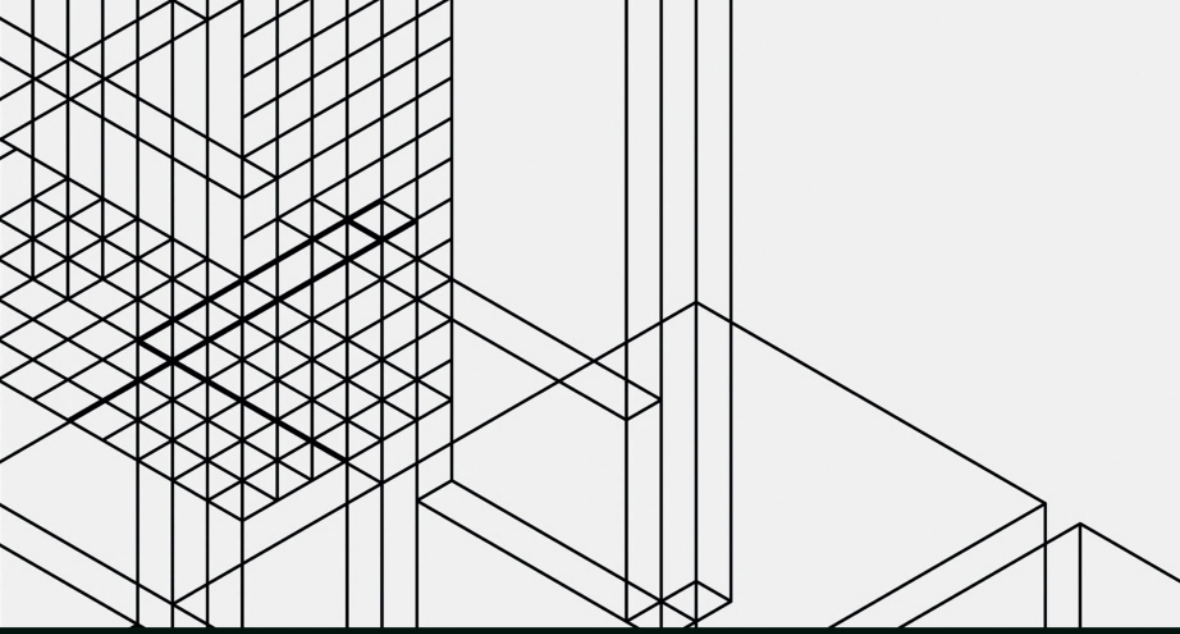
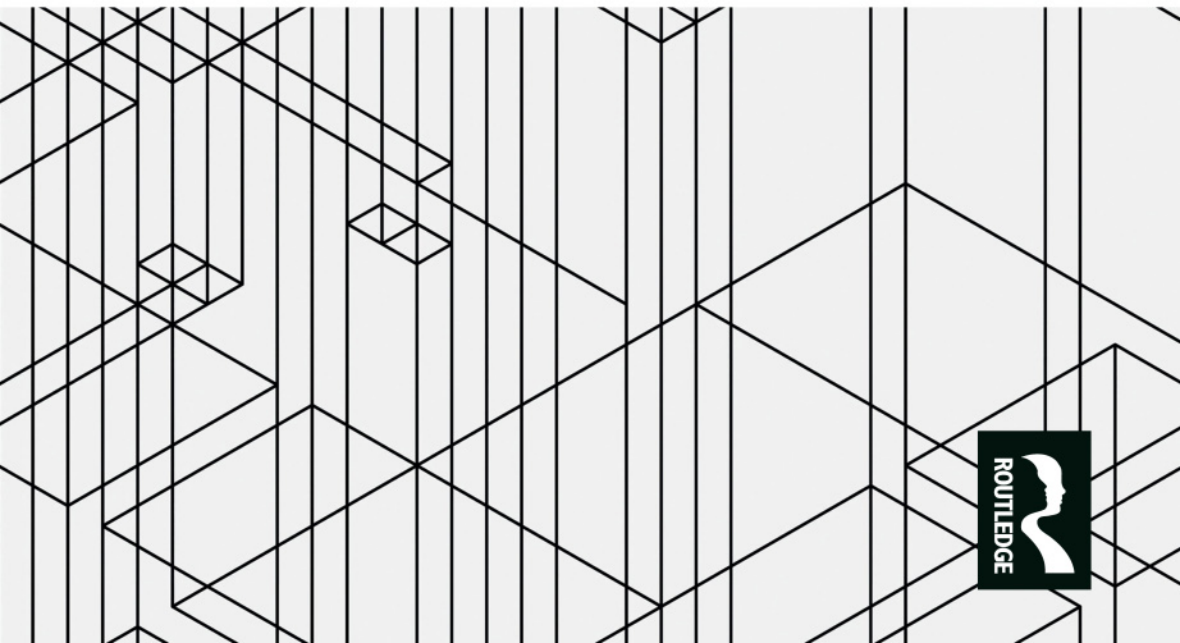


Routledge Studies in Surveillance

BIG DATA, SURVEILLANCE AND CRISIS MANAGEMENT

Edited by
Kees Boersma and Chiara Fonio



Big Data, Surveillance and Crisis Management represents an urgently needed and profoundly relevant contribution to the emerging body of scholarship about the role data and information technologies now play in how crises now unfold and how we respond to them. The voices in this volume are at the front lines of both practice and research in the multiple, interconnected fields that comprise the area of crisis informatics. We would do well to carefully and closely listen to what they are saying about how digital data is changing an already volatile world.

Dr. Nathaniel Raymond, *Director Signal Program on Human Security and Technology, Harvard Humanitarian Initiative (HHI) of the Harvard T.I. Chan School of Public Health*

Kees Boersma and Chiara Fonio undertake a major challenge in their edited book, *Big Data, Surveillance and Crisis Management*, in addressing both the positive and negative aspects of integrating the increasing amounts of digital data available from diverse sources into crisis management. On the positive side, advanced technologies provide access to many more sources of information about an emerging event in near-real time. On the negative side, this same access may compromise rights of privacy and lead to hasty judgments from unverified sources. The authors address this challenge of credibility by examining both the design and use of algorithms to mine the range of data sources and the uses of these methods of analysis in actual crisis situations. This problem warrants serious consideration, and the editors and their co-authors in this thoughtful book present a timely assessment.

Louise K. Comfort, *Professor of Public and International Affairs and Director, Center for Disaster Management, University of Pittsburgh*

This volume brings together two central concerns of our time – big data and crisis management – to provide us with crucial ways of thinking about our changing information environment. It provides a thoughtful and sophisticated exploration of both the potentials and pitfalls of data collection that will be of interest to a range of fields including data ethics, crisis management, and surveillance studies. The issues it explores are only likely to become more pressing with the passage of time, the development of the technology, and the direction in which the world seems to be headed.

Mark Andrejevic, *Professor of Media Studies Pomona College, Monash University*

This volume is essential reading for everybody engaged in the humanitarian sector. Building on the vast potential of new uses of information, social media and big data in humanitarian responses, the book systematically raises the pitfalls, dilemmas and ethical issues related to the use of big data in crisis response.

Dorothea Hilhorst, *Professor of Humanitarian Aid and Reconstruction at the International Institute of Social Studies of Erasmus University Rotterdam*

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Big Data, Surveillance and Crisis Management

Big data, surveillance, crisis management. Three largely different and richly researched fields, however, the interplay amongst these three domains is rarely addressed.

In this title, the link between these three fields is very much explored in a consequential order through a variety of contributions and series of unique and international case studies. Indeed, whilst considering crisis management as an 'umbrella term' that covers a number of crises and ways of managing them, the reader will also explore the collection of 'big data' by governmental crisis organisations. However, this volume also addresses the unintended consequences of using such data. In particular, through the lens of surveillance, one will also investigate how the use and abuse of big data can easily lead to monitoring and controlling the behaviour of people affected by crises. Thus, the reader is invited to join the authors in their debate of how big data in crisis management needs to be examined as a political process involving questions of power and transparency.

An enlightening and highly topical volume, *Big Data, Surveillance and Crisis Management* will appeal to postgraduate students and postdoctoral researchers interested in fields including Sociology and Surveillance Studies, Disaster and Crisis Management, Media Studies, Governmentality, Organisation Theory and Information Society Studies.

Kees Boersma is an Associate Professor in the Faculty of Social Sciences of the VU University, Amsterdam.

Chiara Fonio is currently working at the Joint Research Centre with a contract as CA (Contractual Agent).

Routledge Studies in Surveillance

Kirstie Ball, William Webster, Charles Raab
www.routledge.com/Routledge-Studies-in-Surveillance/book-series/RSSURV

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

Big Data, Surveillance and Crisis Management

Edited by Kees Boersma and Chiara Fonio

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2018
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
711 Third Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging in Publication Data
Names: Fonio, Chiara, author. | Boersma, Kees, author.
Title: Big data, surveillance and crisis management / Chiara Fonio and Kees Boersma.
Description: 1 Edition. | New York : Routledge, 2017. | Includes bibliographical references and index.
Identifiers: LCCN 2017009055| ISBN 9781138195431 (hardback) | ISBN 9781315638423 (eBook)
Subjects: LCSH: Crisis management–Case studies. | Internal security. | Information technology–Security measures.
Classification: LCC HD49 .F6596 2017 | DDC 363.32/8028557–dc23
LC record available at https://lccn.loc.gov/2017009055

ISBN: 978-1-138-19543-1 (hbk)
ISBN: 978-1-315-63842-3 (ebk)

Typeset in Times New Roman
by Wearset Ltd, Boldon, Tyne and Wear

Contents

Contributors

Kees Boersma is an Associate Professor at the Faculty of Social Sciences of the VU University Amsterdam, Department of Organization Sciences. His current research about Smart Disaster Governance is funded by NWO, the Dutch Science Foundation. In 2012 he was visiting scholar at the University of Illinois at Urbana/Champaign. From 2009 to 2013 he was MC-member in the EU COST Action Living in Surveillance Societies (www.liss-cost.eu/). He is the group leader of AREA: Amsterdam Research on Emergency Administration (www.area-vu.nl). In 2012 he co-edited the volume *Internet and Surveillance* (Routledge) with Christian Fuchs, Anders Albrechtslund and Marisol Sandoval. In 2014 he co-edited the volume *Histories of State Surveillance in Europe and Beyond* (Routledge), with Chiara Fonio, Rosamunde van Brakel and Pieter Wagenaar.

Alessandro Burato graduated in Philosophy from the Università Cattolica del Sacro Cuore di Milano, and earned a Master of Science in Risk Analysis at King's College London. Throughout all his course of studies he has been keen on risks and emergencies communication and management processes. He studied the use of media and the role of communication in emergency situations. He is senior researcher at ITSTIME (Italian Team for Security, Terroristic Issues and Managing Emergencies), a research group of the Sociology Department of Università Cattolica del Sacro Cuore. He is editor of *Countering Radicalisation and Violent Extremism among Youth to Prevent Terrorism* (NATO Science for Peace and Security Series) and author of a chapter of the same book titled 'Crisis Management and Violent Radicalization: The Neglected Role of Risk Communication'.

Monika Büscher is Senior Lecturer at the Centre for Mobilities Research at Lancaster University. She researches the digital dimensions of contemporary 'mobile lives' with a focus on IT ethics and crises. In 2011, she was awarded an honorary doctorate by Roskilde University, Denmark. She edits the book series Changing Mobilities with Peter Adey.

Baki Cakici is a postdoctoral researcher at the Department of Sociology at Goldsmiths, University of London. He is currently part of the European

Research Council (ERC) funded research project ARITHMUS. He holds a PhD in Computer and Systems Sciences from Stockholm University. His research interests include surveillance, classification and the politics of information and communication technologies. He is specifically interested in the role of algorithms and big data analytics in knowledge production. In his research, he draws on theories from science and technology studies, and surveillance studies.

Xavier L'Hoiry is a Lecturer in Criminology and Social Policy at the University of Sheffield. He holds a PhD in Criminology with an expertise in organised crime and policing. Since the completion of his doctoral studies, Xavier has worked on international research projects concerning surveillance and policing. In doing so, he has developed expertise in the ongoing development of surveillance technologies, their use in policing serious and organised crime and the subsequent impact upon democratic principles. The latter of these interests is focused specifically on the right of access to personal data and the impact on the concept of informational self-determination.

Rachel Finn is a Practice Manager at Trilateral Research, a multidisciplinary research services company. She manages projects and participates in research related to privacy, data protection and social impacts of current and emerging data technologies and practices, including issues relevant to big data, open data, open government, security technologies (especially drones) and standardisation. Rachel is a member of the Surveillance Studies Network and the Information Systems for Crisis Response and Management (ISCRAM) community. She has a PhD in Sociology from the University of Manchester. Her latest book is *Mobilising Data: Open Data and the Knowledge Society*.

Chiara Fonio (PhD in Sociology and Methodology of the Social Research) is a researcher in Sociology at the Catholic University of Milan. Her research interests range from the history of surveillance to the securitisation of mega-events and the impact of CCTV within urban contexts. She has been involved in several EU-funded research projects focused on surveillance and security. From 2009 to 2013 she was MC-member in the EU COST Action Living in Surveillance Societies (www.liss-cost.eu/). Recent publications: 'Surveillance, Repressions and the Welfare State: Aspects of Continuity and Discontinuity in Post-Fascist Italy' (with S. Agnoletto) in *Surveillance & Society*, 11(1–2), 2013; 'Surveillance under Mussolini's Regime' in *Surveillance & Society*, 9(1), 2011; 'The Silent Growth of Video Surveillance in Italy' in *Information Polity*, 16(4), 2011. In 2014 she co-edited the volume *Histories of State Surveillance in Europe and Beyond* (Routledge), with Kees Boersma, Rosamunde van Brakel and Pieter Wagenaar.

Martin French is an Assistant Professor with the Department of Sociology & Anthropology at Concordia University in Montreal, Canada. Martin's research examines the social dimensions of technology with an empirical

focus on information and communication technology (ICT). It emphasises the broader social and political contexts of ICT, focusing especially on risk, surveillance, privacy and social justice.

Henning Füller is Senior Lecturer at the Department of Geography, Humboldt-Universität zu Berlin. His research is concerned with the conceptual relations of power, space and security. His ongoing book project 'Geographies of Biosecurity' aims to understand the impacts of an emerging diseases worldview on the governing of cities and bodies. Research for this project has been done on epidemic control in Hong Kong after the SARS epidemic and on a system of syndromic surveillance in the US national capital region.

Gemma Galdon Clavell is a policy analyst working on surveillance, social, legal and ethical impacts of technology, smart cities, privacy, security policy, resilience and policing. She is a founding partner at Eticas Research & Consulting and a researcher at the Universitat de Barcelona's Sociology Department. She completed her PhD on surveillance, security and urban policy in early 2012 at the Universitat Autònoma de Barcelona, where she also received an MSc in Policy Management, and was later appointed Director of the Security Policy Programme at the Universitat Oberta de Catalunya (UOC). Previously, she worked at the Transnational Institute, the United Nations' Institute for Training and Research (UNITAR) and the Catalan Institute for Public Security. She teaches topics related to her research at several foreign universities, mainly in Latin America, and is a member of the IDRC-funded Latin American Surveillance Studies Network. Additionally, she is a member of the international advisory board of Privacy International and a regular analyst on TV, radio and print media. Her recent academic publications tackle issues related to the proliferation of surveillance in urban settings, urban security policy and community safety, security and mega-events, the relationship between privacy and technology and smart cities.

Muhammad Imran, PhD, is a scientist at Qatar Computing Research Institute. His research focuses on understanding the role of social networks during natural or man-made disasters by using big data analytics techniques such as data mining, machine learning, and deep neural networks. He is an active researcher with more than 40 publications in top-tier international conferences and journals. Among them two of his papers have received 'Best Paper Award'. He has served as PC of many major conferences (ISCRAM, SWDM, ICWSM, ICET) and has been serving as a track co-chair of the Social Media Studies track at the ISCRAM 2015–2017 conference.

Karolin Eva Kappler is a researcher at the Department of Diagnosis of Contemporary Society, Institute of Sociology, FernUniversität in Hagen (Germany). She holds a PhD in Sociology (2009, University of Barcelona, Spain) and Master's degree in Political Sciences (2003, Institut d'Études Politiques de Paris, France). Her research interests include big data, network

analysis, crisis management and social resilience. Current research projects: associated researcher at the EU-funded research project SUPER (Social Sensors for Security Assessments and Proactive Emergency Management, 2014–2017; http://super-fp7.eu/); researcher at the DFG-funded research project Taxonomies of the Self: The Emergence and Expansion of Calculative Practices of Self-inspection (2015–2018).

Xaroula (Charalampia) Kerasidou is a Research Associate at the Centre for Mobilities Research, Lancaster University. Her research interests lie within the field of feminist science and technology studies where she focuses on the material and semiotic practices of technoscience. Currently, she works on the EU FP7 funded project SecInCoRe (www.secincore.eu).

Charles Leleux is a Researcher with the Centre for Research into Information, Surveillance and Privacy (CRISP), Stirling Management School, University of Stirling (UK). He has worked on EU COST Action: Living in Surveillance Societies (LiSS) 2009–2013; EU FP7: Increasing Resilience in Surveillance Societies (IRISS) 2012–2015; EU FP7: Assessing Societal Impact of Security Research (ASSERT) 2013–2014, and is currently engaged on the ESRC-funded project: Smart Governance of Sustainable Cities (SmartGov) 2015–2019. Research interests include: smart cities; neighbourhood watch; workplace surveillance, and the sale of large datasets containing citizens' information.

Patrick Meier, PhD, is an internationally recognised thought leader on humanitarian technology. His new book, *Digital Humanitarians*, has been praised by Harvard, MIT, Stanford, Oxford, the UN, Red Cross and the World Bank. At present, Patrick serves as Executive Director of WeRobotics and consults for the World Bank, Red Cross, Facebook and Planet Labs. Patrick has a PhD from The Fletcher School, a Pre-Doctoral Fellowship from Stanford University and an MA from Columbia University. Patrick's influential and widely read blog iRevolutions has received close to two million hits.

Clive Norris is Professor of Sociology at the University of Sheffield. He is a world-renowned expert in the field of surveillance and privacy. For the last three decades, his research has involved documenting and analysing the increased use of surveillance in contemporary society. In particular it has focused on the police use of informants, CCTV surveillance and surveillance in criminal justice system. He has also played a central role in establishing Surveillance Studies as a specialist field of knowledge by building the infrastructure to create a viable sub-discipline. This has informed his work in setting up a specialist academic journal (*Surveillance and Society*), creating an academic community through the Surveillance Studies Network, hosting a biennial conference (held in Sheffield 2004, 2006, 2008), being awarded (with others) an ESRC seminar series, and participating in a range of international collaborations with academic and non-academic partners throughout the world.

Katrina Petersen is Research Associate at the Centre for Mobilities Research, Lancaster University. She works on the SecInCoRe project, concerned with the design of secure dynamic cloud concept for crisis management based on a pan-European disaster inventory. Her background is in science and technology studies, public engagement in museums and geology.

Uwe Vormbusch is Professor for the Diagnosis of Contemporary Society, Institute of Sociology, FernUniversität in Hagen (Germany). His main research interests include financial and economic sociology, calculation and society, and critical accounting studies. He is the main researcher of the research project 'Taxonomies of the Self: The Emergence and Expansion of Calculative Practices of Self-inspection' funded by the German Research Foundation (DFG) (2015–2018). He has completed several research projects in the field of economic sociology, calculation and valuation practices.

Kush Wadhwa is a Director at Trilateral Research. He leads teams that specialise in research and advisory services focused upon data sciences. His work in these areas, which have emerged as a dominant force for innovation, is complemented by his prior work in social science projects related to data protection and privacy, crisis management, and work in the private sector in technology development organisations. He has coordinated and participated in a number of European projects. He serves as an Associate Editor of the journal *Studies in Ethics, Law, and Technology*. Mr. Wadhwa holds an MBA from New York University.

Hayley Watson is a Practice Manager at Trilateral Research, a multidisciplinary research services company. Her expertise includes the role of technology including social media in relation to security, and she is interested in the use of ICT in crisis management. She has published peer-reviewed articles on citizen journalism in relation to security and social media and crisis management. She is actively involved in the ISCRAM community (Information Systems for Crisis Response and Management) and co-chairs the ELSI track on Ethical, Legal and Social Issues of IT supported emergency response. Hayley has a PhD in Sociology from the University of Kent.

C. William R. Webster is Professor of Public Policy and Management, University of Stirling (UK). He is a Director of the Centre for Research into Information, Surveillance and Privacy (CRISP), within Stirling Management School, and Chair of the Living in Surveillance Societies COST Action. Professor Webster was the 2016 NZ–UK Link Foundation Visiting Professor, based at the School of Government, Victoria University of Wellington. Research interests include: everyday surveillance practices, the governance and regulation of surveillance and governing in the information age. He is a recognised expert on Closed Circuit Television (CCTV) in public places and has played a lead role in a number of international research projects.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Chapter 1

Big data, surveillance and crisis management

Kees Boersma and Chiara Fonio

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] 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, analyze 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 these 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 analyze 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.

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 Vs" (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 consequences, 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 of maintaining 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 gap 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 efforts through, for instance, the generation of maps or the interpretation of large amounts of data (Mulder et al. 2016). Digital humanitarians – as they are labeled – 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 et al. 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 (Meijer 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 the challenges of working 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.

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 online 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" (Gandy 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 has become 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 define surveillance as an activity that involves "assorted forms of monitoring, typically for the ultimate purpose of intervening in the world" (2010, 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 decentralized and easily accessible, and individuals more easily traced. The internet has 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 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 behaviors and situations, crisis management practices do not have the primary goal of storing information for controlling behavior. 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 side 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 et al. 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 et al. 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 crisis (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 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 an 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 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 Chapters 5 and 6 in this book). On 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 US Federal Emergency Management Agency (FEMA) has a dedicated smartphone app "to crowdsource pictures during disasters" (Meier 2015, p. 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 side 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.

Structure and content of the book

We have divided the chapters of this volume into three parts: Part I addresses social media and crisis management, Part II looks at big data and health surveillance and Part III presents case studies on disasters, crisis and big data.

Part I 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 et al. present an in-depth discussion about social media and big data in the context of digital humanitarianism. They show how social media platforms such as Twitter and Facebook fostered the open environment and convenient ways to produce, share and consume information more quickly and easily than ever before. Recent years have witnessed a huge influx of information in the form of text, images, videos and 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 draw attention to 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 in their decision-making processes during crisis situations. However, there are numerous challenges in the use of social media data for crisis response. The authors elaborate on various challenges that formal disaster management agencies face to successfully filter, process and utilize social media data in 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 not necessary for the purpose of the needed analysis from being collected.

In Chapter 3, Rachel Finn et al. 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 organizations in this case study appears to mitigate many of those impacts. Specifically, humanitarian organizations recognize 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 provide new possibilities for emergency management – but also challenges. This increasing interest in 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 realized. The chapter tackles some of these challenges by reviewing both the state of the art of technological solutions and institutional programs leveraging the use of social media in crisis management. It summarizes 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 minimize societal risks in the design and implementation of participatory tools in the context of crisis management.

Part II is about big data and health surveillance. The developments in big data and crisis management in the context of health-related crises 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. Part II contains two chapters.

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 US 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 toward 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-centering attention and resources toward 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 III of this 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