosecuring public health: the example of ESSENCE, by *Henning Füller*
2. Triggering action: participatory surveillance and event detection in public health emergency management, by *Martin French* and *Baki Cakici*

**Part III Case studies on disasters, crisis and big data**

1. Resilience, surveillance and big data in crisis management: case studies from Europe, the United Kingdom and New Zealand, by *Charles Leleux* and *C. William R. Webster*
2. Monitoring a big data cyclon: the Sardinian case, by *Allesandro Burato*
3. Intersecting intelligence: exploring big data disruptions, by *Xaroula Kerasidou*, *Katrina Petersen* and *Monika Büscher*
4. ‘Value-Veillance’: Opening the black box of surveillance in emergency management, by *Karolin Eva Kappler* and *Uwe Vormbusch*
5. Times of crises and the development of the Police National Automatic Number Plate Recognition System in the UK, by *Clive Norris* and *Xavier D L'Hoiry*

**Chapter 1. Big Data, Surveillance and Crisis Management (page 1-16)**

*Kees Boersma and Chiara Fonio*

1. **Introduction: dealing with information in crisis management**

Today, societies face many potential threats that can turn into crisis situations. Crises (emergencies) upset society, and put its critical infrastructures under stress (Quarantelli 1998; Comfort et al. 2010).[[1]](#footnote-1) Once a crisis occurs organizations, both public and private, are supposed to ‘fight’ the crisis and form coalitions with other agencies and local communities. Since crises are often characterized by multiple causes, ambiguity of effects, and various means of resolution, as well as by a shared belief that decisions must be made swiftly (Pearson and Clair 1998; Van der Vegt et al. 2015), information management is a vital component of preparedness, response and relief. An adequate and effective information management that supports crisis organizations requires processes to collect, analyse and share information about the crisis situation, and about the coordination between the responding organizations. When a crisis occurs, information managers start to collect and produce standard information products to support the coordination of the response operation (Comfort et al. 2004; Oh et al. 2013).

In addition to the data collected, shared, analyzed and used by official organizations, administrations and mainstream media, citizens inform themselves and others about crisis situations through social media platforms, generating bottom-up information networks (Palen 2008; Hughes and Palen 2009; Yates and Paquette 2011). All those actions contribute to the ‘explosion’ in the amount of data and information at times of disasters, which is a challenge for responding organizations to deal with. For example, because crisis information may become outdated soon as crisis conditions change, crisis response needs the management of information flows and networks to build an effective crisis response organization (Pan et al. 2012). Crisis responders then rely on traditional information systems such as enterprise resource systems, but since digital data are practically ubiquitous, the emerging information networks form potentially useful additional sources for the organization of the crisis response. Together, they create a crisis information ecology of dynamic information streams (Turoff et al. 2004; Van de Walle et al. 2009). Information ecology traditionally refers to the total information environment of organizations (Davenport and Prusak 1997) - to understand the characteristics of this ecology is of crucial importance to grasp how people really use information, how they search for it, modify it, share it, or even ignore it. Crisis information management implies that data can be translated into ‘actionable’ information to increase the quality of the crisis response (Boersma et al. 2012; Wolbers and Boersma 2013). In a crisis situation the information ecology leads to a crisis information paradox: on the one hand the (governmental) responding organizations and administrations want to stay *in control* by harvesting and integrating the various and heterogeneous data sources in their information management systems, on the other hand the complex nature of the information ecology make an authoritarian response structure virtually impossible.

With the increased availability of data for effective crisis response, new challenges are added to the burden of crisis management. There are serious concerns related to the (lack of) information standards and accountability mechanisms (Turoff 2002), information overload (Hiltz and Plotnick 2013), the lack of interoperability between the information and communication technologies used by the first responders and the communication sources used by citizens (Truptil et al. 2008), and underdeveloped (big) data analytical skills by the users of crisis information. At the same time, crises, disasters and social disruptions are seen as opportunity windows to create legitimacy to collect and analyse citizens’ data on a large scale (Fonio et al. 2007). In other words, the use of crisis information systems, i.e. networks of hardware and software, to create, collect, filter, process, and distribute data is not neutral, but related to the way crisis information management is organized and legitimized.

1. **The big data debate in crisis and disaster management**

Increasingly, crisis information management includes the processing and use of *big data* by (governmental) responding organizations in order to try to control the crisis situation. Big data refers to a quantitative increase of the size of the datasets that can be used for analytical purposes by a wide range of actors, including academics, marketers, governmental bodies, educational institutions, and – in the context of this book – crisis managers (boyd and Crawford 2012; Shelton et al. 2014). One of the most widely accepted ways to describe big data is the “three V’s” (volume, variety, and velocity) of information (McAfee et al. 2012). ‘Volume’ refers to the generation and collection of data, and implies that the data volume becomes increasingly larger. “Velocity” addresses the timeliness of the data, and the speed of data collection, analysis and use to maximize its utility; finally, “Variety” indicates the various types of data, including semi-structured, unstructured, validated and unvalidated, raw and analyzed data and its technical sources, such as audio, video, webpage, and text (Mayer-Schönberger and Cukier 2013; Chen et al. 2014). Potentially the use of big data will change the way responding organizations make sense of the crisis situations, respond to it and make decisions concerning the crisis response.

For example, a serious challenge at times of crisis is to create a ‘common operational picture’ of the situation and of the actions and interactions of others involved in the crisis management (Wolbers and Boersma 2013). Crisis managers can use big data analytics to create improved operational pictures (Wukich 2015). Another example is the use of *social media* data by crisis management organizations as part of early warning systems (Culotta 2010), and for crowd control and monitoring (Trottier and Schneider 2012; Boersma 2013; Procter et al 2013). There is growing evidence that social media data can contribute to a better understanding of the situation and eventually to a more adequate and robust crisis management (Yin et al. 2012; Cassa et al. 2013). The use of social media data in crisis management, its intended and unintended consequence, is a central issue in the first part of this book (chapters 2, 3 and 4). Because of the promising character of social media data governmental administrations, private organizations and non-governmental organizations invest a lot in crisis management information systems that can harvest valuable data from social media sources. For example, *Twitcident* is a tool used by professionals in emergency control rooms to follow what (relevant) data citizens post on Twitter for the purpose to maintain security in urban environments (Boersma et al. 2016).

The use of big data for any purpose should not be taken for granted as it requires adequate data and information management (Pries and Dunnigan 2015). Databases can indeed generate patterns that have *predictive* power for the crisis operations but not necessarily and automatically *explanatory* power (Andrejevic 2014). It is the extraction of structured data from unstructured inputs that is the most challenging and the biggest gab in the understanding of those who want to use big data in the context of crisis response (Castillo 2016). The availability of big crisis data does not always entail, let alone guarantee, effective crisis management.

However, Floridi (2012) argues that becoming data-richer by the day cannot be perceived as a fundamental problem per se. Big data undoubtedly represents an opportunity in disaster management, especially since “digital humanitarians” appeared on the scene. From the 2010 Haiti earthquake onward, disaster response has been redefined by new players, namely digital volunteers who have supported search and rescue effort through, for instance, the generation of maps or the interpretation of big amounts of data (Mulder et al. 2016). Digital humanitarians – as they are labelled - form a “crowd” that provides various services, such as building situational awareness from social media or generating maps, while using information and communication technology (Link et al 2014). Digital humanitarians have played a vital role in verifying the accuracy of information shared in social media during crises and, in some cases, they have actively shaped disaster response in the aftermath of a major event by helping first responders’ organizations (Burns 2014).

The rise of big crisis data has been explored in the context of humanitarian response, in particular during or in the aftermath of a natural disaster (Meier 2015; Castillo 2016). Increasingly, a sheer amount of data is generated through social media during crises: when a major disaster strikes, a “digital nervous system” (Meier 2015: 27) reacts through various synapses encapsulated in various forms of communication, from tweets to pictures posted on social media. While, in this specific context, the expression ‘big crisis data’ does not have a negative connotation but instead refers to data generated by affected communities and used for the purpose of helping them, it is worth noting that a disaster can turn into a ‘big data crisis’ if first response organizations do not have the capacity to deal with potential valuable information shared in social media. As emphasized by the International Federation of Red Cross and Crescent Societies in 2005 “people need information as much as water, food medicine or shelter. Information can save lives, livelihood and resources. Information bestows power”. Therefore, in current practices of disaster management, it is essential to ensure a proper use of social media during crisis to respond to the information needs of the communities affected by disasters.

It means that the use of big data at times of crisis (and the outcome of the digital humanitarians’ actions for that matter) is not without problems. Like any hype in information and communication technology it asks for a critical analysis: it can trigger processes of change, but also easily can become an empty promise (Meier et al. 2009). A real epistemological problem with big data, according to Floridi, is detecting small and meaningful patterns. This is of particular relevance in the field of crisis management and raises questions that seem to remain unsolved, such as to what extent real-time big crisis data can enhance disaster response instead of turning into a big data crisis due to challenges to work with new data sources. Hence, the debate on the use of big data is concerned with methods used to make sense of data (namely, detecting meaningful small patterns) and decisions made upon the interpretation of patterns. Big crisis data is subject to interpretation and bias like any other data sources (boyd and Crawford 2012). In addition, humanitarianism has been critiqued as a social relation that often privileges people from the global North: data and technologies often reify social and power relations, worldviews, and epistemologies (Elwood and Leszczynski 2013; Burns 2015).

In sum: big crisis data should not be considered as a magic bullet which can save lives just because they are available.

1. **Surveillance crisis management: the intended and unintended consequences of big data in-use**

Whereas in the creation of common operational pictures the use of crisis data from social media and other data sources is promising but problematic in itself for various practical and more fundamental reasons (because of the reasons addressed above), in this edited volume we are in particularly interested in the *surveillance aspect* of crisis management. We believe the surveillance debate is significant for the crisis and disaster studies. The surveillance ‘lens’ is a powerful ‘empirical window’ through which we witness how people and their data doubles (i.e. the on-line identities or classifications that represent the individual to which they are attached, see: Lyon 2007) are being monitored and controlled (Jenness et al. 2007) at times of disasters – and as a consequence of disaster relief.

In disaster response, surveillance practices are used for different purposes and in different phases. Currently the big data debate in disaster management cannot be disentangled from the role of digital humanitarians who seem to have made good use of surveillance practices (e.g. data mining) on the internet. These practices resonate with the concept of “lateral surveillance” as defined by Andrejevic (2002): the use of surveillance tools by individuals rather than by institutions to keep track of each other for several purposes. One could argue that digital humanitarians practice lateral surveillance for humanitarian and crisis management purposes. For instance, surveillance has taken the form of automatic classification of tweets or mapping geo-tagged information. These practices have been explored through lenses which are different from the dystopian views sometimes embedded into surveillance studies. At the same time, data collection, especially of people affected by disasters through different means, is also considered as a routine practice in order to assist individuals and communities. The dimension of *control*, however, is often overlooked in the literature of crisis management due to the positive connotation of control for assessing needs, helping people, and counting human and economic losses.

The surveillance lens helps us to understand how crisis management has become an integral part of what has been called the “surveillance society” (Ghandi 1989; Wood et al. 2006; Ball et al. 2012). Surveillance refers to the rational modernistic thinking: “any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered” (Lyon 2001). Surveillance is a consequence of processes of modernity (Giddens 1985) and became an inherent part of our network societies (Castells 2001). Although the state and state agencies have been playing a major role in surveillance societies (Haggerty and Samatas 2010; Wagenaar and Boersma 2008; Webster et al. 2012; Boersma et al. 2014), surveillance is about much more than state control. Haggerty and Samatas (2010) define surveillance as an activity that involves “assorted forms of monitoring, typically for the ultimate purpose of intervening in the world” (p. 2). The use of computerized systems enables electronic forms of surveillance, not just because electronic databases made it easy to store huge amounts of personal data, but because it has changed surveillance practices.

The speed of data flows has increased, databases became de-centralized and easily accessible, and individuals more easily traced. The Internet enabled a global networked form of surveillance (Fuchs et al. 2011). It has led to *datafication* as a new paradigm in science and society (Van Dijck 2014). Datafication refers to the transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis. Edward Snowden revealed how analysis of such data potentially undermines privacy and civil liberties: governments engage in mass surveillance of their own citizens, contradicting basic democratic practices (Greenwald 2014; Lyon 2015). The use of metadata for surveillance practices, in this respect, is not just the outcome of the use of technologies, such as the storage capacity, but of specific approaches to risk management in for security industries and of consumer clustering in marketing (Andrejevic 2014; Andrejevic and Gates 2014).

Yet, the link between crisis management and surveillance has been rarely explored in surveillance studies. This is perhaps due to the fact that the *surveillant* aspect of crisis management is often perceived as less negative in comparison to other forms of monitoring. For instance, if the surveillance society we live in is characterized by increased investments in bureaucracies and techniques to systematically and over longer time-periods collect, store and use information for the purpose of controlling behaviours and situations, crisis management practices do not have the primary goal of storing information for controlling behaviour. In that sense it is different from *dataveillance* that entails the continuous tracking of (meta)data for unstated pre-set purposes (Andrejevic 2012). At the same time, current crisis management and governance almost ‘cries’ for big data. In this process crisis managers and disaster scholars tend to overlook the dark site of big data collection, storage and analysis.

Recent revelations about the extent of collection, processing and analysis of data at times of crisis in the name of *security* have raised concerns that there is a dangerous trade-off of privacy and liberty against safety and security (Büscher, Perng and Liegl 2015). It is hard to resist the urge to gather more data on crisis situations just because it is possible and potentially useful for improved crisis response. Big data in crisis management, however, also needs to be examined as a political process involving questions of power, transparency and surveillance. For example, as Kerasidou, Petersen and Büscher show in chapter 9 of this book, the refugee crisis and its escalation in Europe resulted in debates on the importance of the control of external borders to protect “fortress Europe” (Hadfield and Zwitter 2015). This crisis has intensified calls for more security measures (in particular in response to the recent terrorist attacks in Paris and Berlin), and the use of big data - not just to improve operational pictures for crisis response, but to ensure security. The problem here is not so much that coping strategies of citizens affected by cries (here: refugees) won’t work, but rather that there is “asymmetry of power between the individual, groups and society as a whole at the one hand, and organizations and state authorities who initiate or implement surveillance measures on the other” (Wright and Kreissl 2015, p. 371).

In this respect, security is being equated with *visibility*. But how individual refugees are made visible matters for both their privacy and security. Surveillance in crisis management is more than just monitoring individual person’s movements, communications and actions. Using big crisis data analysis involves political questions such as: how are the refugees doing what they are doing, what are the patterns of displacement, and how does the that relate to larger social questions like migration and integration, democratic processes and (protecting) the welfare state. This deserves a critical reflection on fundamental concepts of privacy law, including the definition of “personally identifiable information”, the role of individual control, and the principles of data minimization and purpose limitation (Tene and Polonetsky 2012). A similar debate emerges in the context of public *health.* Administrations in this context increasingly rely on big data and real-time surveillance to establish ‘early warning systems’ on the basis of social-media infrastructures for participatory surveillance (see the chapters by Füller, and by French and Cakici in part 2 of this book). At the one hand this will result in improved risk assessment, prevention and efficient crisis management approaches, at the other hand it might lead to privacy violation as part of public health monitoring.

Again, this dark side of big data surveillance has hardly been problematized in the field of crisis management; on the contrary, taking advantage of information shared through social media during crisis through *ad hoc* techniques has been positively framed. It is telling that the U.S. Federal Emergency Management Agency (FEMA) has a dedicated smartphone app “to crowdsource pictures during disasters” (Meier 2015: 176). This way of dealing with data is not considered to be “dark” but rather helpful for effective crisis response. In this book, however, we will draw attention to all the aspects of surveillance in crisis management. Therefore, we have put together contributions which aim at fostering the debate both in surveillance studies and in crisis management studies by dealing with:

* The intended and unintended consequences of surveillance when dealing with big (social media) crisis data,
* Big data and crisis management in the context of public health,
* Case studies which range from resilience at times of natural disasters such as the response to the earthquake in Christchurch, New Zealand, to the use of Police National Automatic Number Plate Recognition in the UK.

The chapters that follow will critically discuss various aspects of big data in the context of crisis management. It will be clear that big data analytics can enable a more efficient and effective crisis response. At the same time, this book aims at provoking discussion and debate on the often overlooked *surveillance* aspect of big data in crisis management. The authors of the various chapters will touch upon issues such as transparency and monitoring, democratization and human rights, privacy protection and the rampant disclosure of personal data. Surveillance practices in crisis response have become interwoven with social and political dynamics including public health, globalization and migration, international terrorism and security. This book will reveal the many faces of surveillance in this context: one cannot paint all surveillance in crisis management in black and white terms.

Finally, this book acknowledges the growing awareness among professionals (and citizen groups for that matter) that surveillance issues in crisis management deserve more attention. For example, the privacy by design approach has been recognized by digital humanitarians to take privacy protection into account early on in the design of crisis information systems. More transparency, accountability and legality are certainly needed. But more importantly is raising awareness and creating a sense of urgency among those involved in (studying) crisis management to take the dark site of monitoring on the basis of data seriously. With this book we critically engage in the debate on big data in the context of crisis management.

1. **Structure and content of the book**

We have divided the chapters of this volume into three different parts: part one is about social media and crisis management, part 2 about big data and health surveillance and the final part 3 about case studies on disasters, crisis and big data.

The ***first part*** of the book further develops the idea that big data can enable a more adequate and effective crisis and disaster response. At the same time it addresses serious concerns related to surveillance practices and privacy (violation) in the context of crisis information management. This part of the book contains three chapters.

In Chapter 2, *Muhammad Imran*, *Patrick Meier* and *Kees Boersma* present an in-depth discussion about social media, big data in the context of digital humanitarianism. They show how social media platforms such as Twitter, Facebook fostered the open environment and convenient ways to produce, share and consume information as fast and easy as never before. Recent years have witnessed a huge influx of information in the form of text, images, videos, SMS that people observe, report, collect and disseminate through social media platforms. Effective crisis management, the authors argue in this chapter, requires cooperation in terms of exchanging valuable information between many crisis management organizations as well as affected people located in different places. At the same time, they ask attention for the – often overlooked - unintended consequences of the use of big data at times of disasters including privacy violation. The authors show why citizen-generated content contains valuable information that can enhance crisis response, and elaborate on the critical issues concerning data processing. Crisis management agencies, they show, have recently started including social media information into their decision-making process during a crisis situation. However, there are numerous challenges in the use of social media data for crisis response. The authors elaborate various challenges that formal disaster management agencies face to successfully filter, process and utilize social media data into disaster response. They propose *privacy by design* as a useful approach for digital humanitarians to take the special requirements of privacy protection into account early on in the design of crisis information systems. Finally Privacy by design might prevent data to be collected not necessary for the purpose of the needed analysis.

In Chapter 3, *Rachel Finn*, *Hayley Watson* and *Kush Wadhwa* pay attention to mining social media for effective crisis response. The authors undertake an in-depth examination of the interaction between human and machine computing to mine social media data for crisis response. The chapter focuses on a specific case study using social media for crisis response to understand how this activity results in positive and negative impacts for those whose data is being mined. As such, it moves beyond current theoretical discussions of the potential impacts of big data to identify where and how these impacts are manifested during actual practice. The authors conclude that the use of big data in crisis exemplifies the Janus-faced nature of surveillance, as crises are a key area in which the *care* elements of surveillance practices emerge, but where *control* elements of surveillance may also be apparent. However, they also find that although there are potentials for big data practices in crises to generate impacts similar to authoritative surveillance, the involvement of humanitarian organisations in this case study appears to mitigate many of those impacts. Specifically, humanitarian organisations recognise these potential impacts and use a variety of tools and strategies to ensure robust protections for members of the public.

Finally, in Chapter 4, *Gemma Galdon Clavell* unravels the use of social media surveillance in disaster management. She argues that in the context of crisis management, all the stakeholders deem helpful to optimize the information available to take decisions and the communication procedures to better intervene before, during and after a disaster. While providing this information was traditionally a monopoly of formal media outlets, she reflects upon recent developments in information and communication technologies, and specifically the growing use of social media, and argues that they provided new possibilities for emergency management – but also challenges. This increasing interest on the use of social media is explained because they provide unprecedented access to information for first responders and other decision-makers, as well as an ability to rapidly disseminate information. However, using participatory tools in emergency management can also lead to wrongful accusations, inefficiencies and mistakes. This complex role of social media makes it a sensitive tool for all stakeholders, and one that requires a careful understanding of the legal, social and ethical impact of its use if its potential is to be realised. The chapter tackles some of these challenges by reviewing both the state of the art of technological solutions and institutional programmes leveraging the use of social media in crisis management. It summarises real-life cases of the use of social media in such settings, revealing both their potential and their shortcomings. By presenting a brief state of the art based on current practices, the author sheds light on how to account for and minimise societal risks in the design and implementation of participatory tools in the context of crisis management.

The ***second part*** of the book is about big data and health surveillance. The developments in big data and crisis management in the context of health related crisis are important not just for the way they configure public health problems, but also for the kinds of governance they imagine and call into being. The authors in this part of the book are concerned with the ongoing “securitization” of health for which administrations increasingly rely on big data and real-time surveillance. This part contains two chapters.

In Chapter 5, by *Henning Füller* is on biosecuring public health and gives the example of ESSENCE (Electronic Surveillance System for the Early Notification of Community-based Epidemics). Drawing on the implementation of the ESSENCE syndromic surveillance system in the U.S. National Capitol Region, Henning aims to point out truth-effects and epistemological shifts in public health practice related to big data. Considering the discourse of digital health technologies in the National Capital Region as well as its use ‘on the ground‘ in several County health departments, the author shows how the promise of data-driven detection and early warning is active in reworking public health towards a pre-emptive rationality. Syndromic surveillance seems to be the right tool confronting the threat of ‘emerging diseases‘ but it is also establishing this very problem perception. Furthermore, working with this system may lead to a de-qualification of health related truth production and real-time surveillance is re-centring attention and resources towards the proof of the non-event.

In Chapter 6, *Martin French* and *Baki Cakici* write about big data and crisis management in the context of public health intelligence. They argue that contemporary developments in public health monitoring and crisis management - particularly those that are meant to leverage big data and social-media infrastructures for participatory surveillance - have less to do with monitoring and making up populations, but more with monitoring and making up *events*. The authors provide a background discussion of global health security and the millennial preoccupation - in the global north - with emerging infectious disease. They offer a preliminary consideration of emergent modes of public health monitoring and event detection. The chapter provides an analytic framework to present an overview of select touchstones for research into event-oriented public health monitoring and crisis management. The authors focus on the event as a key, active concept, and consider the forms of knowledge, diverse informants, and organizational initiatives that this discursive configuration of public health crises presupposes. They conclude with a discussion of the wider implications of the rise of event detection in public health monitoring, and suggest that big data-enabled modes of participatory public health event detection are a key site for future surveillance studies scholarship.

***Part three*** of this edited volume presents five chapters with case studies in different contexts on disasters, crisis and big data.

In Chapter 7, *Charles Leleux* and *C. William R. Webster* address the topic of *resilience* and surveillance in crisis management, illustrated by case studies from Europe, the UK and New Zealand. This chapter examines the emergent intertwined relationship between resilience and surveillance in contemporary crisis management processes in a number of different settings. In doing so, the chapter explores the evolution of established crisis management institutions and techniques alongside the increasing use of new technologies. At the heart of the chapter lies analysis of three different, but complementary, case studies, each exploring resilience and surveillance at a different level, the supra-national, national and local levels, involving different institutions, actors and actions. This analysis draws out comparable, complementary and conflicting activity and highlights the degree to which traditional crisis management processes are resilient to societal and technological change, and the increasing role played by surveillance technologies in this process. The cases presented in the chapter are: civil protection and resilience within the European Union (the supra-national level); the role of the Westminster and Scottish Governments in crisis management and resilience building in the UK (the national level), and the resilience of the local community and local/national agencies in response to the earthquake in Christchurch, New Zealand, 2011 (the local level). The chapter provides new knowledge through case study methodology and comparative analysis, of the strength of the link between resilience and surveillance, and surveillance technologies, in the context of crisis management, at the supra-governmental, national and societal levels.

In Chapter 8, *Allesandro Burato* asks attention for monitoring a *big data cyclon* with illustrations by the Sardinian case. In this chapter, social media in relation to surveillance, monitoring and privacy issues is central. The author argues that there is an increasing concern about how information shared via these new ways of communication is intercepted, stored, analysed and eventually used. Leaving aside all the daily aspects in which social media are used and focusing only on crises, when the public interest and the seeking of information related to the event in question raise exponentially, they are thought to be the best-unfiltered and up-to-date way of receiving information. Among them, *microblogging* is the most adopted form not only to look for information but also to share it, making the public information producer. The author builds upon the various studies that have shown how microblogging-generated big data can enable crisis management: they are a source for the creation of situational awareness by allowing users to rapidly send short messages through different platforms and they can sensibly improve emergency response by drawing a pre-disaster assessment.

Next, *Xaroula Kerasidou*, *Katrina Petersen* and *Monika Büscher*, in Chapter 9, explore the disruptive momentum of big data in crisis management. Taking departure in discourses on big data in the global refugee crisis and its manifestation in Europe in 2015/16, they identify complex socio-technical dynamics of ‘intersecting intelligence’. The ‘datafication’ of everyday life even in crises may enable a richer common operational picture and understanding of crisis. But it also frames the socio-political complexities of crises as a problem of intelligence and information/data, fostering practices of categorization that can have far-reaching effects on human rights and values of equality and freedom. By exploring frictions at the intersections of different types and practices of ‘intelligence’, the authors argue that understanding big data as disruptive can enable more creative, critical and ethically circumspect innovation.

In Chapter 10, *Karolin Eva Kappler* and *Uwe Vormbusch* introduce the concept ‘Value-Veillance’. The chapter offers a new perspective on big data, surveillance and crisis management by adapting approaches from the fields of financial sociology as well as from the emerging field of the social studies of valuation. It presents a detailed description of how surveillance ‘is made’. Based on a qualitative study of research documents, scientific publications and interviews with developers of big data-algorithms and stakeholders in emergencies, the chapter analyses how algorithms work and how they are meant to work through the lens of valuation studies. Following key concepts within sociology, such as performativity, sociocalculation or social inequality, several crucial thresholds in algorithmic practices are detected and critically questioned. In order to draw attention to the black box of surveillance based on algorithmic processes and on big data, the authors propose the term “value-based surveillance” or “valueveillance”, claiming that algorithms have to be considered key actants in the field of surveillance.

Finally, *Clive Norris* and *Xavier D L'Hoiry* present the development of the Police National Automatic Number Plate Recognition (ANPR) Network in the UK in Chapter 11. It tracks the historical development of ANPR surveillance technologies in the UK and specifically the use of this surveillance tool by the British police. In particular, the chapter traces the growth of the use of ANPR against high-profile instances of crises in the form of political unrest and terrorist attacks. The authors outline the development of the National ANPR Strategy in the UK, which has led to a network of over 8,000 cameras feeding into a centralised police database. They also consider the current operational uses of ANPR in the context of big data before describing some key controversies that have arisen surrounding ANPR. In discussing these instances of controversy, the analysis in this chapter demonstrates the manner in which national security can be applied as a blanket exemption which seemingly supersedes other key public interests arguments such as informational rights and freedom of information. The analysis culminates by highlighting the crisis in democratic oversight and the rule of law brought about by the ongoing proliferation of ANPR surveillance which has continued in the UK in the absence of any statutory regulatory instruments. The impact upon transparency and accountability is fundamental and profound, and eventually the authors discusses how and why the police, together with the British government, have been able to continue developing ANPR technologies outside of such basic democratic principles.

**References**

Andrejevic, M. 2002. The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4): 479-497.

Andrejevic, M. 2012. Exploitation in the data-mine. In: *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, eds C. Fuchs, K. Boersma, A. Albrechtslund, and M. Sandoval, 71-88. New York: Routledge.

Andrejevic, M. 2014. Surveillance in the big data era. In *Emerging Pervasive Information and Communication Technologies* (PICT) (pp. 55-69). Springer Netherlands.

Andrejevic, M. and Gates, K. 2014. Big data surveillance: Introduction. *Surveillance & Society*, 12(2): 185-196.

Ball, K., Haggerty, K. and Lyon, D. (Eds.) 2012. *Routledge Handbook of Surveillance Studies*. London: Routledge.

Boersma, K., Wagenaar, P. and Wolbers, J. 2012. Negotiating the ‘Trading Zone’. Creating a shared information infrastructure in the Dutch public safety sector. *Journal of Homeland Security and Emergency Management*, 9(2): 6.

Boersma, K. 2013. Liminal Surveillance. Intensified use of an existing CCTV system during a local event. *Surveillance & Society*, 11(1/2): 106-120.

Boersma, F.K., van Brakel, R., Fonio C. and Wagenaar F.P. (Eds.). 2014. *Histories of State Surveillance in Europe and Beyond*. London: Routledge.

Boersma, F.K., Diks, D., Ferguson J. and Wolbers, J.J. 2016. ‘From Reactive to Proactive Use of Social Media in Emergency Response: A Critical Discussion of the Twitcident Project’, in Silvius, G. (Ed.). *Strategic Integration of Social Media into Project Management Practice*, IGI, pp. 236-252.

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.

Burns, R. 2014. Moments of closure in the knowledge politics of digital humanitarianism. *Geoforum*, 53: 51-62.

Burns, R. 2015. Rethinking big data in digital humanitarianism: practices, epistemologies, and social relations. *GeoJournal*, 80(4): 477-490.

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

Cassa, C.A., Chunara, R., Mandl, K. and Brownstein, J.S. 2013. Twitter as a sentinel in emergency situations: lessons from the Boston marathon explosions. *PLoS currents*, 5.

Castells, M. 2001. *The rise of the network society: The information age: Economy, society, and culture* (Vol. 1). Oxford: Blackwell.

Castillo, C. 2016. *Big Crisis Data*. Cambridge: Cambridge University Press.

Chen, M., Mao, S. and Liu, Y. 2014. Big data : A survey. *Mobile Networks and Applications*, 19(2): 171-209.

Comfort, L.K., Ko, K. and Zagorecki, A. 2004. Coordination in rapidly evolving disaster response systems the role of information. *American Behavioral Scientist*, 48(3): 295-313.

Comfort, L.K., Boin, A. and Demchak, C.C. (Eds.). 2010. *Designing resilience: Preparing for extreme events*. Pittsburg: University of Pittsburgh Press.

Coombs, W.T. 2015. *Ongoing Crisis Communication* (4th ed.). Thousand Oaks, CA: Sage

Culotta, A. 2010, July. Towards detecting influenza epidemics by analyzing Twitter messages. In Proceedings of the first workshop on social media analytics. *ACM*: 115-122.

Davenport, T.H. and Prusak, L. 1997. *Information ecology: Mastering the information and knowledge environment*. Oxford: Oxford University Press.

Floridi, L. 2012. Big data and their epistemological challenge. *Philosophy & Technology*, 25: 435–437.

Fonio, C., Giglietto, F., Pruno, R., Rossi, L. and Pedrioli, S. 2007. Eyes on you: Analyzing user generated content for social science. *Towards a Social Science of Web*, 2.

Fuchs, C., Boersma, F.K., Albrechtslund A. and Sandoval M. (Eds.). 2011. *Internet and Surveillance*. London: Routledge.

Gandy, O.H. 1989. The surveillance society: information technology and bureaucratic social control. *Journal of Communication*, 39(3): 61-76.

Giddens, A. 1985. *A Contemporary Critique of Historical Materialism: The nation-state and violence* (Vol. 2). Berkeley: University of California Press.

Greenwald, G. 2014. *No place to hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Picador.

Haggerty, K.D. and Samatas, M. (Eds.). 2010. Surveillance and Democracy. New York: Routledge-Cavendish.

Hadfield, A., and Zwitter, A. 2015. Analyzing the EU Refugee Crisis: Humanity, Heritage and Responsibility to Protect. *Politics and Governance*, 3(2): 129-134.

Hiltz, S.R. and Plotnick, L. 2013. Dealing with information overload when using social media for emergency management: emerging solutions. In *Proceedings of the 10th international ISCRAM conference*: 823-827.

Hughes, A.L. and Palen, L. 2009. Twitter adoption and use in mass convergence and emergency events. *International Journal of Emergency Management*, 6(3): 248-260.

International Federation of Red Cross, Red Crescent Societies, & Centre for Research on the Epidemiology of Disasters. 2005. *World Disasters Report*. Kumarian Press.

Jenness, V., Smith, D. and Stepan-Norris, J. 2007. Editors' Note: Taking a Look at Surveillance Studies. *Contemporary Sociology: A Journal of Reviews*, 36(2): vii-viii.

Link, D., Meesters, K., Hellingrath, B. and Van de Walle, B. 2014. Reference Task-based Design of Crisis Management Games. In *Proceedings of the 11th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*: 592-596.

Lyon, D. 2001. *Surveillance society: monitoring everyday life*. Buckingham: Open University Press.

Lyon, D. 2007. *Surveillance studies: An overview*. Cambridge: Polity Press.

Lyon, D. 2015. The Snowden stakes: challenges for understanding surveillance today. *Surveillance & Society*, 13(2): 139-152.

Mayer-Schoenberger, V. and Cukier, K. 2013. *Big Data. A Revolution that will transform how we live, work, and think*. London: John Murray Publishers.

McAfee, A., Brynjolfsson, E., Davenport, T.H., Patil, D.J. and Barton, D. 2012. Big data. The management revolution. *Harvard Bus Review*, 90(10): 61-67

Meijer, A., Boersma, F.K. and Wagenaar, P. (Eds.). 2009. *ICTs, Citizens and Governance: After the Hype!* Amsterdam: IOS Press.

Meier, P. 2015. *Digital humanitarians: how big data is changing the face of humanitarian response*. Crc Press.

Mulder, F., Ferguson, J., Groenewegen, P., Boersma, F.K. and Wolbers, J. 2016. Questioning Big Data: Crowdsourcing crisis data towards an inclusive humanitarian response. *Big Data & Society*, 3(2): 1-13.

Oh, O., Agrawal, M. and Rao, H.R. 2013. Community intelligence and social media services: a rumor theoretic analysis of tweets during social crises. *MIS Quarterly*, 37(2): 407-426.

Palen, L. 2008. Online social media in crisis events. *Educause Quarterly*, 31(3): 12.

Pan, S.L., Pan, G. and Leidner, D.E. 2012. Crisis response information networks. *Journal of the Association for Information Systems*, 13(1): 31-56.

Pearson, C.M. and Clair, J.A. 1998. Reframing crisis management. *Academy of Management Review*, 23: 59–76.

Pries, K.H. and Dunnigan, R. 2015. *Big Data Analytics. A Practical Guide for Managers*. London: Routledge.

Procter, R., Vis, F. and Voss, A. 2013. Reading the riots on Twitter: methodological innovation for the analysis of big data. *International journal of social research methodology*, 16(3): 197-214.

Quarantelli, E.L. (Ed.). 1998. *What is a disaster?: perspectives on the question*. London: Routledge.

Shelton, T., Poorthuis, A., Graham, M. and Zook, M. 2014. Mapping the data shadows of Hurricane Sandy: Uncovering the sociospatial dimensions of ‘big data’. *Geoforum*, 52: 167-179.

Tene, O. and Polonetsky, J. 2012. Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, 11: xxvii.

Trottier, D. and Schneider, C. 2012. The 2011 Vancouver riot and the role of Facebook in crowd-sourced policing. BC Studies: *The British Columbian Quarterly*, 175: 57-72.

Truptil, S., Bénaben, F., Couget, P., Lauras, M., Chapurlat, V. and Pingaud, H. 2008. Interoperability of information systems in crisis management: Crisis modeling and metamodeling. In *Enterprise Interoperability III* (pp. 583-594). Springer London.

Turoff, M. 2002. Past and future emergency response information systems. *Communications of the ACM*, 45(4): 29-32.

Turoff, M., Chumer, M., Van de Walle, B. and Yao, X. 2004. The design of a dynamic emergency response management information system (DERMIS). *Journal of Information Technology Theory and Application*, 5(4): 1-35.

Van de Walle, B., Turoff, M. and Hiltz, S.R. (Eds.). 2009. *Information systems for emergency management*. New York: ME Sharpe.

Van Dijck, J. 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, 12(2): 197.

Vegt, van der, G.S., Essens, P. Wahlström, M. and George G. 2015. From the editors. Managing risk and resilience, *Academy of Management Journal*, 58(4): 971–980.

Wagenaar, P. and Boersma, F.K. 2008. Soft Sister and the Rationalization of the World: The Driving Forces Behind Increased Surveillance. *Administrative Theory & Praxis*, 30(2): 184-206.

Webster, C.W.R., Balahur, D., Zurawski, N., Boersma, F.K., Ságvári, B. and Backman, C. (2012). Living in Surveillance Societies: The Ghosts of Surveillance. *Proceedings of LISS Conference* (Vol. 2).

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

Wood, D.M., Ball, K., Lyon, D., Norris, C. and Raab, C. 2006. *A report on the surveillance society*. Surveillance Studies Network, UK.

Wright, D. and Kreissl, R. (Eds.). 2015. *Surveillance in Europe*. London: Routledge.

Wukich, C. 2015. Social media use in emergency management. *Journal of Emergency Management*, 13(4): 281-295.

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

Yin, J., Lampert, A., Cameron, M., Robinson, B. and Power, R. 2012. Using social media to enhance emergency situation awareness. *IEEE Intelligent Systems*, 27(6): 52-59.

1. A crisis is a low-probability, high-impact event that threatens the viability of the system. In a narrow sense, crisis management is defined as “a set of factors designed to combat crises and to lessen the actual damage inflicted by a crisis” (Coombs 2015). In this edited volume, crisis management is considered as an “umbrella term” which covers the response to a number of disasters (i.e. from incidents and accidents to pandemics and earthquakes) and a number of ways of managing and/or dealing with crisis. [↑](#footnote-ref-1)