Universitat Autònoma de Barcelona

Crowdsourcing Crisis Management Platforms: A Privacy and Data Protection Risk Assessment and Recommendations

Buddhadeb Halder

Final Examination 2017

Alma Mater Studiorum – Università di Bologna

in partnership with LAST-JD Consoritum

Università degli studi di Torino

Universitat Autonoma de Barcelona

Mykolas Romeris University

Tilburg University

and in cotutorship with the

University of Luxembourgh

PhD Programme in

Erasmus Mundus Joint International Doctoral Degree in Law, Science and Technology

Cycle 29 – a.y. 2013/14

Settore Concorsuale di afferenza: 12H3
Settore Scientifico disciplinare: IUS20

Crowdsourcing Crisis Management Platforms: A Privacy and Data Protection Risk Assessment and Recommendations

Submitted by: Buddhadeb Halder

The PhD Programme Coordinator

Supervisor

Antoni Roig Batalla

Year 2017

Universitat Autònoma
de Barcelona

Departament de Ciència Política i Dret Públic

CROWDSOURCING CRISIS MANAGEMENT PLATFORMS: A PRIVACY AND DATA PROTECTION RISK ASSESSMENT AND RECOMMENDATIONS

Dipositat a la Universitat Autònoma de Barcelona com a
requeriment per al grau de Doctor en Dret, Ciència i Tecnologia del PhD Programme in
Erasmus Mundus Joint International Doctoral Degree in Law, Science and Technology
Cycle 29 – a.y. 2013/14

Institut de Dret i Tecnoogia (IDT), Àrea de Filosofia i Teoria del Dret

per
Buddhadeb Halder
Bellaterra, Desembre 2016

Director:
Dr. Antoni Roig Batalla

Tutor:
Dr. Antoni Roig Batalla

Certifico que he llegit aquesta tesi, que és adequada i compleix tots els requeriments de qualitat per obtenir el grau de Doctor en Dret, Ciència i Tecnologia.

Bellaterra, Desembre 2016

_____

Dr. Antoni Roig Batalla
Director de la tesi

_____

Buddhadeb Halder
Doctorand

Tribunal:
Dr. Lorenzo Cotino Hueso
Dr. Tom van Engers
Dr. Jorge Olcina Cantos

Suplents:
Dr. Agustí Cerrillo
Dr. Anna Ribas Palom
Dr. Miquel Peguera Poch

Thesis Contribution to the Field:

1. Various roles in crowdsourcing process have been identified.
2. Identified various risks and presented an analysis for 'risk-informed decision making (RIDM)' process in form of a general framework for crowdsourcing crisis management.
3. A concrete Privacy and Data Protection Risk Assessment and Recommendations for disaster management platforms can offer valuable recommendations for law makers and other stakeholders like disaster management communities and digital volunteers which are presently missing from type 3 or 4 regulations.
4. This Privacy and Data Protection Risk Assessment and Recommendations will certainly fulfil two *i.e.* a) how the Priority Action 1 of the Sendai Framework for Disaster Risk Reduction 2015-2030 can be enhanced more by highlighting the importance of 'data protection' in using crowdsourcing process in any disaster / crisis management event and b) how to strengthen disaster risk governance to manage disaster risk as described in the Priority Action 2 of the Disaster Risk Reduction Sendai Framework.

Table of Content

IV. Ethical and Legal Concerns of Crisis Management Platforms **72**
4.1 Risks associated with Crisis Crowdsourcing 72
4.2 Tasks of Online Volunteers and Risks 75
4.3 Data retrieval and selection concerns 76

Crowdsourcing Crisis Management Platforms: A Privacy and Data Protection Risk Assessment and Recommendations

Buddhadeb Halder
The Universitat Autònoma de Barcelona, Spain.
{buddhadeb.halder@unibo.it}

Abstract. Over the last few years, crowdsourcing have expanded rapidly allowing citizens to connect with each other, governments to connect with common mass, to coordinate disaster response work, to map political conflicts, acquiring information quickly and participating in issues that affect day-to- day life of citizens. As emerging tools and technologies offer huge potential to response quickly and on time during crisis, crisis responders do take support from these tools and techniques. The 'Guiding Principles' of the Sendai Framework for Disaster Risk Reduction 2015-2030 identifies that 'disaster risk reduction requires a multi-hazard approach and inclusive risk-informed decision-making (RIDM) based on the open exchange and dissemination of disaggregated data, including by sex, age and disability, as well as on easily accessible, up-to-date, comprehensible, science-based, non-sensitive risk information, complemented by traditional knowledge. Addressing the 'Priority Action' 1 & 2, this PhD research aims to identify various risks and present recommendations for 'RIDM Process' in form of a general Privacy and Data Protection Risk Assessment and Recommendations for crowdsourcing crisis management. It includes legal, ethical and technical recommendations.

Keywords: Crowdsourcing, Disaster Management, ICT, Privacy Analysis, Security, Data Protection, Recommendations.

I. Introduction

1.1 Definitions, forms, methods and different domains of crowdsourcing

Over the last few years, the term “crowdsourcing” has become really well known to the interdisciplinary research community. What is “crowdsourcing’ all about? The term "crowdsourcing" is the combination of two words “crowd” and “outsourcing” coined by Jeff Howe and published in a June 2006 *Wired* magazine article “*The Rise of Crowdsourcing*”[1]. Jeff Howe describes that ‘crowdsourcing’ is the combination of ‘crowd’ and ‘outsourcing’. He defines crowdsourcing as,

> [....] the act of taking a job traditionally performed by a designated agent (usually an employee) and outsourcing it to an undefined, generally large group of people in the form of an open call’ [2].

There are various crowdsourcing definitions found in the literature. For the first time, the *Oxford English Dictionary*, in its June 2013 edition included the word ‘crowdsourcing’ and defines it as ‘Practice of obtaining information or sources by soliciting input from a large number of people’. Several authors and experts e.g. Howe, Brabham, Kleeman et al., Grier, Vukovic, and Whitla have defined the term ‘crowdsourcing’ more than once in different articles published between 2006 and 2011 [3].

In De Vreede et al. (2013), Triparna de Vreede and others have rightly identified some confusions in identifying which applications are

crowdsourcing and which are not[1]; whether Web 2.0 and other social networking are crowdsourcing platforms and whether 'user innovation' is corwdsourcing. However, Peter van der Windt describes 'user innovation' as 'Crowdseeding' and not 'Crowdsourcing' [4].

Jeff Howe- the expert who coined the term 'crowdsourcing' has pointed out some possible categories of web-based crowdsourcing that can be used well in the business world. Some of these crowdsourcing initiatives include crowdfunding, wisdom of the crowd, creative crowdsourcing, crowdvoting, microwork, and inducement prize contests.[2] However, these categories may not be the complete list of different types of crowdsourcing [5]. To perform different types of tasks, people use other ways of crowdsouring as well. Henk van Ess explains,

> [....]Crowdsourcing is exploiting nice people…the crowdsourced problem can be huge (epic tasks like finding alien life or mapping earthquake zones) or very small ('where can I skate safely?'). Some examples of successful crowdsourcing themes are problems that bug people, things that make people feel good about themselves, projects that tap into niche knowledge of proud experts, subjects that people find sympathetic or any form of injustice" [6].

[1] For example, Huberman et al. (2009 apud De Vreede et al., 2013) consider YouTube as crowdsourcing, while Kleeman et al. (2008, De Vreede et al., 2013) do not consider YouTube as crowdsourcing platform.

[2] http://en.wikipedia.org/wiki/Crowdsourcing

After analysing 40 different definitions, and after considering some specific aspects of the crowd, the initiator and the underlying process Estelles-Arolas & Gonzalez-Ladron-de-Guevara have proposed an integrated definition of crowdsourcing.

> "Crowdsourcing is a type of participative online activity in which an individual, an institution, a non-profit organization, or company proposes to a group of individuals of varying knowledge, heterogeneity, and number, via a flexible open call, the voluntary undertaking of a task. The undertaking of the task, of variable complexity and modularity, and in which the crowd should participate bringing their work, money, knowledge and/or experience, always entails mutual benefit. The user will receive the satisfaction of a given type of need, be it economic, social recognition, self-esteem, or the development of individual skills, while the crowdsourcer will obtain and utilize to their advantage that what the user has brought to the venture, whose form will depend on the type of activity undertaken" [3].

This definition covers all about 'crowdsourcing'. However, it is too long. The definition has also a limitation. Crowdsourcing is not just an 'online activity' but an offline activity as well. Thus, very simply the term 'crowdsourcing' could be defined as the process of finding needed information and service for a common goal from a large number of people.

1.2 Forms, methods and different domains of crowdsourcing

In his book 'Crowdsourcing for Dummies', David Alan Grier identifies five major forms of crowdsourcing i.e. Crowdcontests, Macrotasks, Microtasks, Crowdfunding, Self-organised Crowds. Each form involves a crowdsourcer or manager, a crowdmarket and a crowd of people. By choosing the right form of crowdsourcing, someone can manage huge jobs with thousands of workers or do small jobs that require just a single person. Someone can create jobs that he can carefully monitor and control, or he can let the crowd organise itself and decide how it should do the work [7]. Daren C. Brabham, in his book, Crowdsourcing, published in 2013 puts forth a problem-based typology of crowdsourcing approaches [8]. These four problem-based typologies are i). Knowledge Discovery and Management; ii). Distributed Human Intelligence Tasking; iii). Broadcast Search and iv). Peer-Vetted Creative Production.

Marta Poblet, Esteban García-Cuesta, and Pompeu Casanovas proposed four different types of 'crowdsourcing roles' based on two variables:[3]

a. low/high involvement of crowdsourced agents on processing the data and

b. passive/active participation of crowdsourced agents.

They have identified four categories i.e. Crowds as sensors, Crowds as social computers, Crowds as reporters and Crowds as microtaskers [9].

[3]They have proposed in their paper titled Crowdsourcing Tools for Disaster Management: A Review of Platforms and Methods. The article has been shared with the author in October 2013.

As the definition of crowdsourcing by Jeff Howe [1] captures the most important characteristics of crowdsourcing i.e. a crowdsourcing initiative should have the following three elements: (1) Users are producers, not only consumers; (2) The number of participants is undefined and (3) Users' contributions are towards completing a specific task. De Vreede et al. (2013) differentiate three sub-crowdsourcing models - virtual labor marketplace, closed collaboration, and open collaboration. After analyzing several definitions of crowdsourcing, Hetmank has identified four components (i.e. user management, task management, contribution management, and workflow management) of crowdscourcing [10]. Every crowdsourcing component has several functions like register user, evaluate user, design task, enable coordination etc. Thus, experts have proposed different types of crowdsourcing. However, based on the intention of the crowdsourcing coordinator, this research proposes a further division of crowdsourcing:

i) Crowdsourcing for Crisis Response Management: (Natural crisis / Man-made crisis);
ii) Crowdsourcing for Public Governance;
iii) Crowdsourcing for Business;
iv) Crowdsourcing for Innovation / Contest;
v) Crowdsourcing for Opinion gathering i.e. Opinion poll etc.;
vi) Crowdsourcing for Fund Collection i.e. Crowdfunding and
vii) Crowdsourcing for general purpose.

The use of crowdsourcing in different domains not only makes it possible to mine, aggregate and classify data but also helps in preparedness to face a particular situation, response during the situation and recovery after the situation. Crowdsourcing initiators can connect individuals and communities to gather data or to complete one or a set of easy tasks, such as measurements, identifying disaster prone areas or to guide someone who is in need etc. Crowdsourcing process allows individuals and organizations take part in several types of initiatives. Out of different crowdsourcing domains (e.g. art, business, political, scientific research, governance, health service, software development, and natural disaster related etc.), contributors to the political crowdsourcing initiatives are most vulnerable to the security and privacy threat. Crowdsourcing platforms allow common citizens and organizations to install, deploy, and manage crowdsourcing platforms in response to social issue, health issue and sudden outburst emergencies ranging from natural disasters, to the political conflict in any geographical region. They can also communicate with other crowdsourcing initiators with whom they can share different outcomes on similar issues. Another option can also work the other way round: experts can contribute their expertise to a particular problem.

To further improve the understanding of crowdsourcing, the attention has been drawn on some main domains of crowdsourcing. As a result from the literature review, the present research identifies four main areas of crowdsourcing:

i. Art (Design competition, literature competition etc);
ii. Science (Scientific Innovation);

iii. Finance (Crowdfunding for social causes, business / investment) and

iv. Social science (Opinion gathering, Opinion Poll etc),

It is to be noted that every main area has several sub-areas or sub-domains e.g. design / logo contest, scientific innovation, crowd-investment, crowdfunding, crisis response etc.

In this research a thorough analysis has been carried out on -

i). Seventeen crowdsourcing communities, tools and platforms[4] that contributes to the crisis response management work;

ii). Three crowdsourcing innovation challenges platforms[5] that are being used to find innovative ideas or develop innovative tools to tackle different social issues or empower the mankind and lastly

iii). Four crowdsourcing platforms used for Miscellaneous Purposes[6].

Different types of crowdsourcing have expanded rapidly allowing citizens to connect with each other, governments to connect with common mass, acquiring information quickly and participating in issues that affect citizens. The extensiveness and increasing access to the communication technologies and the growing interest in engaging

[4] Ushahidi, SwiftRiver, Crowdmap, Eden–Sahana, PyBossa, CrisisTracker, OpenIR, ArcGIS, Recovers, PADDDtracker.org, Google Crisis Map, GeoChat, Souktel, InaSAFE, Geofeedia, Geo-pictures and CrisisCommons.
[5] Knight Foundations Challenges; MIT IDEAS Global Challenge and Mass Challenge
[6] InnoCentive; Innoget; Inpama and SolutionXchange.

common people i.e. crowd to find innovative solutions to public problems have inspired governments, aid agencies, other organisations and networks to use crowdsourcing processes for crisis management [11].

Several crowdsourcing initiatives across various fields such as art [12], business [13], governance [14], journalism [15] and medicine [16] have increased the use of crowdsourcing platforms and the positive development of crowdsourcing help common people to become more active and informed citizens. Crowdsourcing methods provide a low cost and scalable way to access ideas that might be difficult or expensive to obtain internally [17]. There are several crowdsourcing platforms available and usually they are open sourced digital platforms. With the help of those platforms governments, crisis response teams, NGOs, business organisations and other individuals can collect data- through the information that the 'crowd' i.e. common mass share- and use those data to develop new policies, innovative idea for new products, help victims of natural calamities to find shelters, medicines and other emergency needs, solve minor technical problems, send collective voice to the authority etc.

Crowdsourcing platforms allow citizens to connect with each other, governments to connect with common mass, humanitarian workers to coordinate disaster response work promptly, to map political conflicts, acquiring information quickly and participating in issues that affect day-to- day life of citizens. However, in crowdsourcing,

important concerns arise from data quality and accuracy, privacy, security, and data protection points of view.

On this background, we will identify possible ways to overcome these challenges in crowdsourcing crisis management.

1.3 Scope

We wanted to offer Privacy and Data Protection Risk Assessment and Recommendations for disaster management platforms based on, or using, crowdsourcing. The existing international disaster regulations do not provide some general principles that can guide current crisis management platforms in protecting users' data efficiently. Various, national, regional and international data protection principles coming from national or regional data protection regulations can also provide worthy indications for disaster management communities and response teams. Following the World Disaster Reduction Conference in 2005 the United Nations General Assembly endorsed the Hyogo Framework for Action (HFA1) (UNGA Resolution A/RES/60/195). The same was replaced by the Sendai Framework for Disaster Risk Reduction (2015-2030) (HFA2) in 2015. Thus, the latest one i.e. Sendai Framework will be the starting point of our present work.

1.4 Delimiting the Field

1.4.1 Crisis Management Platforms

Crisis, disaster or emergency management includes different stages like initial planning, preparedness and warning, the detection of a crisis event and its impact, and the response, recovery and mitigation.

Crisis management is so complex that a growing set of Information and Communication Technology (ICT) is needed. Concretely, a collaborative technology like social networking platforms, mobile devices with integrated cameras, location-aware services, multi-touch surfaces, web-based systems and crowdsourcing systems can be envisioned for this purpose.

1.4.2 Disaster Management Stages and Various Roles

The role of the digital volunteers is evolving from a passive source of raw data to a more proactive context builder and even an expert knowledge source for decision support tools trained by volunteers. During this digital era, various crisis management stages have different roles that can be identified as follows:

A. Retrieval and Selection

Digital volunteers help in aggregating relevant data from different sources. One of the main functions of various online platforms is to retrieve information. However, more data does not necessarily mean better information. Data relevance and accuracy are indeed crucial to add value to disaster management using crowdsourcing processes. Different strategies for obtaining accurate data like collective task-solving from online communities, crisis mapping and even selection by data analytics with social network data mining, user ranking, semi-supervised content classification and sensors etc. are being implemented.

B. Situational Awareness

Communities of trusted volunteers can be effective support teams to discover and select relevant information and data. Most of the virtual volunteers become active during the crisis event. They search and filter relevant information in social media and in the news, and receive various indications from different emergency response teams.

C. Decision Support Systems

Organizations like the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) and other traditional organizations submit requests and rely on digital volunteer groups. For example, the Digital Humanitarian Network (DHN) has been created to organisations like OCHA and other international or regional organisations. These digital volunteer groups have various solution teams with the relevant volunteer members within the volunteer communities. These core solution support teams are strong help in the decision making process during crisis events. However, the use of automatic tools in decision making is being increased as we move forward. This also helps crisis response team enormously. Thus, retrieval and context enrichment is now complemented by different predictive codes and decision support tools.

During the early days of digital crowdsourcing, various crisis management platforms used digital volunteers mainly for retrieving, validating and classifying information. Now volunteers are human sensors and they get help from artificial intelligence and machine learning technologies. Post disaster events' data are reused to enhance

the predictive capabilities for future crisis management decision-support tools.

1.5 State-of-the-Art

The explosive growth of information technologies across the world has given enormous power to the hands of common people. Though, different positive aspects of crowdsourcing have already been recognized, serious concerns have also been raised in terms of privacy, security and personal data protection in using crowdsourcing during any crisis events. Thus, a research has been conducted on numbers of crowdsourcing crisis management platforms to understand some ethical and legal concerns in crowdsourcing crisis informatics.

More than 80 hazard and risk modelling software packages are available for flood, tsunami, cyclone and earthquake[7]. OpenQuake[8], for instance, targets highly advanced users; CAPRA, on the other hand, is a multi-hazard risk platform for non-specialists who want to interact with data sets produced by experts and volunteers like as InaSAFE. Open source geospatial tools, such as QGIS and GeoNode, are also valuable tools for understanding national and subnational risks.

1.5.1 Disaster Management Platforms

Numbers of crowdsourcing tools and platforms[9] were investigated to

[7] Global Facility for Disaster Reduction and Recovery, 2014a, Understanding Risk: The Evolution of Disaster Risk Assessment since 2005, Background Paper prepared for the 2015 Global Assessment Report on Disaster Risk Reduction. Geneva, Switzerland: UNISDR.

[8] Tool developed under the Global Earthquake Model Foundation.

[9] Crowdsourcing tools and platforms are: Ushahidhi, MicroMappers, Digital Humanitarian Network, PyBossa; CrisisTracker, OpenIR; ArcGIS; Recovers; PADDDtracker.org; Google Crisis Map; GeoChat, Souktel; InaSAF; Geofeedia; Geo-pictures; CrisisCommons.

understand the privacy, security and data protection issues associated with crowdsourcing crisis management platforms. Finally, four different platforms i.e. Ushahidhi, MicroMappers, Digital Humanitarian Network and Google Crisis Map were intensively investigated.

A. Ushahidi

Ushahidi (USH) is considered as the pioneer and innovative crowdsourcing platform that paved the way for using ICT based crowdsourcing in crisis management works. Ushahidi first started its ground-breaking work with the deployment of an innovative crowdsourcing platform to monitor incidents of post-election violence in Kenya in 2008 and peace efforts throughout the country based on reports submitted via the web and mobile phones. Platforms like Ushahidi and its' sister platforms like SwiftRiver and Crowdmap offer volunteers and other users to create "reports" from social media updates, direct information and conventional media activities accompanied by GPS location for the report when available and possible. In Ushahidi, volunteers and users can track his reports on the map and over time, filter his data by time, and see when things happened and where. This platform allows you to easily collect information via text messages, email, twitter and web-forms.

Ushahidi has recently developed another 'check-in tool' called 'Ping' that would support crisis management works using crowdsourcing by adding users' contacts to a group helping anyone to 'Ping multiple people with the push of a button'. This tool can 'create and store contacts with multiple numbers and email addresses for each for multiple points of contact'.

B. Digital Humanitarian Network (DHN)

There are numbers of networks that voluntarily works to address different crisis situations. The Digital Humanitarian Network (DHNetwork) is the network of Volunteer & Technical Communities of its' kind to leverage digital networks in support of humanitarian response. The aim of this platform is to "provide an interface between formal, professional humanitarian organizations and informal yet skilled-and- agile volunteer & technical networks". DHN use different tools to address crisis issues. Some examples are the Humanitarian UAV Network (UAViators) or Planetary Response Network for crowdsourcing satellite imagery analysis for humanitarian response. Humanity Road has also worked under the Digital Humanitarian Network's Solution Team to build up a Situation Report for OCHA's team in the Philippines. Indeed, some DHNetwork Coordinators are in charge of contacting volunteers and technical teams' members of Digital Humanitarians to build a Solution Team for particular request. DHN uses different tools while working towards managing a crisis. For example, DHN uses 'Verily' that collects crowdsourced evidence, and provide important information for crisis responses. In the present 'Disinformation Age', finding the truth in the huge amount of contradictory and confusing information is becoming increasingly difficult for crisis responders. Verily is an experimental web tool designed to rapidly share verified information during humanitarian disasters, it uses a time-critical crowdsourcing process to verify information during major disasters on behalf of humanitarian

organizations and media groups.

C. MicroMappers

The platform 'MicroMappers'(MM) has been identified for the research as it has started AI (Artificial Intelligence) for the first time to select data and information provided by users. It is a collection of websites or Clickers (beta version) and each clicker or volunteer can easily tag different types of information. There are several categories of digital volunteers associated with MicroMappers[10]. 'Text Clickers' for instance identify the relevance of Tweets during an emergency or disaster. 'Image Clickers' are volunteers who rate the damage by looking at images. These volunteers check, verify and rate different crowdsourced information and data and then the platform passes that information to 'Geo Clickers' who put those tweets, pictures and videos on the map. In the recent earthquake in Nepal in May 2015, over 2800 volunteers from all over the world reviewed tweets and images to support humanitarians with information insights. These 'clicks' and 'selections' of texts by volunteers produced a highly accurate dataset about the earthquakes in Nepal that was shared and incorporated into the damage assessment and decision-making processes. At the end of the process, some empowered group of volunteers insert the obtained information on a map, where the type and seriousness of incidents are reported. At this stage the support

[10] Volunteer categories are 1. 'Text Clickers' for Tweets, 2.'Image Clickers' for Pictures, 3.'Aerial Clickers' for Aerial Pictures, 4. 'Video Clickers' to tag videos and finally, 5. 'Geo Clickers' to map tweets, pictures and videos. There will be another category called 'Translate Clickers' to crowdsource the translation of tweets very soon.

teams and the decision-makers work together to accelerate the crisis management. MicroMappers uses artificial intelligence. For example, MicroMappers is using AIDR (Artificial Intelligence for Disaster Response) - an artificial intelligence engine developed to power consumer applications like MicroMappers. This platform permits humans and machines to work together to apply human intelligence to large-scale data at high speed. Meier has identified that 'the free and open source Artificial Intelligence for Disaster Response platform leverages machine learning to automatically identify informative content on Twitter during disasters' [18].

D. Google Crisis Map

Google Crisis Map (GCM) has been selected for this research to identify, having all latest technological facilities, how does it care about privacy, security and data protection issues. Google has been responding to natural disasters since Hurricane Katrina in 2005 by making information such as storm paths, shelter locations, emergency numbers, and donation opportunities easily accessible. Only after mid 2012 Google has started creating Crisis Maps. Google Crisis Map is a collection of national and regional-scale layers related to weather, hazards, and emergency preparedness and response, mostly for the US. Google has developed several tools to help responders to achieve their goals in crisis situations. For example, Google Public Alerts, Google Person Finder, Google Maps Engine Lite, Google Earth etc. First responders can use these tools to streamline internal operations and get information to the public as quickly, broadly, and effectively as

possible.

1.5.2 Risks in Crowdsourcing Processes

From the literature review, we have identified some risks associated with crowdsourcing process:

A. Security breach due to system malfunction or insecure data transmission

B. Personal Information Disclosure, location data management, sensitive data (health, political opinion…), quality of data and discrimination

C. Lack of coordination

D. False positives, automatic decision-making

A. Data Protection Risks in different stages

Data Retrieval and Selection

Collection and filtering can be fulfilled by digital volunteers, achieving collective task solving and crisis mapping. It can also be implemented using data analytics, like social network analysis, user ranking, machine learning, sensors and ultimate meta-data crisis mapping. Security and privacy will be the risks endangered by data retrieval and selection.

Situational Awareness

On the other hand, situational awareness is offered by human sensors, support teams and humanitarian networks. Digital volunteers are more organized than in the past and these networks trigger new risks. Coordination between response teams and digital volunteers, and also ad hoc solution teams created by digital communities are the risks

related to situational awareness tasks.

Decision Support Systems

The last group of tasks involves decision-making support: OCHA and the Digital Humanitarian Network coordinate to offer decision support, but we will consider it as a coordination risk. On the contrary, simulation, geomatics and emotion classification will soon be a decision support tool for response teams. It is at this stage when false positives might be more dangerous.

1.5.3 Disaster Management Frameworks

The Hyogo Framework for Action (2005-2015)

The Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters (HFA) was developed and agreed on with the many partners needed to reduce disaster risk - governments, international agencies, disaster experts and many others - bringing them into a common system of coordination[11]. The Hyogo Framework outlines five priorities for action, and offers guiding principles and practical means for achieving disaster resilience. Its goal was to significantly reduce disaster losses by 2015 by building the resilience of nations and communities to disasters. This means reducing loss of lives and social, economic, and environmental assets when hazards strike.

According to these five priorities action,

[11] The Hyogo Framework was adopted by the UN General Assembly in the Resolution A/RES/60/195 following the 2005 World Disaster Reduction Conference.

"Countries that develop policy, legislative and institutional frameworks for disaster risk reduction and that are able to develop and track progress through specific and measurable indicators have greater capacity to manage risks and to achieve widespread consensus for, engagement in and compliance with disaster risk reduction measures across all sectors of society.

The starting point for reducing disaster risk and for promoting a culture of disaster resilience lies in the knowledge of the hazards and the physical, social, economic and environmental vulnerabilities to disasters that most societies face, and of the ways in which hazards and vulnerabilities are changing in the short and long term, followed by action taken on the basis of that knowledge.

Disasters can be substantially reduced if people are well informed and motivated towards a culture of disaster prevention and resilience, which in turn requires the collection, compilation and dissemination of relevant knowledge and information on hazards, vulnerabilities and capacities.

Disaster risks related to changing social, economic, environmental conditions and land use, and the impact of hazards associated with geological events, weather, water, climate variability and climate change, are addressed in sector development planning and programmes as well as in post-disaster situations.

At times of disaster, impacts and losses can be substantially reduced if authorities, individuals and communities in hazard-prone areas are well prepared and ready to act and are equipped with the knowledge and capacities for effective disaster management.'

Though, the Hyogo Framework was a 10-year plan to make the world safer from natural hazards that was endorsed by the United Nations General Assembly. Under the Priorities Action 5, this framework advised for 'strengthening policy, technical and institutional capacities in regional, national and local disaster management, including those related to technology, training, and human and material resources'. Also it suggested to 'promote and support dialogue, exchange of information and coordination among early warning, disaster risk reduction, disaster response, development and other relevant agencies and institutions at all levels, with the aim of fostering a holistic approach towards disaster risk reduction'. Most importantly, it mentioned about 'developing coordinated regional approaches, and create or upgrade regional policies, operational mechanisms, plans and communication systems to prepare for and ensure rapid and effective disaster response in situations that exceed national coping capacities'. Also advised to promote the establishment to support response, recovery and preparedness measures and to develop specific mechanisms to engage the active participation and ownership of relevant stakeholders, including communities, in disaster risk reduction, in particular building on the spirit of volunteerism.'

This framework also suggested that the international

organizations, including organizations of the United Nations system are called upon to make links with 'existing networks and platforms, cooperate to support globally consistent data collection and forecasting on natural hazards, vulnerabilities and risks and disaster impacts at all scales. These initiatives should include the development of standards, the maintenance of databases, the development of indicators and indices, support to early warning systems, the full and open exchange of data and the use of in situ and remotely sensed observations'.

However, this framework does not highlight anything about the privacy, online security and data protection during the emergency.

Sendai Framework for Disaster Risk Reduction 2015-2030 (HFA 2)

The Hyogo Framework was replaced by the Sendai Framework for Disaster Risk Reduction 2015-2030 (HFA2). The Third United Nations World Conference in Sendai, Japan, on March 18, 2015 adopted The Sendai Framework for Disaster Risk Reduction 2015-2030[12], also known as HFA 2. The Sendai Framework for Disaster Risk Reduction 2015-2030 did not talk on the potential risks of using emerging ICTs and crowdsourcing in disaster management [19]. However, the United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER) in a report on Crowdsource Mapping for Disaster Risk Management and Emergency Response developed during the International Expert

[12] It replaces the Hyogo Framework for Action (HFA) 2005-2015: Building the Resilience of Nations and Communities to Disasters. It is also known as HFA 2. United Nations International Strategy for Disaster Risk Reduction (UNISDR) has been tasked to review the Sendai Framework.

Meeting in February 2013 discussed about the use of crowdsourcing, issues and potential steps to take to deal with some existing issues [20].

The use of crowdsourcing in crisis governance has grown exponentially across the planet. It has been identified that crowdsourcing approaches like the Distributed Human Intelligence Tasking, using Machine Learning and Artificial Intelligence to gather and analyse data and a combined approach to both machine learning and human volunteers' support in crisis governance decision–making are three main approaches for crisis governance [11].

This framework, like the Hyogo Framework, HFA (2005-2015), helps raising institutional awareness and local and global coordination with stakeholders. Governments lead the regulatory and coordination role, but also need to involve people, volunteers and online disaster communities in the design and implementation of policies and standards. The Sendai Framework applies to the risk of "disasters caused by natural or man-made hazards, as well as related environmental, technical and biological hazards and risks"[13]. The goal to pursue is to "prevent new and reduce existing disaster risk through the implementation of integrated and inclusive economic, structural, legal, (…), technological, political and institutional measures". One of its global targets is to increase disaster risk information and assessments to people by 2030[14].

Some Sendai principles are directly related to crowdsourcing disaster

[13] Sendai Framework, art.15.
[14] Sendai Framework, art.18 (g).

management like empowerment participation, and the "improvement of organized voluntary work of citizens"[15]; also, crucial the reference to "disaggregated data" and "non-sensitive risk information"[16]. To achieve understanding of disaster risks, the Sendai Framework suggests developing "location-based disaster risk information, including risk maps, to decision makers, the general public and communities at risk of exposure to disaster in an appropriate format by using, as applicable, geospatial information technology"[17]. Governments should in general use "information and communications technology innovations to enhance measurement tools and the collection, analysis and dissemination of data"[18]. Community-based and non-governmental organizations are also in charge to disseminate disaster risk information[19]. At a global or regional level, the United Nations Office for Disaster Risk Reduction coordinates existing networks and scientific research institutions in order to strengthen disaster risk governance to manage disaster risk[20].

Moreover, sectoral laws and regulations on land use, urban planning, building codes, environment and resource management and health and safety standards need "to ensure an adequate focus on disaster risk management"[21]. The role of stakeholders is crucial: "Civil society, volunteers, organized voluntary work organizations and community-

[15] Sendai Framework, art.19 (d).
[16] Sendai Framework, art.19 (g) and art.24 (e).
[17] Sendai Framework, art.24 (c).
[18] Sendai Framework, art.24 (f).
[19] Sendai Framework, art.24 (o).
[20] Sendai Framework, art.25 (g) and art.26.
[21] Sendai Framework, art.27 (d).

based organizations [have] to participate, in collaboration with public institutions, to, inter alia, provide specific knowledge and pragmatic guidance in the context of the development and implementation of normative frameworks, standards and plans for disaster risk reduction"[22]. One way of achieving this goal is "to promote the use and expansion of thematic platforms of cooperation, such as global technology pools and global systems to share know-how, innovation and research and ensure access to technology and information on disaster risk reduction"[23]. To sum up, Priority 1, *i.e.* "Understanding disaster risk", and Priority 2, "Strengthening disaster risk governance to manage disaster risk" are directly related to crowdsourcing crisis management[24]. The 'Guiding Principles' of the Sendai Framework for Disaster Risk Reduction 2015-2030 identifies that 'disaster risk reduction requires a multi-hazard approach and inclusive 'risk-informed decision-making'[25] based on the open exchange and dissemination of

[22] Sendai Framework, art.36 (a).
[23] Sendai Framework, art.47 (c).
[24] Chart of the Sendai Framework for Disaster Risk Reduction 2015-2030, Priorities for Action, Priority 1, Understanding disaster risk; Priority 2, Strengthening disaster risk governance to manage disaster risk; Priority 3, Investing in disaster risk reduction for resilience; and Priority 4, Enhancing disaster preparedness for effective response, and to <Build Back Better> in recovery, rehabilitation and reconstruction.
[25] Risk-informed decision-making (RIDM) is a deliberative process that uses a set of performance measures, together with other considerations, to "inform" decision-making. The RIDM process acknowledges that human judgment has a relevant role in decisions, and that technical information cannot be the unique basis for decision -making. This is because of inevitable gaps in the technical information, and also because decision-making is an intrinsically subjective, value - based task. In tackling complex decision -making problems involving multiple, competing objectives, the cumulative knowledge provided by experienced personnel is essential for integrating technical and nontechnical elements to produce dependable decisions. (Source: NASA (2010).Risk-informed decision making handbook (NASA/SP-2010-576). Technical Report, NASA.)

disaggregated data, including by sex, age and disability, as well as on easily accessible, up-to-date, comprehensible, science-based, non-sensitive risk information, complemented by traditional knowledge.'[26]

In the 'Priority Action' 1: Understanding Disaster Risk' under the 'Priorities of Action', the Sendai Framework mentions, 'to promote the collection, analysis, management and use of relevant data and practical information and ensure its dissemination, taking into account the needs of different categories of users, as appropriate.'[27]

Most importantly, in the 'Priority 2: Strengthening disaster risk governance to manage disaster risk', the Sendai Framework mentions, 'to assign, as appropriate, clear roles and tasks to community representatives within disaster risk management institutions and processes and decision-making through relevant legal frameworks, and undertake comprehensive public and community consultations during the development of such laws and regulations to support their implementation.'[28]

Addressing the 'Priority Action' 1 & 2, we aim to identify various risks and present recommendations for 'risk-informed decision-making (RIDM)' process in form of a general Privacy and Data Protection Risk Assessment and Recommendations for crowdsourcing crisis management. We find assessing privacy and data protection risks and offering recommendations for crowdsourcing crisis management platforms

would be the most important contribution as the Sendai Framework has identified.

Thus, the proposed privacy and data protection risk assessment and recommendations will certainly fulfil some of the expectations highlighted under the Sendai Framework and it will also address some risks in using crowdsurcing for crisis management. Consequently, the description of the different stages or roles of crowdsourcing in disaster management to our best knowledge is beyond the state-of-the-art, and can help focussing the crowdsourcing disaster management discussion on concrete risk scenarios. Moreover, from the perspective of Priority Action 1 & 2 of the Sendai Framework, the monitoring of some well-known platforms to check their level of "compliance" would highlight existing risk scenarios. Hope remains that this PhD thesis would potentially be very supportive document while adapting some privacy policies by various stakeholders including various authorities of governments.

1.5.4 Disaster Risk Management (DRM) laws

In last one decade numbers of countries enacted disaster management laws, regulations and policies. The International Federation of Red Cross and Red Crescent Societies have grouped all Disaster Risk Management (DRM) laws into four main types[29]:

[29] International Federation of Red Cross and Red Crescent Societies, *Effective law and regulation for disaster risk reduction: a multi country report*, June 2014, esp. page 41-42.

- **Type 1 laws** focus on preparedness and response. The scope is not oriented to managing natural hazards in advance or on long term reconstruction process (Iraq, Nepal).
- **Type 2 laws** have a broad DRM focus. Even if it includes some elements of risk reduction, it does not regulate resourcing, risk mapping or education (Brazil, South Africa).
- **Type 3 laws** give Disaster Risk Reduction (DRR) priority with a high level of detail. Resourcing, risk assessment, risk mapping, early warning and education are regulated, like in Mexico, Philippines and Vietnam.
- **Type 4 laws** give DRR priority with a low level of detail. Laws can be on specific hazards, on resource management, building and construction and on local governance. The general disaster risk governance capacities are sufficiently developed and integrate into existing governance structures, such in Japan and New Zealand.

A concrete Privacy and Data Protection Risk Assessment and Recommendations for disaster management platforms can offer valuable recommendations for lawmakers and other stakeholders like disaster management communities and digital volunteers which are presently missing from type 3 or 4 regulations.

1.5.5 Data Protection

The general principles of Privacy and Data Protection apply to the personal information involved in the disaster management platforms. For instance the International Committee of the Red Cross

has adopted some rules on Personal Data Protection and includes these basic principles[30]:

- Legitimate and Fair Processing (art. 1)
- Transparent Processing (art. 2)
- Processing for specific purposes / Further Processing (art. 3)
- Adequate and Relevant Data (art. 4)
- Data Quality (art. 5)
- Retention, destruction, and archiving of data that are no longer needed (art. 6)

According to these principles, some rights of the data subjects are then mentioned:

- Information (art. 7)
- Access (art. 8)
- Correction (art. 9)
- Erasure (art. 10)
- Objection (art. 11)
- Profiling (art. 12)
- Assertion of data protection rights by individuals (art. 13)

Based on these Principles and rights, the ICRC Commitments refer to responsibility and accountability (art. 15), Data protection by design and by default (art. 16), Data Protection Impact Assessments (art. 17), Documentation of Processing (art. 18), Cooperation with supervisory authorities (art. 19), Data Breaches (art. 20) and Data Security (art. 21).

[30] ICRC Rules on Personal Data Protection, The ICRC Data Protection Reference Framework, adopted by the Directorate of the ICRC on 24 February 2015 and updated on 10 November 2015.

A concrete chapter is also reserved to Data transfers and its limitations (arts. 22 -24). On the other hand, an ICRC Data Protection Office and ICRC DP Commission ensure effective implementation of the rules (arts. 25 – 27).

Another example of Data Protection general framework used for Disaster management is the Policy on the Protection of Personal Data of Persons of Concern to UNHCR[31].

The general principles of data protection legislation should also be present in the crowdsourcing crisis management framework. The Commission draft proposals released on 25 January 2012 a General Data Protection Regulation and a Police and Criminal Justice Data Protection Directive. The GDPR has been adopted in April 2016 and will replace the 1995 EU Data Protection Directive[32]. On its recital 46, humanitarian purpose is considered as lawful processing of personal data. However, sensitive data require explicit consent (recital 51), although some situations and facts (recitals 52, 53 and 54) can justify concrete derogations (also art. 9). One interesting new protection is the right to be forgotten (art. 17, recitals 65 and 66). It is also worth noting an evaluation or profiling leading to a decision on a person cannot be based solely on automated processing (recital 71, art. 4, 4 and art.22). Privacy by design and privacy by default are also expressively

[31] Policy on the Protection of Personal Data of Persons of Concern to UNHCR, adopted on May 2015.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

mentioned in art.15 (and recital 78). Other relevant safeguards are data protection impact assessments (recitals 84, 90, 91 and 94, art. 35) and codes of conduct (art. 40). Security issues, and concretely data breaches are also included in recitals 85 and 86 and art. 33. Certifications and data protection seals should be also considered according to recital 100 and art. 42. Last but not least, following the accountability principle (art. 5.2), the controller shall be able to demonstrate compliance.

Thus, based on the existing security and data protection concerns in various crowdsourcing platforms and existing general risk reduction and data protection principles, the crucial need emerged is to provide a general Privacy and Data Protection Risk Assessment and Recommendations for current crowdsourcing disaster management platforms. Hope remains that the Privacy and Data Protection Risk Assessment and Recommendations would partially address the need mentioned in Priority Action 1 and Priority Action 2 of the Sendai Framework for Disaster Risk Reduction 2015-2030.

1.6 Specific Aims

To address two priority actions mentioned in the Sendai Framework for Disaster Risk Reduction 2015-2030, the research work aimed to offer privacy and data protection recommendations for Crowdsourcing Crisis Management Platforms. So, the whole research was conducted with the following aims.

Aim 1: To identify how the Priority Action 1 of the Sendai Framework for Disaster Risk Reduction 2015-2030 can be enhanced more by

highlighting the importance of ‘privacy’ and ‘data protection’ in using crowdsourcing process in any disaster / crisis management event.

Aim 2: To contribute in fulfilling partially the Priority Action 2 of the Sendai Framework by assessing privacy and data protection risks and offering recommendations for Crowdsourcing Crisis Management Platforms.

1.7 Relevance of the Topic

The initial rigid separation between volunteers, as data source, and first response teams, as decision-makers, is not taken for granted in current crowdsourced crisis informatics. The empowerment of volunteers makes them be part of the initial decision-making process and their participation is being monitored and led by domain experts. However, some relevant questions are still unanswered. For example, whether there is a need for more data in the decision-making stage during a crisis event to have a positive impact on the empowerment of volunteers at the selection and coordination stages? Will the next generation crowdsourced crisis management focus more on automatic decision-making support than human decision-making support? Is the empowerment of automatic decision tools less risky for experts than the empowerment of volunteers? Would the decisions made by experts also become soon raw data for data analytics and automatic decision support tools? This research tries to address all these relevant questions at least from the legal and ethical perspective.

1.8 Research Methodology and Approach

Based on the in-depth desk research, understanding about the privacy, security and data protection issues; and to address two priority actions mentioned in the Sendai Framework, the following research methodology and approach guided the PhD research work:

1.8.1 Research Aim 1: *To identify how the Priority Action 1 of the Sendai Framework for Disaster Risk Reduction 2015-2030 can be enhanced more by highlighting the importance of 'data protection' in using crowdsourcing process in any disaster / crisis management event.*

A. Specific Research Question:

Based on the Priority Action 1 of the Sendai Framework for Disaster Risk Reduction 2015-2030, how to enhance 'data protection' and 'privacy' issues in using crowdsourcing process in any disaster / crisis management event?

B. Research Focus

Identification of Crowdsourcing Crisis Management Platforms

We had some pre-selected criteria relevant to our particular research questions and we used purposive sampling to identify crowdsourcing crisis management platforms. We could not fix the number of crowdsourcing platforms to be investigated prior to the data collection. On the basis of the 'theoretical saturation'[33], we decided to use purposive sampling. Also the

[33] The point in data collection when new data no longer bring additional insights

identification of the platforms depended on the on the resources and available time we had, as well as our research objectives. As we conducted data analysis and review in conjunction with the data collection, we found purposive sampling was most useful for our research.

To understand privacy, security and data protection aspects within existing different crowdsourcing crisis management approaches, a qualitative research study was conducted among Ushahidi, Digital Humanitarian Network, MicroMappers and Google Crisis Map.

i. Ushahidi has been identified for the research as it is considered as the pioneer crowdsourcing crisis management platform.
ii. The Digital Humanitarian Network (DHNetwork) has been identified for the research as DHN is the network of Volunteer & Technical Communities of its' kind to leverage digital networks in support of humanitarian response.
iii. The platform 'MicroMappers'(MM) has been identified for the research as it has started AI (Artificial Intelligence) for the first time to select data and information provided by users.
iv. Google Crisis Map (GCM) has been selected for this research to identify, having all latest technological

---

to the research questions

facilities, how does it care about privacy, security and data protection issues.

Mapping 'data protection' and 'privacy' issues of crowdsourcing platforms

Based on various privacy, security and data protection components related to different crowdsourcing crisis management platforms, we mapped data protection and privacy issues of crowdsourcing crisis management platforms.

Mapping existing national, regional and international laws, regulations and policies and identifying best practices

We also assessed different national, regional and international laws, policies and frameworks to understand the data protection, privacy and security issues of individuals while engaged in crowdsourcing process. We also identified some best practices.

1.8.2 Research Aim 2: *To contribute in fulfilling partially the Priority Action 2 of the Sendai Framework by assessing privacy and data protection risks and offering recommendations for Crowdsourcing Crisis Management Platforms.*

A. Specific Research Question:

What could be the potential components of privacy and data protection recommendations for Crowdsourcing Crisis Management Platforms that can contribute in fulfilling partially the Priority Action 2 of the Sendai Framework?

B. Research Focus:

Identification of different stages

Three different stages in using crowdsourcing platforms for crisis management were identified. The stages are a) Retrieval and Selection (RS); b) Situational Awareness (SA); and c) Decision Support Systems (DSS).

Mapping of clear roles of community volunteers

Various roles of community volunteers were identified i.e. Retrieval and Selection, Situational Awareness and Decision Support Systems.

Identification of decision – making process

While exploring the research question for the Aim 2, we identified various decision-making processes in crowdsourcing crisis management.

Exploring existing relevant frameworks

To strengthen disaster risk governance to manage disaster risk, we tried to explore the gap in existing disaster management framework and to propose solutions 'to assign, as appropriate,

clear roles and tasks to community representatives within disaster risk management institutions and processes and decision-making.

1.9 Potential Contribution to the Field

The Sendai Framework for Disaster Risk Reduction 2015-2030, and the 2005 Hyogo Framework for Action (HFA1) settled the disaster risk reduction principles. The 'Guiding Principles' of the Sendai Framework for Disaster Risk Reduction 2015-2030 identifies that 'disaster risk reduction requires a multi-hazard approach and inclusive RIDM based on the open exchange and dissemination of disaggregated data, including by sex, age and disability, as well as on easily accessible, up-to-date, comprehensible, science-based, non-sensitive risk information, complemented by traditional knowledge.'[34] The potential contribution to the field concentrates to two main priority actions i.e Priority Action 1 and Priority Action 2 that proposed in the Sendai Framework for Disaster Risk Reduction 2015-2030.

In the 'Priority 1: Understanding Disaster Risk' under the 'Priorities of Action', the Sendai Framework mentions, 'to promote the collection, analysis, management and use of relevant data and practical information and ensure its dissemination, taking into account the needs of different categories of users, as appropriate.'[35] The Sendai

[34] Art 19 (g), Sendai Framework for Disaster Risk Reduction 2015-2030, (2016). UNISDR, United Nations, pp. 13.
[35] Art 24 (a), Sendai Framework for Disaster Risk Reduction 2015-2030,

Framework does talk about importance of 'data' but not the 'data protection' during disaster.

Thus, the 'data protection risk' of different stages or roles of crowdsourcing in disaster management is beyond the state-of-the-art; and the potential solutions can help focussing on discussions about concrete risk scenarios in various stages of crowdsourcing disaster management.

In the 'Priority 2: Strengthening disaster risk governance to manage disaster risk', the Sendai Framework mentions, 'to assign, as appropriate, clear roles and tasks to community representatives within disaster risk management institutions and processes and decision-making through relevant legal frameworks, and undertake comprehensive public and community consultations during the development of such laws and regulations to support their implementation.'[36]

Thus, we find that assessing privacy and data protection risks and proposing some recommendations for crowdsourcing crisis management platforms would be the most important urge of the hour. These recommendations will certainly fulfil one of the several expectations under the Sendai Framework. Hence, offering recommendations to address various legal, ethical and technical issues related to crowdsourcing crisis management platforms definitely goes beyond the state-of-the-art.

(2016). UNISDR, United Nations, pp. 14.

[36] Art 27 (f), Sendai Framework for Disaster Risk Reduction 2015-2030, (2016). UNISDR, United Nations, Pp. 17.

Consequently, the description and analysis of the different stages or roles of crowdsourcing in disaster management to the best of our knowledge is beyond the state-of-the-art, and can help focussing the crowdsourcing disaster management discussion on concrete risk scenarios.

The assessment and proposed recommendations for Crowdsourcing Crisis Management Platforms describes the risk scenarios and, for the first time it also provides clear Recommendations both to disaster platforms, digital volunteers, and authorities. We hope this will allow a more focused discussion not only on concrete real situations but also on general principles to apply. Moreover, the recommendations ready-to-use should be confronted with real disaster events and the subsequent discussion can improve them and be helpful for policymakers and lawmakers.

1.10 Description of the content

This thesis moves from a review of historical background of crowdsourcing, and then focuses on contemporary research practices of researchers and disaster management community members. Based on the evidences and experiences, a set of recommendations for crowdsourcing crisis management platforms have been developed. A short description of various chapters is given below. Supporting research work and publications are provided in appendices.

1.10.1 Evolution of Crowdsourcing

This chapter contains the description of evolution of crowdsourcing and it outlines the history of crowdsourcing and highlights some historical

and recent examples that occurred before and after the term ‘crowdsourcing’ existed. This chapter aims to provide a basic understanding on crowdsourcing, while it illustrates the use of different types and methods, advantages and several concerns of crowdsourcing. This chapter also provides a brief analysis on potential Data Protection, Privacy and Security concerns under the New Media Age.

1.10.2 Evolution of Crisis Management Platforms

This chapter contains the evolution of modern time crisis management platforms. Since 2008, crowdsourcing platforms have played a crucial role in crisis management. This chapter highlights the fact is that although use of crowdsourcing allows a higher availability of information, inaccurate reports provided by volunteers are increasing that requires some filtering and proper selection from experts. This chapter identifies the lack of coordination between emergency response groups and also identifies that digital humanitarians has also blurred the initial expectations of using crowdsourcing for crisis events. Gradually, this chapter discusses the automatic crowdsourced data analytics- a new generation of crisis informatics that combines crowdsourcing with data analytics.

1.10.3 Detection of Risk Scenarios

As the crisis management is now based on combination of crowdsourcing retrieval and filtering, and decision support systems, this chapter records different risk scenarios in relation to various steps of

crowdsourcing crisis management. This chapter is founded to identify some ethical and legal concerns in crowdsourcing crisis management process. Finally, this chapter provide some possible solutions for disaster response platforms' management contributing to Disaster Risk Reduction.

1.10.4 Possible General Solutions

As emerging tools and technologies offer huge potential to response quickly and on time during crisis, crisis responders do take support from these tools and techniques. In spite of existing risks, the Sendai Framework for Disaster Risk Reduction 2015-2030 has not offer potential solutions of risks in using emerging ICTs and crowdsourcing in disaster management. In continuation of chapter 5.3 this chapter identifies those risks once again and present solutions in form of general recommendations for crowdsourcing crisis management platforms. It includes legal, ethical and technical recommendations for crowdsourcing disaster management. Concrete recommendations for three different stages i.e Retrieval and Selection (RS), Situational Awareness (SA) and Decision Support Systems (DSS) of crowdsourcing crisis management platforms and crowdsourced crisis data are proposed in this chapter.

1.10.5 Recommendations for selected crowdsourcing crisis management platforms

As identified during the research that following the birth of 'digital'

crowdsourcing for crisis response, numbers of platforms have been developed by different crisis response to address crisis. Present crisis response work is more affordable, more accurate and more trustworthy. However, researchers and crisis responders mention some risks of using emerging ICTs and crowdsourcing in disaster management. To understand and identify these risks properly, an intensive research was conducted among four crowdsourcing platforms. In this chapter, the investigation result of four different crowdsourcing crisis management platforms i.e. Uhahidi, Digital Humanitarian Network, MicroMappers and Google Crisis Map is given and platform specific recommendations are given.

1.10.6 Conclusions and Future works

The final chapter – 'conclusion and future works' provides the brief description of whole research activities that we have conducted in past three years. This chapter also mentions the research result or outcome. Based on the research result, some future activities along with brief recommendations proposed in this final chapter.

II. Crisis Crowdsourcing

2.1 Crowdsourcing Improves Disaster Management

Crowdsourcing crisis management - either man-made or natural - has been successful helping victims to find a safe place [21]. It is a great way to engage the community and to gather the accurate real-time information from the ground. Thus, it helps to manage any crisis properly and promptly. Crowdsourcing has also been used in public governance. Crowdsourcing is also very convenience in gathering public opinion to amend laws e.g. in Iceland in 2011 and in India in 2013 [22], informing citizens about a potential storm or helping poor farmers to find the best market to sell the products [23] etc. Like other professionals, health professionals also are using crowdsourcing as a faster alternative to traditional methods for predicting and monitoring infectious disease outbreaks. For example, in Haiti in 2010, informal sources like group discussions in social media including Facebook and Twitter revealed a cholera outbreak's in the country two weeks before the health ministry issued its report on the cholera situation [24].

The use of crowdsourcing in crisis management not only makes it possible to mine, aggregate and classify data but also helps in preparedness to face a particular situation, response during the situation and recovery after the situation. Crowdsourcing initiators can connect individuals and communities to gather data or to complete one or a set of easy tasks, such as measurements, identifying disaster prone areas or to guide someone who is in need etc. Crowdsourcing platforms allow common citizens and organizations to install, deploy, and manage

crowdsourcing platforms in response to social issue, health issue and sudden outburst emergencies. They can also communicate with other crowdsourcing initiators with whom they can share different outcomes on similar issues. Another option can also work the other way round: experts can contribute their expertise to a particular problem.

However, with all these positive impacts of crowdsourcing crisis management platforms, some concerns exist as well.

2.2 General Concerns about Crowdsourcing Crisis Management

Governments, different security agencies, multinational corporations and also terrorist organizations are able to virtually spying on any person if they wish to. In the context of 'political crisis' like the crisis in Libya and in Syria, governments can avail GPS/GPRS-based data provided by citizens and misuse them to oppress oppositions. Using crowdsourcing in public governance is a potential threat to the privacy and protection of personal and sensitive data of users. As millions of data can easily be gathered, governments and others could have very detailed information of who we are, our mobile numbers, IP address of our computers, geographical location etc. Sometimes secret agencies collect different types of information using crowdsourcing method and they can easily guess what type of person we are. This assumption can lead a problem if they are used to target on the ground of assumed health status, age, gender, race, religion, political ideology, sexual orientation, etc. The situation gets even more serious when governments, with the help of their 'muscle power' want to gain access to this personal and sensitive personal

information and other data with the intent to dominate over opposition voices. Sometimes governments itself initiate collecting data using different crowdsourcing means to oppress those individuals or groups who are against governments [25]. Thus, the contributors of crowdsourcing initiatives become potential victims of human rights violations by the secret agents of governments, multinational companies or even by oppositions or terrorist organizations sometimes.

In the context of political crowdsourcing, the contributors reporting on abuses or speaking out against these forces have found themselves targeted for attack by the forces themselves or their proxies - with consequences ranging from harassment to imprisonment and death [26]. For example, during the election monitoring effort of Ushahidi in Egypt encountered regular harassment by members of Egyptian Security Services [27] It has also been noted that the volunteers with fair local knowledge have left the crisis mapping work for Libya in 2011, as they are likely to be the most sensitive to the possible security concerns [28]. The 'Libya Crisis Map' was private initiative. When the United Nations Office for the Coordination of Humanitarian Affairs (*UN OCHA*) decided to make the map public, every Libyan volunteer left [21]. This fact of driving away the most important members in the Libya Crisis Map initiative has also raised the question of proper coordination along with the security and privacy concerns of using the Ushahidi crowdsourcing software. The privacy issue in the context of disaster response crowdsourcing initiatives is not really potential threats to life of the contributors. Here, the privacy issue is

very much linked with personal data of individuals. Not all contributors want to publicize their mobile number, name, sex, place etc.

During the Haiti earthquake all contributors said to have been able to access the messages through private channels. Partners in this initiative did not have permission to publish the messages received in the emergency mobile number 4636 on a public-facing map -by their own conditions for publication-. Such type of privacy breach in a more high-risk conflict situation would have serious consequences for those contributors whose identities were exposed [21]. The 'Grand Round Table' -an online platform- is being used to find possible help from a secure, intimate group of colleagues in health service sector. In this platform physicians can post difficult cases to seek help. Sometimes, it is being used for diagnosis and medical treatment. Medical transcription[37] process based on the crowdsourcing methods has created a wider base for medical transcriptionists, who can be trained at home and online, and, ultimately, perform the work on a more cost-effective basis [29]. Another mobile-based crowdsourcing platform, 'MedAfrica' mobile application is a Medical Services Content Platform (MSCP) that seeks to create health awareness among citizens from the comfort of their mobile phones. This extraordinary mobile system seeks to increase interactions and purposeful engagements between health practitioners and common people of their services [30]. Generally, service users are a bit reluctant to share

[37] A process where written records and notes are translated into an electronic form, entered into a database, and used in the wider-spread arena of documenting the occurrence and frequency of specific illnesses.

their private information e.g. name of diseases, sex, age etc. in a public forum. In terms of mobile-based crowdsourcing health service platforms, the biggest privacy concern with the use of cell phones in healthcare is lost or stolen phones that contain unencrypted patient data [31]. Even the World Bank has identified that 'the health sector remains both complex and challenging' and the 'Privacy and security concerns' is one of 'the most relevant challenges to the greater uptake of mobile-based health service [30]. Contributors in any crowdsourcing initiatives would look for high level of privacy, security, anonymity and guarantee for data protection [32]. Unfortunately, not all crowdsourcing platforms could provide the same but high level of security, privacy and private data protection. These three aspects of crowdsourcing are really vital in making sure the security of contributors. These are also important in terms of security information that integrated with different crowdsourcing platforms.

In spite of different crowdsourcing systems, platforms and the method of interaction there may be some level of security and privacy risk linked with contributors. In one hand, there are some platforms that facilitate anonymous contributions that may pose low risk, and in the other sending various levels of personally identical information that may pose higher risk to contributors. Similarly, opportunistic systems may pose a high level of security risk than participatory systems where users manually control data collection [33]. The Ushahidi platform deployed in Haiti by the Fletcher team had the potential to provide hyper local information on the security situation through the

population but did not capture enough reports with specific information to make better decision [34]. In the age of 3-G phones, citizens have further opportunity to participate in crowdsourcing process- not only because of their portability and easy access to the Internet but also because of other functionalities like GPS / GPRS, cameras, and accelerometers attached with 3-G phones or smart phones [35]. While all these functionalities and other 3-G mobile applications are being considered as highly productive in different context, they may also expose users to latest types of security and privacy concerns. In such circumstances, the World Bank observes, 'citizens often express concern about the security of their private and confidential information, possible surveillance, and anonymity'. In the report it suggests, 'without strong protection or the quick resolution of any breach, citizens will be wary of sharing their information with the government, and efforts to connect and interact would quickly be undermined'[30].

Recent emergence of ICTs, some platforms including social media networks and other web 2.0 tools have changed the perception about privacy and it is becoming increasingly confusing [36]. It looks that users really do not care about to sharing personal information about him/her, about one's friends or networks in digital environments. Sometimes it becomes really confusing for the user to distinguish between what is public and what is private [37]. Users act in the same way when it comes contributing in crowdsourcing initiatives. Even sometimes some energetic contributors become desperate to share confidential, sensitive and personal information in

crowdsourcing initiatives. In the crowdsourcing process all data received from contributors store on a centralized server and 'storing the preference information on a centralized server can expose the users to security and privacy breaches, and in any case requires a great deal of trust' [38]. Despite the potential use of mobile or web based crowdsourcing platform for natural disaster, conflict resolution, health and diseases related issues, experts say they worry about the added risks of security breaches, privacy violations and other concerns that come with the increasing use of different crowdsourcing processes.

The issue of data protection in crowdsourcing initiatives is very important. In every crowdsourcing initiative, data protection is the key. As the scope of crowdsourcing is becoming wider, people are using it for different purpose. In the context of crowdsourcing efforts for pharmaceutical research, people need to be aware of some challenges like tissue handling [39], handling patients of infectious diseases with rare etc. The International Organization for Migration has developed 13 data protection principles which are: 1. Lawful & Fair Collection, 2. Specified and Legitimate Purpose, 3. Data quality, 4. Consent, 5. Transfer to Third Parties, 6. Confidentiality, 7. Access and Transparency, 8. Data Security, 9. Retention of Personal Data, 10. Application of the Principles, 11. Ownership of Personal Data, 12. Oversight, Compliance & Internal Remedies and 13. Exceptions [40]. However all these principles cannot be applicable in crowdsourcing process. For example, the first principle states, "Personal data must be obtained by lawful and fair means with the knowledge or consent of the

data subject." "What does this mean when the data is self-generated and voluntarily placed in the public domain? This question also applies to a number of other principles including "Consent" and "Confidentiality"[41]. Thus, from the above-analysis, it is clear that there is a need for some relevant data protection principles especially for 'New Media' as the character of crowdsourced dataset is not similar to other types of dataset those do not necessarily fall under 'New Media' dataset category.

The implication of crisis crowdsourcing has been so far positive for the society. No serious disadvantages that originated from crowdsourcing have been identified yet. However, the recent disclosures by NSA contractor Edward Snowden established the fact that the privacy of common people is really in danger. These would have huge impact on our society and also on different communication platforms and communication tools. So, an exceptional attention with innovative approach is needed when developing new communication tools and platforms, as users will look for guaranteed quality, high level of anonymity, privacy, and security. Research institutions, governments, NGOs, business organisations should take initiative to handle those threats from ethical, legal and technological context. Finally, a universal framework for 'New Media' communication should be developed to address the security, privacy and data protection issues.

III. Evolution of Crisis Management Platforms

3.1 From Crowdsourcing Crisis Management to Crowdsourced Crisis Informatics

By deploying the crowdsourcing platform to monitor incidents of post-election violence and peace efforts throughout the country in Kenya in 2008, Ushahidi paved the way for crowdsourced crisis informatics, *i.e* the use of platforms for crowdsourcing crisis management [42]. Using Ushahidi's products, Crisisnet and Crowdmap, volunteers and other users can send "reports", either directly, or through social media or conventional media updates. Since 2010, more crowdsourced crisis informatics tools have been introduced, such as Sahana Eden[38][43], which was used by individuals, organizations and governments for several disasters[39]. CrisisTracker is another example of first generation crowdsourced crisis platforms.

All these tools improve the decision-making of expert response teams by providing updated knowledge and information. Users and volunteers are a source of relevant data and these tools gather information and connect non-experts with experts, enhancing the situational awareness of the latter. Today, increasing amounts of data used by experts come from social networks, mobile phones and

[38] Eden stands for '(Emergency Development Environment) for Rapid Deployment Humanitarian Response Management.

[39] Flooding in Venezuela and in Pakistan on 2010; hurricane in Veracruz, Mexico on 2010; earthquake and Tsunami in Japan on 2011; flooding in Colombia on 2011; wildfires in Chile on 2012; Typhoon Haiyan (Yolanda) – November 2013, Typhoon Ruby – Philippines – December 2014 and Earthquake in Nepal (April – May 2015).

digital volunteer communities[40], and the involvement of volunteers and non-experts is clearly relevant. Nonetheless, current crowdsourced crisis informatics is not limited to data retrieval. Two new capabilities are also based on crowdsourcing: first, the empowerment of trusted volunteers gradually consolidated as support teams; second, the use of data analytics. As a result, current crowdsourced crisis informatics combines human collective intelligence with big data and machine learning [44,45,46,47,48,49,50,51,52].

Why disaster management is evolving this way? Crowdsourcing crisis management has shown to be successful at producing more data than traditional governments and news reports, even if it has yet to reach its potential impact [53]. However, having more data does not necessarily imply a more efficient response. Experts need accurate, relevant and updated information on time [54,55,56]. Data filtering and selection are therefore crucial, and crowdsourcing can also be helpful for this emergent challenge.

Accuracy and reliability is not the only aspect to consider for an efficient disaster response. Direct access to the top emergency response team in real-time could be overwhelming. Therefore, coordination strategies between experts and selected non-experts are emerging. In other words, an intermediate layer of decision-support teams is envisioned. Volunteers are increasingly empowered to participate in the decision-making process, and new strategies of coordination are

[40] Some examples of current crowdsourcing disaster management platforms are OpenIR; Google Person Finder; ArcGIS; Ping; Recovers; PADDDtracker.org; Google Crisis Map; GeoChat; InaSAFE; Geofeedia; LEEDIR; Geo-pictures; CrisisCommons, etc.

being proposed, such as situational awareness services.

The decision-making process of the first response teams is hence conditioned by previous selection and situational awareness processes based on crowdsourcing. The initial rigid separation between volunteers, as data source, and first response teams, as decision-makers, is not taken for granted in current crowdsourced crisis informatics. The empowerment of volunteers allows them to participate in the initial design of the decision-making, although their participation is still monitored by experts. Moreover, digital volunteers might also be replaced by a sort of e-crowdsourcing, based on Artificial Intelligence (AI). AIDR is a crisis management platform based on AI. Retrieved and classified data of past events allow modelling the risks of future events.

3.2 Crowdsourcing-based Data Retrieval and Selection

Retrieval and selection can be directly based on crowdsourcing or can be indirectly based on it to train tools that perform this task automatically in the future. We will start with selection done by volunteers and communities, and then we describe tools based on crowdsourcing that offer selection capabilities.

3.2.1 Selection by digital volunteers and online communities

It has been recognized that reports from first responders, such as firemen or emergency medical personnel and crisis response coordinators working on the ground assure highly accurate information. In terms of the participation of ordinary people to provide information

on incidents, Internet users or online volunteers can provide additional perspectives, and this might sometimes be crucial for response teams and even for other citizens who can make informed decisions based on near-real-time information [57]. Sometimes, the relevance or the accuracy of crowdsourced information is very low, thus appropriate selection is needed. Users and volunteers filter and select information by reading reports, or visualizing a photograph or an aerial picture, or sometimes identifying the geolocation of a particular incident.

Collective task-solving from online communities is also helpful for selection. Tools like Verily and The Internet Response League (IRL) collect crowdsourced evidence and provide important information for crisis responses. Verily is an experimental web tool designed to rapidly share verified information during humanitarian disasters. It uses a time-critical crowdsourcing process to verify information during major disasters on behalf of humanitarian organizations and media groups [58]. Humanitarian organizations and emergency management responders are completely unprepared to deal with this volume and velocity of crisis information [59]. The Internet Response League (IRL) is based on online gamers. Because more than half a billion people worldwide use computers and videogames for at least an hour a day and are frequently connected to the internet, they can play a significant role in supporting disaster response operations worldwide. Indeed, it has been estimated that if all these gamers had been invited to search through the 20 million tweets posted during Hurricane Sandy that would have taken just 20 seconds [60].

According to experts, initiatives like Verily and IRL show how different types of online communities (i.e. online gamers, social networking site users, etc.) can help solve small tasks in just few seconds, and also assist crisis experts and humanitarians in the management of disasters and in providing prompt and effective responses to crisis situations [58, 59, 60]. However, as the most of the online gamers' age is below 20 years, solely using gamers for verification of crisis incidents could be dangerous. Crisis mapping platforms are an excellent example of this kind of crowdsourced-based selection. Geo-location reports usually convert locations to GPS locations and plot on a map. Normally, reliability and accuracy of incidents are verified by the disaster management team. The team of experts verifies reports and additional about crisis incidents. Trust is associated with group membership created by users. The group administrator requests high reliability level from a system administrator. Users then filter reports and rank them by trustworthiness or by another factor, for example, location or type of incidents like flood, earthquake, and road displacements etc.

For instance, 'MicroMappers' online volunteers select information on incidents. There are several categories of digital volunteers associated with MicroMappers[41]. 'Text Clickers', for instance, identify the

[41] Volunteer categories are 1. 'Text Clickers' for Tweets, 2.'Image Clickers' for Pictures, 3. 'Aerial Clickers' for Aerial Pictures, 4. 'Video Clickers' to tag videos and finally, 5. 'Geo Clickers' to map tweets, pictures and videos. There will be another category called 'Translate Clickers' to crowdsource the translation of tweets very soon.

relevance of Tweets during an emergency or disaster. 'Image Clickers' are volunteers who rate the damage by looking at images. These volunteers check, verify and rate different crowdsourced information and then the platform passes that information to 'Geo Clickers' who put those tweets, pictures and videos on the map. In the earthquake in Nepal in May 2015, over 2800 volunteers from all over the world reviewed tweets and images to support humanitarians with information insights. These 'clicks' and 'selections' of texts by volunteers produced a highly accurate dataset about the earthquakes in Nepal that was shared and incorporated into the damage assessment and decision-making processes. At the end of the process, some empowered group of volunteers insert the obtained information on a map, where the type and seriousness of incidents are reported. At this stage the support teams and the decision-makers work together to accelerate the crisis management.

3.2.2 Selection by Data Analytics

Without the participation of volunteers, the relevance and accuracy of data, and the trustworthiness and reliability of users and volunteers could not be assured automatically. Crowdsourcing allows now to envision a new selection based on data analysis of social networks, user rankings, content classification, sensors and a new generation of crisis mapping.

Using social networks' data mining, a platform can perform good selection. It can help extracting data from public pages for emergency platforms. For instance, users' actions, likes, comments and posts on the Facebook page allowed the creation of a training set

for the “Hurricane Sandy lost and found pets” page [61]. The number of reports submitted or bookmarked, and successful or unsuccessful matches have been extracted and used to label the user as active or not, and as effective or not. To obtain a model of highly active users, users were also ranked based on the number of their likes, comments and posts. Active and effective users are thus preferred when assessing the relevance and accuracy of data.

Machine learning, data mining and game theory can also combine to assign users a score or weight [57]. Users are evaluated as active or effective, but the ultimate goal is to rank them. Initially everyone has zero points; then users can get points added or deducted. The selection of data shifts then into a users’ ranking. For instance, valuable information can be collected from mobile sensors and locations and this information is sent to remote databases where machine learning takes place. Interconnections between collection of reports, classification of crowdsourced information and the resulting network models after using machine learning might offer fascinating statistic correlations to improve trustworthiness models. In such cases data accuracy is not obtained or checked directly but is rather retrieved from selected trustworthy participants.

Sometimes data accuracy becomes the main goal for several reasons. For instance, machine learning has been used to automatically evaluate -within seconds- tweet trustworthiness based on social media message contents. Based on semi-supervised learning *TweedCred* [62] requires first training set of tweets with well- known trust. Tweets are to be

considered informative, and then definitively credible. The next step is the extraction of tweet meta-data -number of seconds since the tweet, source of tweet-, tweet content -number of characters, presence of negative emotion words-, tweet author -number of followers-, tweet network -number of retweets- and tweet links -ratio of likes-.

Another interesting example is the Artificial Intelligence Disaster Response (AIDR). Twitter messages are classified by at least three volunteers. If they agree and come to one conclusion, then AIDR starts to learn and auto-tags twitter messages. AIDR evaluates and shares the confidence level -for instance 75%- of the auto-classification, and the more tweets a person sends the higher AIDR's confidence level [47][6]. Interestingly, classified tweets are then provided to first responders, aid agencies and NGOs. MicroMappers, as before mentioned, also combines volunteer filtering with machine learning on a "Text-Clicker" option. Semi-automatic image "Aerial-Clicker" and video streaming "Streaming-Clicker" options will be soon ready.

Social Networking Data Mining and machine learning are not the only automatic selection tools. Risk analysis can be based on sensors. For instance, visual and audio analysis can alert of high or low level risk events, *i.e.* anomalous events [54], according to algorisms. Past anomalous events are added to a map to obtain correlations with new alerts with the same level of risk to eventually update the model or generate alarms. This sensor detection can be a perfect complement and can even confirm previous alarms coming from

mobile phones. Parameters of the alarm map resulting from sensors can be modified to obtain added information and confirm or discard previous alarms.

The MicroMappers community aims to have an ultimate comprehensive map to display the resulting data filtered both via data analytics and with Geo Clickers (volunteers). This enhanced map would display filtered tweets, text messages, photos, videos, satellite and unmanned aerial vehicles (UAVs) imagery. Each data type would be a different layer on a "Meta-Data Crisis Map". This eventually will be an ultimate selection and classification platform, based on crowdsourced data analytics for crisis management.

3.3 Crowdsourcing-based Situational Awareness

Selection and classification are only initial steps towards decision-making. Situational awareness can also be envisioned afterwards. And, likewise for selection, it starts with digital volunteers and based on their inputs it evolves to data analytics.

3.3.1. Expert volunteers for Situational Awareness

Communities of trusted volunteers can be effective support teams to discover and select relevant data. Access to users' live video streaming from mobile devices could help experts coordinate their activities. Users would provide their devices' sensors to improve the situational awareness of emergency response teams [63]. Users of location-based services, like microblogs for instance, create time-stamped and geo-located data using smart phones with GPS [64]. The augmented view of their environment might be crucial in scenarios of limited visibility like

fire rescues.

These virtual volunteers are only active during the event. They search and filter relevant information in social media and in the news, and receive indications from the emergency response team. They also warn against negative users' comments. Experts can view the video stream and interact with the source of the video if needed. Volunteers provide geo-referenced information, like sensors would do, to contribute to crisis situational awareness. Virtual volunteers usually employ group chat and Skype conversations, and some crisis informatics is now offering management tools to these small support teams [65]. For example, the Digital Humanitarian Network (DHNetwork) is a network of Volunteer & Technical Communities (V&TCs) to leverage digital networks in support of humanitarian response. More specifically, the aim of this platform is to 'provide an interface between formal, professional humanitarian organizations and informal yet skilled-and-agile volunteer & technical networks' (Humanitarian UAV Network (UAViators), Planetary Response Network for crowdsourcing satellite imagery analysis for humanitarian response). Numbers of services, for example, i) Real-time media monitoring of mainstream and social media; 2) Rapid geo-location of event-data and infrastructure data; 3) Creation of live crisis maps for decision support; 4) Data development and data cleaning; 5) GIS and Big Data analysis; 6) Satellite imagery tagging and tracing, and others are being offered by the DHNetwork. With the plan to organize a crisis simulation to assess workflows of DHNetwork in the near future, a number of DHNetwork Coordinators are engaged regularly to 'review activation-requests

and rapidly liaise with the different volunteer and technical teams who are members of Digital Humanitarians to build a Solution Team best able to act on' a particular request.

In the aftermath of some of the recent disasters we have witnessed an increasing number of informal actors, largely volunteer based, entering the field of crisis mapping for humanitarian response. The development of ICTs has opened unprecedented space for engagement to a variety of individuals and groups, regardless of their physical location and affiliation to traditional responders. Similarly, with increased access to technology local communities – always the first responders in crisis situations – are not only building and improving their own preparedness and response systems, but are also more effectively engaging in traditional humanitarian preparedness. We can mention some interesting examples like PeaceGeeks, GISCorps, Standby Volunteer Task Force (SBTF), ESRI, Humanity Road and OpenStreetMap. The Humanitarian OpenStreetMap Team's (HOT) reaction to Haiti earthquake on January 2010 remains one of the most significant 'examples of what's possible when volunteers, open source software and open data intersect' [66]. After the 7.0 magnitude earthquake struck, information on the Google Map of downtown Port-au-Prince was not possible to use humanitarian response as the map was simply incomplete. However, within days, hundreds of volunteers from the 'OpenStreetMap (OSM) community used satellite imagery to trace roads, shelters and other important features to create the most detailed map of Haiti ever made'[67]. One of the remarkable works done by GISCorps in collaboration with and ESRI was to

identify the geo-location of “Mild” and “Severe” damaged tagged images out of over 7,000 images, in the aftermath of Typhoon Yolanda, clicked by users using MicroMappers ImageClicker tool [60, 66]. They have created a live crisis map of the disaster damage tagged using the ImageClicker. One of the remarkable tasks of Humanity Road was ‘to deliver a detailed dataset of pictures and videos (posted on Twitter) which depict damage and flooding following the Typhoon Pablo in 2012, which was projected on a map. Humanity Road (HR) was one of the two volunteer groups worked under the Digital Humanitarian Network’s Solution Team to rapidly consolidate and analyse data to compile a customized Situation Report for OCHA’s team in the Philippines.

3.3.2 Data Analytics for Situational Awareness

Crowdsourced data analytics, for instance visual analytics, will probably support rapid situational decision-making in the near future [64]. Time-stamped and geo-located data from smart phones with GPS, for example, allow pre- and post-event comparisons. This information can unveil trends difficult to detect for humans. As a result, geo-located abnormal use of smart phones due to natural disasters can help in the identification of the main affected areas. Crowdsourcing is also combined with sensors located in specific areas and UAVs [61]. The idea is to merge data and information from different sources and to generate a better situational awareness, thus faster and more accurate event detection. Moreover, this kind of platforms is supposed to offer a decision-planning tool for a prompt response in case of an emergency

[61, 64].

This is a clear example of the continuum between situational awareness and decision-making: the former allows the latter, but also anticipates it. Data coming from different sources are merged and classified as emergency event or normal situation, according to general risk management. Situational awareness is a prerequisite for decision-making, and decision support systems [67]. Therefore, a tool supporting automatic situational awareness is fundamental. Such a tool collects data and offers situation assessment, in this case based on risk estimation. An estimation of the event probability and severity produces an estimation of the risk. If the risk is unacceptable according to some known parameters, then a recovery is suggested. The identification of the risk-reduction components leads to risk management and decision-making. This is only an approximate model of experts' risk level classification.

First response teams might have incorrect information provided by failed sensors or unreliable users, or might not even have any information at all. In these cases, having automatic risk estimation can be useful for unskilled or semi-skilled operators [67]. Well-skilled response team still trust their education and experience rather than determine risk levels using only automatic tools. In these complex cases another option is to trust humanitarian networks, with their digital volunteer teams and data analytics tools.

3.4 Crowdsourcing-based Decision Support Systems for Crisis Management

3.4.1 Volunteers and Communities Support for Decision-making

In crisis response work, common users, responders and other volunteers work mainly under the advice and direction of core decision-making support groups. The United Nations Office for the Coordination of Humanitarian Affairs (OCHA) is 'part of the United Nations Secretariat responsible for bringing together humanitarian actors to ensure a coherent response to emergencies'. Either directly or indirectly, OCHA takes part in any humanitarian crisis management work. By mobilizing and coordinating effective and principled humanitarian action in partnership with national and international actors in order to alleviate human suffering in disasters and emergencies. As OCHA ensures there is a framework within which each actor can contribute to the overall response effort, one of the important efforts it makes is to work directly with digital activists and volunteers to understand the crisis well as it allows OCHA to get reports from the ground. This initiative helps OCHA advocating for the rights of people in need, promoting preparedness and prevention and facilitating sustainable solutions. This UN organ has partnered and worked with different digital humanitarian groups. To deliver OCHA's action plan on the ground, it forms a core decision-making support team that decides on different aspects of crisis response works.

The Digital Humanitarian Network (DHN) is a network-of-networks, 'enabling a consortium of Volunteer and Technical Communities

(V&TCs) to interface with humanitarian organizations that seek their services'. The DHN has been created specifically in order to coordinate the activities of digital humanitarian volunteers. The network brings together many of the major volunteer and technical communities to increase their visibility both amongst themselves and amongst the traditional humanitarian community. This approach of DHN has helped to define a clear activation process among the volunteer communities. Organizations like OCHA and other traditional organizations are able to submit a request and rely on the DHN to build a solution team with the relevant volunteer members within the volunteer communities. This core solution team is responsible for any decision for further course of actions in regards to a particular deployment to manage disaster response activities. As disaster responders use numerous innovative digital tools and techniques, and also other human volunteers, they could easily gather the digitally analysed information on a particular situation. Such type of analysed information helps core 'solution team' or 'decision makers' to take the final decision on further actions in disaster situations.

3.4.2 Data Analysis for Decision Support Systems

Forest fire spread predictions can successfully assess decision support systems. If those tools want to be effective, they need to run quickly enough to provide the output before the real fire evolution, with real-time constraints [68]. In simulation's output is limited to three hours maximum and this leads to a trade-off between resolution and availability. The optimization of algorithms is the way to offer on time

enough accurate data to expert response teams. Housing decision support systems are also starting to provide simulations for the post-disaster housing problem [66]. Real-time housing recommendation needs complex heuristics, and even then two more emerging problems are still unsolved: temporary workers involved in the recovery must be housed, which may not have been included in the simulation, and coordination between housing recommendation institutions has also to be taken into account.

Rapid mapping, *i.e.* "on-demand and fast provision (within hours or days) of geospatial information in support of emergency management activities immediately after an emergency event" is another data analytics valuable technique for disaster management [69]. Rapid mapping is increasingly used in crisis management and there is even an International Working Group on Satellite Emergency Mapping.

Some crowdsourced mapping initiatives like OpenStreetMap (OSM) and the Humanitarian OpenStreetMap (HOT) complement national agencies. Data analytics is also used to generate information. For instance, part of the map production is based on automatic affected population estimations or potential infrastructure damages evaluation. Obviously, this is only possible when there are areas with detailed reference datasets available, otherwise *ad-hoc* crowdsourced mapping would be necessary. Image analytics can also start with volunteer identification of objects and places, and then use data analytics or be available for expert response teams.

Social Networks and media are not only source of data. They can also be important for becoming aware of how communicated alert messages

are perceived by citizens. Tweets sent during the Sandy hurricane, where annotators have manually tagged the emotional content: anger, fear, positive and others. This initial work has been used to train algorithms [61]. The resulting classifications have allowed new retrieval of crisis tweets, previously unseen.

Crisis informatics is now based on crowdsourced data analytics- a combination of crowdsourcing retrieval and filtering, and decision support systems. Digital volunteers are using machines to achieve real-time data analytics. Along with providing information, volunteers also participate in collective task-solving requests. Digital humanitarian networks offer the task of data analysis to volunteer communities. In near future, more accurate digital data i.e. image, geo-location and text, collected through excellent techniques like sensors system, GPS, UAV or satellite, will definitely make tasks more effective. However, there will be more risks as we use emerging communication tools and methods for disaster response management works. The next chapter is going to be based on identifying some ethical and legal concerns in crowdsourcing crisis informatics. Some possible solutions for disaster response platforms' management contributing to Disaster Risk Reduction are also proposed briefly.

IV. Ethical and Legal Concerns of Crisis Management Platforms

Various positive aspects of crowdsourcing have already been recognized. However, some serious concerns have also been raised in terms of privacy, security and personal data protection in using crowdsourcing during any crisis events. At the international level the third United Nations World Conference on Disaster Risk held in March 2015, the Sendai Framework for Disaster Risk Reduction 2015-2030, adopted a ‘concise, focused, forward-looking and action oriented Post-2015 framework for disaster risk reduction [70]. This framework neither used a single word on the role of emerging ICTs in disaster risk reduction nor the potential risks of disaster response workers or volunteers. However, some indirect references to disaster management and response were made. In 2005, The Hyogo Framework for Action (HFA1) settled the disaster risk reduction principles. Risk identification and reduction, disaster response and adaptive governance converge, and crisis informatics plays a relevant role in the disaster management system.

One of the most exciting contributions of ICTs in disaster response coordination work is the use of ICT-based crowdsourcing and crisis mapping. Though, some risks have been identified which are associated with this approach:

4.1 Risks associated with Crisis Crowdsourcing

4.1.1 Security breach due to system malfunction or insecure data transmission: OCHA identifies, ‘as more data systems and devices go

online, there has been an explosion of cyber-crime, as well as cyber-warfare' [71]. Using crowdsourcing in humanitarian crisis management could create risks like attacks on communities like 'aid recipients, such as marginalized groups or displaced people' or groups; attacks on humanitarian partners and this type of attacks could come from terrorist organisations, opposition groups engaged in conflicts etc. 'This motive could be linked to a conflict or political dispute, religious or ethnic tensions, or social mores, such as targeting women who report sexual or gender- based violence' [71]. According to OCHA perpetrator groups may find 'humanitarian organizations as a soft point of entry to government or commercial data sets or networks'. As humanitarian organizations begin using ICT-based crowdsourcing tools and procedures, more sophisticated communication systems and internet-linked tools, cyber- attacks are becoming really easy for perpetrators. Failure to understand these challenges can put victims and others directly at risk that is more than enough to damage the trust humanitarian organizations require doing their work [71].

4.1.2. Personal information disclosure, location data management, sensitive data (health, political opinion and etc.), quality of data and discrimination: Using crowdsourcing process in humanitarian crisis management means dealing with information, personal data and even sensitive data like health or ethnic origins or sexual orientation and etc. Privacy might thus be at risk due to the crowdsourced response platforms involved in the disaster management. The general principles of Fair Information Practice (FIP) and EU data protection should be preserved when using crisis informatics. For

instance, improving the data quality (data format, taxonomy, clarity, etc.) in disaster response operation is must. On the other hand, if crisis responders, researchers and academia fail to develop proper standards, guidelines and practices to facilitate the exchange and transferability of data between groups and individuals, this will also add further risks.

4.1.3 Lack of coordination: Another important risk in crowdsourcing for humanitarian crisis management is the absence of a common mechanism specifically designed for collaboration and coordination between different agencies working for disaster response cause [72]. Also a common platform for humanitarian crisis response coordination work among different stakeholders engaged in crisis response management work is missing. Using crowdsourcing for humanitarian crisis management would not get the optimum response without such type common platform for collaboration and coordination. The United Nations suggested as 'several actors including NATO, OGC, ISPRS and GEO are working on similar issues and could be integrated in a concerted effort' [73].

4.1.4 False positives, automatic decision-making: Last but not least, decision support systems soon will replace volunteers as a source of information, selection and response teams' support. These automatic decision support tools will generate a number of false positives and might in some cases even substitute expert's decision-making. However, in the legal field, a decision cannot be solely based on automatic tools. This general principle shall also apply for crisis informatics.

As some risks have already been identified, it is time to take a look how they are linked with the tasks conducted by online volunteers in crisis management:

4.2 Tasks of Online Volunteers and Risks

4.2.1 Data retrieval and selection: Collection and filtering can be done by digital volunteers. They contribute in achieving collective task solving and crisis mapping. It can also be implemented by using data analytics, like social network analysis, user ranking, machine learning, sensors and ultimate meta-data crisis mapping. However, security and privacy risks re very much associated with data retrieval and selection processes.

4.2.2 Situational awareness: On the other hand, situational awareness is offered by human sensors, support teams and humanitarian networks. Now, digital volunteers are more organized than in the past. But these networks trigger new risks. Coordination between response teams and digital volunteers, and also ad hoc solution teams created by digital communities are the risks related to situational awareness tasks.

4.2.3 Decision support: The last group of tasks involves decision-making support: OCHA and the Digital Humanitarian Network coordinate to offer decision support. This can be considered as coordination risk. On the contrary, simulation, geomatics and emotion classification will become a decision support tool for response teams very soon. It is at this stage when false positives might be more dangerous.

4.3 Data retrieval and selection concerns

Current crisis crowdsourcing platforms suggest collective task solving for volunteers. Some disaster response networks like Digital Humanitarian Network (DHN) offer these resulting tools to volunteer communities and response teams. In sum, crowdsourcing remains a source of information, but is quickly becoming a training procedure for data analytics. These complex disaster management networks need to preserve security and privacy, not only for the traditional crowdsourcing of data, but also for new automatic retrieval and selection capabilities.

4.3.1 Collective task-solving and mapping

Upon filtering the relevant data, crowdsourcing crisis informatics has proved to be useful for response teams. Only near-real-time and highly accurate information is required for response teams. Duplicate reports and unavailability of essential information are added problems for response teams [74]. Crowdsourcing crisis mappers want to offer useful and relevant information, which also needs to be identified as trustworthy partner in officially decision-making process for emergency management. Most of the crisis-mapping deployments lack enough accuracy of crowdsourced data compared with more ‘traditional data’. The quality of data from 2008 to 2011 has shifted from trustworthiness to “good enough” [75]. More recently, crisis informatics based on data analytics offer new trust options. Some risks are also due to the absence of data validation from end-users, gaps in reporting back on on-going emergencies and lack of publicity of crowdsourcing activities [73]. There are ways to minimize those risks. Firstly, filtering the data, i.e.

asking where the information originates from. Secondly, cross checking the collected data with other data sources. Thirdly, by setting up guidelines where the crowd verifies the crowd, respecting transparency and open data policies and practices [73].

Inaccuracy and bellow quality of data are not only crisis mapping risks; security needs also to be preserved. Recent studies suggest that humanitarian organisations have a long way to go to ensure a sufficient level of technical security against cyber-attacks [76]. The same applies in using crowdsourcing tools or methodologies for humanitarian crisis management as well. Gao et al. [74] suggest that crowdsourcing tools for crisis response management do not have adequate security features for users and reporters, registered users, relief organizations, and relief operations. Online activities of humanitarian organisations are highly vulnerable to cyber-attacks [76].There are reliable reports of human rights activists and other 'people communicating with humanitarian organisations over Skype being tortured to give up their passwords, with their accounts then used to transmit malware to NGO staff and their contact networks' [76,77]. Different social media page of the International Secretariat of Amnesty International faced nuisance cyber-attacks in 2011 by Syrian Electronic Army. One of the several examples is the nuisance attack was on a crowdmap platform that was developed by the Amnesty International. Syrian Electronic Army used to send spams in every other minute.[42] The same 'Syrian Electronic Army' did the same to Human Rights Watch [78]. In the case of

[42] This was the personal experience of this researcher as he was then employed at the IS as an Online Communities Officer.

crowdsourcing for humanitarian crisis management, 'attempts to steal data or to spy on a target are probably the greatest concern since they can endanger assisted people and aid workers' [71]. Another risk of using crowdsourcing for humanitarian crisis management is that in the present 'network-age', governments have access to sophisticated interception and surveillance software[43]. Thus, all these facts pose difficult challenges for humanitarian crisis response workers, especially for those are working with digital platforms including crowdsourcing tools and platforms. Humanitarian aid workers on the ground and other workers need to consider several risks. Network access and system continuity management are sensitive aspects to protect [79]. Trusted network access, with authentication of users and encryption might provide the required security. Some secured data backups would add new safeguards. The information gathering also needs security measures like a privacy-preserving information system and an authenticated broadcasting.

Other risks are due to personal information disclosure and location data management [79, 80]. For example, publicizing the details of victims, users, relief efforts etc. can put people associated with a particular crowdsourcing effort in danger. Easy procedures like mask up or forwarding, and more complicated ones like obfuscation and

[43] The Blue Coat Packetshaper, a type of malware used for this type of surveillance, was found in Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela, according to research done by the Citizen Lab at the University of Toronto. For more information, see Planet Blue Coat: Mapping Global Censorship and Surveillance Tools, 15 November 2014. Available at https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

perturbation might be considered. Health information is sensitive data, and should thus be even more protected. Gender discrimination might also be present in crisis informatics. The rate of female staff in disaster management sections is only 5-10 per cent. Gender equality centres can help gender perspectives to be included in disaster management [81].

4.3.2 Risks related to retrieving and selection with crowdsourced data analytics

Accurate and relevant information can be selected by trained volunteers. But automated data collection and selection are increasingly used in crisis informatics. For instance, social networks data mining, user ranking, information automatic classification and sensors are examples of partial or complete automatic retrieving and selection.

A. Social network data mining risks

Social networks data mining can help extracting data from the public pages on emergency platforms. Security, access controls, and privacy are weak by design on most social networks because their popularity and commercial value hinge upon their easy and open access to all Internet users [82]. As Social Media Platforms provide open and easy access, their users take many unconscious risks by publicly disseminating personal communication, personal information and images etc.

The quality of data depends heavily on data providers' profiles. Some 'general' crowd and subgroups of trusted volunteers provide data during crisis management work. There are potential risks for registered users as those volunteers have to provide personal information to create

their profiles. Providing too much information while creating profiles is highly risky dangerous in terms of privacy, security and personal data protection. Thus, data mining after setting up guidelines where the crowd i.e. digital volunteers verify data, respecting transparency, rights and open data policies and practices could be the solution [73].

However, by publicly announcing the 'trust' level of Social Networking Sites could reduce some risks mentioned earlier. Tech companies should develop tools with Privacy Enhancing Technologies (PET) integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as 'anonymous'. Private companies also should not illegally collect data in the form of online survey, using third party apps etc. from any online platforms including crowdsourcing platforms. Such type of illegal collection of personal data should be punishable by the law [83].

B. User Ranking and content classification risks

Numbers of crowdsourcing platforms have ranking systems for their registered users, *i.e* trust in people first, then in data [75]. These platforms calculate users' activities like, the number of reports submitted or bookmarked, or successful or unsuccessful matches have been extracted and used to label the user as active or not, and as effective or not. To identify active users, users were ranked based on the number of their likes, comments and posts. Active and effective users are thus preferred when taking into account the relevance and accuracy of data. On the other hand, high ranking volunteers were not always highly trustworthy participants in crowdsourcing crisis

management activities. So, when they select and rank a crisis incident, they might do mistakes. Some participants can provide misleading information intentionally. In such type of cases, data is not cross checked among different sources and thus not validated. So, in such cases, a total accuracy is not possible.

In crowdsourcing crisis informatics, machine learning has been used to evaluate trustworthiness of Tweets automatically and within seconds. In Artificial Intelligence Disaster Response (AIDR), Twitter messages are classified by at least three volunteers. MicroMappers also combines volunteer filtering with machine learning on a "Text-Clicker" option. However, it has been noticed in some cases that ranking or scoring data using Machine Learning techniques is not hundred percent accurate at all time. To address the issues of content classification risks, crowdsourcing crisis coordinators should cross check crowdsourced data with other sources and finally, tally the analytics of data between digital volunteers and machines.

C. Risks associated with sensors

Valuable Information can be also crowdsourced by using mobile sensors. Geo-location information and other relevant data are sent to remote databases where machine learning takes place. However, wrong information gathering could also happen with sensors.

There are also some major privacy concerns due to the fact that sensors have the potential to detect levels of detail that were impossible earlier. As sensors have the ability to routinely gather data at a particular point or land mark, privacy suddenly becomes a major concern as sensors has

potential to gather unwanted data as well. This privacy dimension is informational and ‘relates to those attributes, activities, or information that an individual may wish to conceal from others’ [84]. Sensors may collect data on locations and habits of people and gathered data could be correlated with data coming from sensors from the real world. Thus, knowledge base virtual world contain pervasive information revealing individuals’ habits, routines, or decisions [85]. Secondly, as gathering and manipulating information is a form of power in a global information economy [86]; enterprises can control data collections and knowledge bases. Thirdly, some oppressive governments also keep such data into their system to ‘prevent’ future crisis.

To deal risks associated with sensors, a safe-use framework should be developed and illegally collection of personal data should be made punishable by the law of the land [83].

D. Situational awareness risks

Generally, crisis management increasingly adds context information. It is called situation awareness and can be provided by individual volunteers and crisis communities, but also by situation awareness systems or risk estimation. The diversity of crisis situations which originated from different events and the variety of users and tools have in fact led crisis management organizations and crisis management coordinators to face specific risks covering different areas, including situational awareness, data visualization, (geo)visual analytics, visual representations, advanced (mobile) interfaces, communication technology and collaborative approach among

different volunteer communities [87].

E. Situational awareness provided by volunteers and communities

Virtual volunteers usually employ group chat and Skype conversations and also some crisis informatics are now offering management tools to these small support teams [88]. Volunteers provide geo-referenced information, like sensors would do, to contribute to crisis situational awareness. Accessing users' live video streaming, personal image updates, geo-location etc. can be effective for support teams in discovering the actual incident and selecting relevant data to allow emergency response teams improve their situational awareness [89], however, by accessing such activities of users' could infringe individual privacy. Real-time updates from users of location-based services, like microblogs, for instance create time-stamped and geo-located data using smart phones with GPS [90], also have a potential adverse perspective in terms of right to privacy and security. Some crowdsourcing tools force users to revel their geo-location information. For example, the crowd control LEEDIR (Large Emergency Event Digital Information Repository) demands access to GPS data and when images and video are uploaded using the LEEDIR application [91].

Sometimes, crisis responders are not highly trained with the use of emerging technologies. For example, in Spain, fire fighters use sensors during bush fires. They really cannot concentrate on sending temperature update using sensors as they concentrate in controlling bush fires. Sometimes, they left the sensor in one particular location

and try to control bush fires in a different location. So, in such cases sensors are unable to send accurate information. In their research on collaboration exercises during rescue operation in Sweden, Berlin et. al (2014) identified, 'Organizations worked sequentially and in parallel but without common coordination' [92].

The issue of reporting information can be ‘altered or restricted depending on the nature of the disaster in question, especially where there is lack of interagency communication’ [93]. Real-time reporting of crisis is extremely useful but may cause another problem. For example, volunteers want to contribute but they work on ad-hoc basis. This happens because of the lack of coordination. As all volunteers are not expert, they cannot follow coordinators’ indication during crisis management work, while time management is one of the most important issues in any disaster. In most of the cases, crisis coordinators develop some predefined categories to identify the right information. However, predefined categories may risk excluding useful contents failing to capture contextual tone of the text [94]. Thus, lack of coordination is a major problem in implementing a successful disaster management process among inter-agencies involved [95].

Many disaster evaluation reports mention the issues like disconnects between relief organizations and local communities, a lack of information sharing between organizations, misalignment between needs and recovery actions, and sub-optimal decision making etc [96]. When disasters occur, organizations like the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) must quickly make

decisions based on the most complete information of the situation they are able to obtain. They are responsible for organizing search and rescue operations, emergency food assistance, and similar tasks [97]. Normally, volunteer organisations are in charge of providing situational awareness during disasters. Organizations like the OCHA and other traditional organizations are able to submit a request and rely on the Digital Humanitarian Network to build a solution team with the relevant volunteer members within the volunteer communities.

Different information management officers (IMOs) and humanitarian affairs **o**fficers **(**HAOs**)** of the OCHA have different skill sets, but as a group, they are tasked with gathering data, liaising with various cluster leaders, communicating with volunteers, updating databases and common data repositories, and producing a variety of documents. In the immediate aftermath of a disaster, they often experience "ad-hoc craziness" brought on by a need to complete myriad tasks in a short period of time [98]. This core solution support team decides on different aspects of crisis response works. However**,** current decision making support systems and frameworks do not appear to sufficiently handle dynamic decision-making supports in the contexts of any large-scale disaster situations [99].

Apart from this, there are concerns with the reliability and accuracy of crowdsourced data. In crowdsourcing, **'**while lower levels of abstraction (e.g., tweets with individual requests and specific local references) risk overwhelming the human reviewer, high levels of abstraction risk denying a role for human interpretation' [94]. As of

now, there is no mechanism to demonstrate the accuracy of crowdsourced data after comparing with more 'traditional data' and also to document the efforts made on the evaluation and verification of the crowdsourced data. So far, just an example of a joint verification of data has been identified in Indonesia which was set up between Open Street Map, NGOs and the Government to build a stronger level of confidence [73]. Though, the organizations involved in crisis response work use social media to disseminate important information during crises, but government institutions and other established entities should use social media as a tool to disseminate information, so that users would rely on such trusted sources. Other risk is that even though numbers of organizations, donors, other partners work in a particular crisis, they do not take decisions together or work together on the same issue. If Ushahidi is working on such a crowdsourcing platform and OCHA/UNHCR has also developed a common platform - it is wastage of human resource, money and time. Such types of approaches by organizations bring less trust among citizens and individual crisis response platforms become more vulnerable and criminals can take the opportunities of this vulnerability.

Crowdfunding is one of the common functionalities for crisis management activities. Crisis victim communities can seek funds using crowdfunding channels and crowdfunding scams can take on many different ways. There have been several incidents that have raised concerns about crowdfunding [100]. Apart from this, some information that humanitarians collect could be valuable to criminals. Account information for cash transfers is an obvious target, but other types of

data may have value for insurance fraud, identify theft, or corruption [71].

On the other hand, collaboration between professional organizations is a major issue in disaster recovery. Duffy (Ed.) identified that the 'current state-of-the-art in technological support for recovery activities reflect the same variety, increasing the risk of misinformation and collaboration gaps. Each professional organization uses its' own support tools (e.g. EU platform GDACS; Global Disaster Alert Coordination System) which are not shared' and it has also been identified the reason is that due to competition for scarce funding. [96] To deal such decision making support risks, a general framework for context-aware multi-party coordination systems proposed by Way, and Yuan (2013) could be the answer which can be used to enhance the current understanding of emergency response systems as well as support situations requiring dynamic decision making for managing large complex crisis by multiple stakeholders [99].

F. Situational Awareness Services and risk estimation

In crowdsourced data, consent is very critical. As it has been mentioned earlier that when third party gather information about victims through VAVs or Satellites; or even try to gather reports something like, 'xyz' has been molested by the opposition group members etc. could be really problematic. Because of online nature of crowdsourced data and complex crisis environment, it is not possible all time to maintain the ethical principles of 'Not to Harm'. Larrauri describes, "Humanitarian actors at times argue that the imperative to save lives trumps the need

for consent in certain situations and / or at certain levels of data aggregation". Recognising the importance of the argument, the author questions further, 'but how applicable is it to collecting data on civilian protection' as 'it is much harder to draw the line on what is life-threatening in a conflict context' [101]. Larrauri argues that 'there is significant trauma among local populations who have witnessed drone strikes that appeared to come from nowhere' as residents in conflict regions fear humanitarian UAVs as threatening military equipment. Humanitarian organisations need to address this issue speedily to have the best positive outcome of using UAVs in humanitarian crisis management.

Situational Awareness is a prerequisite for decision-making, and Decision support systems [102]. The advent of new technologies has changed the landscape of crowdsourcing crisis informatics considerably in recent years. The increasing trends of using different digital tools for humanitarian crisis management, crowdsourcing tool coordinators started giving more emphasis on smart technologies and frameworks in crisis management work. With readily available software platforms and tools such as online discussion platforms and news aggregators; different crowdsourcing platforms like GroupSourcing, Crisis Response Game, Use of Linked Open Data for crisis management, Digital Governance Framework for Crisis Management, Interactive 'Crowdsourcing Unheard Voices' Platform for Crisis Reporting, AIDR Use of satellite images by Amnesty International and use of Unmanned Aerial Vehicles (UAVs) [103, 104, 105, 106, 107, 108, 109, 110, 111, 112]. Though, organisations can now disseminate, acquire and analyse

information more efficiently and comprehensively, there are some potential risks in using only machines for risk estimation as machines can do mistakes as well. On the other hand, well-skilled response team may still have better trust in their knowledge and experience than determine risks levels using only automatic tools. So, in decision-making for crisis governance work, the combination of machines and unskilled and semi-skilled operators could be risky. So, if humanitarian crisis response workers and others associated with humanitarian crisis work are not careful enough, their digital platforms including crowdsourcing platforms, 'their data systems, particularly biometrics or other individual or household level registration tools, can be co-opted into becoming an extension of state surveillance, even after a crisis ends' [71].

However, there are some ways to be safe and protected while working in crisis period. Firstly, law enforcement agencies should not monitor crowdsourcing process for crisis governance to identify 'evidences' illegally in the suspicion of future terrorist attacks or conflicts (in man-made crisis). For counter-terrorism purpose governments could do so with prior judicial authorizations. Secondly, crisis response coordinators must collect and handle information containing personal details in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection. Thirdly, they should establish standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection. Fourthly, crisis

governance coordinators must not use any digital tool that has potential risk of security breach and finally, they must develop guidelines for the crisis reporters and other users including journalists.

G. Decision support risks

The collection, analysis and interpretation of the earth's surface data for crisis management create some absolute risks. Like other aspects of crisis management activities, geomatics also has some general risks that include the security and privacy of a particular area and population of that area. For instance, earthquake, tsunamis and floods forecasting and modelling through remote sensing and geodetic data allows providing both long-term planning as well as short-term identification of most damaged areas [113, 114, 115]. Data mining and statistics on past events can also be useful for this purpose [116, 117].

Simulations are also increasingly used. For instance, modeling the movement of people until they escape from a hazard, *i.e.* activity recognition, can also be decision support systems for disaster management. Thus mapping and evacuation planning under uncertainty, based on these simulations, are theoretically available [118, 119]. Fire detection has also being a preferred field for simulations. Since 2000 decision support systems help fire detection, reduce false alarms, offer fire data analysis and predict future fires [120]. Simulation is also suggested for floods management [121].

Rapid mapping[44] is another valuable data analytics technique for

[44] On-demand and quick mapping (within hours or days) of geospatial information immediately after an emergency event. See more at http://bit.ly/1PyOvGs.

disaster management [122]. However, some features of rapid mapping can bring huge risks to the community, volunteers and victims of disasters. For instance, part of the map production is based on automatic affected population estimations or potential infrastructure damages evaluation. Obviously, this is only possible when there are areas with detailed reference datasets available, otherwise *ad-hoc* crowdsourced mapping would be necessary and that is not the ideal situation.

One of the exciting emerging techniques is being used during crisis response work is 'Sentiment Analysis'[45]. For instance, emotional behaviour simulations provide better assessments for emergency evacuations [123]. This natural language processing, text analysis and computational linguistics has the potential to provide wrong data analytics. Secondly, as this process uses some latest data mining techniques, there is huge chance for an individual to be exposed in public. So, this technique could violate right to privacy.

Along with security, privacy and data protection risks, the other risk of unlawful surveillance on decision support system also an important threat. The collection, analysis and interpretation of the earth's surface data for crisis management create some absolute risks. In terms of image analytics, it can also start with volunteer identification of objects and places, and then use data analytics or be available for expert

[45] Sentiment analysis is also known as opinion mining. It refers to the use of natural language processing, text analysis and computational linguistics to identify and extract subjective information in source materials.

response teams[46]. Here, the risk is, most of the cases volunteers do not gave proper consent to use images of a vital set up or information about an unknown individual and so far, there is very little safeguard to protect someone's data and privacy.

Crisis coordinators should use tools with PET[47] integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as 'anonymous'. On the other hand, crowdsourcing reporters in humanitarian crisis must ask for options to be 'anonymous'; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as users will be able to apply these options if needed.

H. Automatic decision and false positives

Use of automatic tools in crisis response work is extremely helpful if tools give the correct information. However, making decisions solely based on automatic crowdsourcing tools is highly risky. For example, forest fire spread predictions can successfully be assessed by using already gathered crowdsourced data through decision support systems. Such tools will not be effective if they fail to run quickly and on time. In different crisis response initiatives, real-time information is very helpful for making a decision. However, automatic decision systems lack the full trust.

To the best of our knowledge there is no concrete ruling of automatic decision and false positives. Nonetheless, some general principles

[46] For more, please visit http://www.tomnod.com
[47] Privacy Enhancing Technologies

issued from privacy and data protection are available. For instance, in one Opinion on Drones, the Article 29 of Data Protection Working Party offered some worthy recommendations [124]. Using drones for decision support system is a good example because they have visual recording and detection equipment. Several risks are highlighted in terms of safety, third party liability, privacy and "chilling effect", *i.e.* the legitimate exercise of civil liberties and rights. Some suggested privacy by design solutions are envisioned like processing the images by using blurring or other graphical effects, so as to avoid unnecessary identification of people. More interesting for our purpose are the recommendations for law enforcement reasons. Crisis management, likewise law enforcement, is an example of legitimate purpose. Even though, they should respect general privacy principles: necessity, proportionality, data minimisation, strict and restricted retention period. Also, there is a concrete principle directly related to automatic decision-making: the prohibition of automated enforcement of decisions solely based on machines. In other words, the data processed via automatic decision support systems should be further scrutinised by a human first response expert before any decisions adversely affecting an individual is made. Courts should also be able to review the decision-making process. Some internal and external supervisor should eventually check the compliant use of the system according to an *ad hoc* legal framework.

4.3.3 Possible Solutions

To sum up, the identified legal and ethical risks of crowdsourcing crisis informatics could be divided into three stages. The stages are:

- Retrieval and Selection;
- Situational Awareness; and
- Decision Support System.

A brief mention of possible solutions is being presented here in a form of table. No explanatory text about these solutions is being provided here will be given as an extensive explanation is given in the next chapter i.e. Chapter V.

A. Retrieval and Selection (RS)

Retrieval and Selection by Volunteers	
Risks	**Possible Solutions**
Security breaks: cyber-attacks, nuisance attacks Mass surveillance	Trusted network access, authentication, encryption, data backups, privacy-preserving information systems authentication broadcasting
Quality and accuracy of data	Filtering, cross-checking, verification by the crowd
Personal Information Disclosure, location management, sensitive data	Mask up, forwarding, obfuscation, perturbation, Additional safeguards for sensitive data.
Retrieval and Selection by Data Analysis	
Risks	**Possible Solutions**
Profiling with data mining	Privacy preserving data mining Privacy Enhancing Technologies (PET)
Geolocation using sensors	PET for geolocation
User ranking and content classification	Cross-checking

B. Situational Awareness (SA)

Risks	Possible Solutions
Situational Awareness by Volunteers	
Geo-referenced information	PET for geolocation
Lack of coordination between experts and volunteers	Solution Support Teams
Lack of collaboration between agencies	Context-aware multi-party coordination systems
Situational Awareness by Data Analytics	
Non-acceptance of SA services by users	Purpose limitation (only for disaster management)
Information collection and storage	Privacy Enhancing Technologies

C. Decision Support Systems (DSS)

Risks	Possible Solutions
Reliability	Cross-Checking
Decision adversely affecting humans solely based on automatic DSS	First response team monitoring and cross-checking
Traceability of the automatic decision	Logs and internal and external supervision

V. Ethical and Legal Recommendations for Crowdsourcing Crisis Platforms

In the previous chapter, various positive aspects of crowdsourcing have already been recognized; serious concerns have also been raised in terms of privacy, security and personal data protection in using crowdsourcing during any crisis. We have identified several ethical and legal concerns in terms of privacy, data protection and security of crowdsourcing during crisis governance work. Earlier, we also discussed about the Sendai Framework for Disaster Risk Reduction 2015-2030. This chapter aims to present solutions of those identified risks in form of a general recommendations for crowdsourcing crisis management. It includes legal, ethical and technical recommendations for crowdsourcing disaster management.

The Sendai Framework for Disaster Risk Reduction 2015-2030 did not use a single word on the potential risks of using emerging ICTs and crowdsourcing in disaster management [125]. We present here some solutions in form of general recommendations for crowdsourcing crisis management. It includes legal, ethical and technical recommendations.

The United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER) in a report on Crowdsource Mapping for Disaster Risk Management and Emergency Response developed during the International Expert Meeting in February 2013 discussed about the use of crowdsourcing,

issues and potential steps to take to deal with some existing issues [126]. Different positive aspects of crowdsourcing have already been recognized, serious concerns have also been raised in terms of privacy, security and personal data protection in using crowdsourcing during any crisis. We have already identified several ethical and legal concerns in terms of privacy, data protection and security of crowdsourcing. Thus, during our research work conducted on crowdsourcing crisis management platforms, we also tried to understand possible solutions of different concerns that already been identified.

In the earlier chapter, we have mentioned some risks. During the research on crowdsourcing tools and platforms, the following four overall categories of risks have been identified.

A) Security breach due to system malfunction or insecure data transmission;

B) Personal Information Disclosure, location data management, sensitive data (health), quality of data and discrimination;

C) Lack of coordination; and

D) False positives, automatic decision-making.

These risks are directly or indirectly linked to the tasks that volunteers do in three different phases (i.e. a) Data Retrieval and Selection; b) Situational Awareness; and c) Decision Support) in using crowdsourcing for crisis management. To tackle these identified risks, a risk-solution general recommendations are being proposed.

5.1 Ethical and Legal Solutions for Data Retrieval and Selection

5.1.1 Security Breach

Crowdsourcing crisis platforms should add security measures to their services. System continuity management, network access and information gathering/broadcasting are three areas to protect [127]. We start with system continuity management. Servers can be damaged in a disaster. Thus, cloud architectures could preserve servers from physical damage. However, but this leads to cloud computing services risks: secure computation, data backups and user authentication [127]. As a general rule, the computation is secure if the platform provider cannot obtain any information from the execution environment such as physical memory. Software protection in cloud computing or monitoring insider activities achieves secure computation. On the other hand, a backup service is secure if it encrypts and has an efficient access control. Local authentication is a risk and can be complemented by delegated authentication [127]. The LifeNet Project [128] is free open-source software that connects devices to obtain *ad hoc* networks without any infrastructure. But then general authentication mechanisms are difficult or even impossible [127]. A Trust network access should thus be based on distributed trust computations and it could be evaluated according to trust metrics [127, 129]. Centralising all the information in a server does not seem the most flexible and robust option. It is better to consider distributed and dynamic architectures for the platform. Information gathering/broadcasting services need first a location data management

[127, 1297]. Obfuscation, perturbation or anonymization of location information protects privacy in this case. Location perturbation blurs the concrete location by clustering with other users (k-anonymity). Strong authentication of streaming data would be the last measure to adopt. Digital signatures and hash values detect alteration and masquerading [127].

5.1.2 Quality and Accuracy of Data

In the crisis domain, identifying the authenticity of information posted on social media is a major concern for those who process information and also for users [130]. One way to preserve quality of data is using experienced users that verify the information. This filtering reduces the amount of information and confirms that trust first begins with people and not with data [131]. Thus, cross checking is required before uploading data to crisis platforms. This is even more important if it is envisioned as information ready for first-response teams' decision-making. Information platforms and decision-support tools are converging and data's accuracy can sometimes be as important as recommendations for the decision-making process that might be based on it. Data accuracy is the very first stage of decision-making.

5.1.3 Personal Information Disclosure

The EC Data Protection Directive -also known as Directive 95/46/EC- can be useful for personal information disclosure. It has now become a truly international standard for data protection [132]. Moreover, the Article 29 Data Protection Working Party (WP), an independent

European advisory body on data protection and privacy [133] has adopted some interesting reports like WP199, WP203, WP211, WP216, WP221, WP223, and WP228. They provide some legal guidance for personal information disclosure, location management and sensitive data protection (adapted from WP 223):

- *Notices or warnings should be designed to frequently remind users that sensors are collecting data*
- *Applications should facilitate the exercise of data subject rights of access, modification and deletion of personal information.*
- *Application developers should provide tools so that data-subjects can export both raw and/or aggregated data in a standard and usable format.*
- *Developers should pay special attention to the types of data being processed and to the possibility of inferring sensitive personal data from them.*
- *Application developers should apply a data minimisation principle. When the purpose can be achieved using aggregated data, developers should not access the raw data. More generally, developers should follow Privacy by Design approach and minimise the amount of collected data to that required to provide the service.*

5.1.4 Location management and sensitive data

PET for geolocation and cross-checking are also needed. For example, a simple model based on the frequency of mobile phone calls between two

locations and their geographical distance incorporating the social dimension of mobility can avoid potential geo-location privacy problems [134]. Sensitive information datasets need additional safeguards. One way to protect it is k-anonymity, a method that alters data in a way that it is not distinguishable from at least k-1 other records in the same dataset. As a result, data is anonymized and privacy is preserved [135].

5.1.5 Profiling with data mining

WP199 and Opinion 08/2012 also provide further input on the data protection reform discussion. For instance, the rule is that "*Every natural person shall have the right not to be subject to a measure which produces legal effects ... or significantly affects this natural person ... intended to evaluate certain personal aspects ... or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability, behaviour.* The exception is that profiling is allowed when it *is carried out in the course of entering into (…) a contract, with (…) safeguards (…) such as the right to obtain human intervention (a), is expressly authorized by a Union or Member State law (…) (b) or is based on the data subject's consent (c).* In any case, Privacy-Enhancing Technologies (PET), like Privacy preserving data mining, are needed.

5.1.6 Geolocation using sensors

The detection of building damages, for instance, can be measured automatically, with remote sensing [136]. This technique provides a

rapid evaluation of density and intensity of damage, and might be crucial for areas that may not be accessible on the ground. The results are so far less accurate than a manual mapping and might be relatively time-consuming and need a specialist. For instance, it would be misleading to simply plotting points on a map and assuming a direct relationship between the location of tweets and the disaster events [137]. One way to solve this issue is to complement the retrieving activity with a human or automatic situation awareness described below. More data does not always means more accurate and better information. A multi-method approach for collection and classification is often considered better than only trusting statistics [138].

5.1.7 User Ranking and Content Classification

Accuracy or quality assessment is also a major challenge for data analytics. For example, algorithms are being used to detect false product reviews and deployed by most major online retailers [139]. In the case of information classification, it is possible to use automatic classification to filter out content that is unlikely to be considered credible [140] or to annotate messages seen by users with credibility scores automatically [141]. Quality assessment for crowdsourcing disaster information is one of the main research areas of the EU FP7 research project EmerGent [142]. The quality assessment called Social Haystack starts with keyword queries for content on social media. Then it uses natural language processing (NLP) to enrich semantically the data with geo-location. It has also an interface to show the results of the searches to the user.

5.2 Solutions for Lack of Coordination related to Situational Awareness

5.2.1 Lack of coordination between experts and volunteers

During the coordination work, the public itself can be mobilized to confirm or discredit a claim through crowdsourcing [143]. At the time of crisis response work using crowdsourcing platform after the devastating earthquake in Haiti in January 2010, there was no common information system for coordination that could be shared by all of the groups providing resources for the response. In Haiti, both government and non-government organizations provided resources for the crisis response initiative without a common information system for coordination that could be shared by all of the groups providing resources for the response [11]. Though, using social media during disasters is an important first step with strong focus on situational awareness but might not be enough for emergency management. As during an emergency, social media are used as an information source in order to make decisions, the '*next-generation systems should be designed and evaluated in terms of their decision-support capabilities*' which ' *might even include forecasting using signals from social media*' [140]. Crowdsourced applications also have lacked the ability to efficiently provide a mechanism to help coordinate responses during a crisis [11]. The process of crowdfeeding is another way that is being applied in crisis governance. For example, Ushahidi has introduced the notion of "crowdfeeding" as part of a "Get Alerts" feature that allows the crowd itself to subscribe to crowdsourced crisis alerts via automated text messages and emails [11]. Thus, governments or different Law Enforcement Agencies could potentially keep an eye on a particular

platform to know more about any initiative and to get the first 'clue' about individuals who are contributing to the crowdsourcing initiative. Considering the numbers of reasons, user-centric platform design is the most powerful way to minimize the gap in coordination between experts and volunteers during crisis and also to know the usefulness and usability of those systems. The user-centric platform should answer at least the following questions: firstly, '*how should information be presented to users*' and secondly, '*how should users interact with it*'? '*The key to answering these question lies with the users themselves, who should be brought into the process of designing the systems, dashboards, and/or visualizations that they require to serve their needs*' [140].

5.2.2 Lack of collaboration among agencies

The conversation among common mass, volunteers and formal agencies can be conducted through crowdsourcing platforms that, instead of passively waiting for people to post information, ask them directly to answer certain questions that are relevant for the emergency response or relief operations [144]. An innovative crowdsourcing tool CrowdMonitor assessed digital and physical activities of citizens [145]. On the other hand, SUPER (Social sensors for secuUrity assessments and Proactive EmeRgencies management) aimed to develop technologies to aid in the real- time management of emergencies using social media. As researchers feel that leveraging social media can provide tangible benefits during emergency and security response situations, researchers have identified how this might be achieved in

terms of event mitigation, increasing preparedness and during response and recovery based on feedback from real emergency-response organizations [146].

Computational methods can be applied to enhance the information in a number of ways. For example, hashtags can be used not only to help formal response agencies choose which hashtags to use but, more generally, to help them design and evaluate effective communication strategies in social media [147]. Matching problem-tweets to solution-tweets [148] and matching tweets that describe urgent need of resources in Disaster situation with tweets describing the intention to donate them [149].

A special issue of the Journal on Computer Supported Collaborative Work explores various ways that computing can support collaboration and coordination during an emergency [150]. Institutions in charge of disaster management "*often combine a hierarchical command structure with distributed teams on site and at regional command centres to better coordinate crisis response efforts in the impact zone. There are also a number of inter-organizational coordination mechanisms, but the resulting division of work is highly situational and thus difficult to anticipate requiring improvisation and pre-negotiated processes and routines*" [150].

Data from different sources should be processed and integrated: "*The strategies of emergency services organizations must also recognize the significant interweaving of social and other online media with conventional broadcast and print media*" [151]. There are some examples of the processing of other types of information items

during crises, including short messages (SMS), news articles in traditional news media and blogs and images [140]. Coordination work is widely perceived as an important function of crisis and disaster management, as the decision-making process in crisis depends on the success of the coordination work of any crisis. After analysing failures, Bion and other researchers have developed a crisis coordination framework [152]. Traditional coordination tools only based on *top/down* approaches, in their opinion, have limited applicability in high-velocity environments like disaster events. *Bottom/up* approaches or emergent coordination needs to be added to the former, provided it defines clear protocols and roles of *ad-hoc* teams, it combines differentiated communities and it engages in active knowledge sharing. As a result, we obtain a *collective decision-making process that is formal, consensus-oriented, and deliberative*, what is also called an *instant institutionalization* [152].

5.2.3. Solutions for Situational Awareness Services

Situational awareness is not only provided by volunteers. Disaster risk reduction is a growing interdisciplinary field with increasing presence of technologies. Prospective risk assessment is usually based on statistics, or a combination of empirical risk estimation and statistics. It estimates the evolution of the risk and the damages according to past disasters' evaluations [153, 154, 155, 156]. Those situational awareness and risk estimation services can eventually be considered decision support systems. But even if the risk estimation is not supporting automatically the decision-making

process, other concerns need to be faced. For instance, the non-acceptance of these technologies, like using drones for geolocation, has to be considered. In these cases, it is important to assure to the users and victims that the empirical information collected, will be only used for disaster management (purpose limitation). Some Privacy Enhancing Technologies should avoid further reutilisation of data without authorisation. Logs should also be available for internal and external oversight of the use of data.

5.3 Solutions for Decision Support Systems

Situation awareness is the first stage of decision-making. The use of ICT in disaster management increases the importance of decision support systems. Retrieving and selection tools are now more focussed on directly supporting first response teams, as detection of events [157]. This trend might be useful when facing easy cases with accurate information where quick decisions are required. Nonetheless, some events might not be easy to manage. For instance, information might be inaccurate, context and risk evaluation might be difficult or time-consuming and only experts might understand and properly use the decision support system. In these hard cases, some safeguards need to be implemented. Here we describe some tools and possible ways to proceed.

Empirical and statistical analysis of past events allows not only modelling the relevant context for situational awareness, but also using the resulting model for prediction of human disaster behaviour [158]. Victims without mobile phones and worldwide events have not being taken into consideration so far when building these human disaster

mobility patterns. In other cases the modelling is even more complicated, like agent-based models for crisis management supply chains [159]. Anyway, possible false positives and also successful technology with constitutive social effects are the risks to deal with.

The enrichment of micro-level context, situational awareness or resilience, seems to be more important than macro-level theories and causation [160]. No matter how much information we have, we might be confronted with new situations or we might have an irrelevant statistical correlation that leads to a false positive. Crosschecking and expert monitoring should never be replaced by these automatic support tools. Even if they can most of the time be deeply useful.

On the other side, a successful use of technology can also lead to risks for victims. This is the case for biometrics and disaster management [161]. Iris registration can for sure help refugees' repatriation, but the potential risks of biometrics for the implicated refugee population are not duly taken into consideration. Situational awareness and general recommendations should describe the conditions of secure biometrics for disaster management. Concrete legal and ethical recommendations are the best way to preserve both users' rights and allow efficient disaster management.

5.4 Ethical and Legal Solutions (General Recommendations)

As various risks have already been identified, it is natural that there will be various possible solutions.

- For any security breaks, cyber-attacks, nuisance attacks and mass surveillance risks - trusted network access, proper authentication,

encryption, data backups, privacy-preserving information and systems authentication broadcasting etc are important.

- For the issue of quality, reliability and accuracy of data - filtering, cross-checking, and verification by the crowd are useful.
- For personal information location disclosure, and management of sensitive data - Mask up, forwarding, obfuscation, perturbation; and additional safeguards for sensitive data are essential.
- For profiling with data mining, information collection and storage - privacy preserving data mining and use of Privacy Enhancing Technologies (PET) are important.
- For the use of geolocation and Geo-referenced Information, PET for geolocation is must.
- For 'user ranking' and 'content classification' - cross-checking is needed.
- For the lack of coordination between experts and volunteers - Solution Support Teams need to set up.
- For the lack of collaboration between agencies - context-aware multi-party coordination systems is essential.
- For non-acceptance of Situational Awareness services by users - Purpose limitation (only for disaster management) is needed.
- When decision adversely affecting humans solely based on automatic decision-making Support System - First response team monitoring and cross-checking is must
- For risks related to traceability of automatic decision making- Logs and internal and external supervision are must.

5.5 Concrete Recommendations for Crowdsourcing Crisis Management Platforms

Various risks have been described earlier. Now it demands possible solutions and concrete recommendations. In this section, a set of recommended solutions for existing crowdsourcing crisis management platforms will be developed. This would potentially address the legal, ethical and technical issues associated with existing crowdsourcing crisis management platforms.

5.5.1. Recommendations for Information / Data Retrieval, Selection and Storage

The following brief recommendations are for volunteers to uphold while supporting crisis management using crowdsourcing process.

Volunteers must collect and handle information containing personal details in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection [162].

A. Recommendations for Information / Data Retrieval

- Encryption technology should be integrated with the crowdsourcing platform
- Standard verification process by the crowd need to be established
- Data filtering facilities should be integrated with the crowdsourcing platform
- Privacy-preserving information systems authentication and broadcasting norms have to be applied
- Privacy preserving data mining procedures needs to be in place

- Tech companies that develop crowdsourcing tools that should publicly announce the 'trust' level of the tool.
- PET principles should be applied for determination of exact geolocation point of crisis reporters.
- Trusted network access for communication tools have to be established.

B. Recommendations for Information / Data Selection

- The authenticity of data needs to be identified by cross-checking available information.
- Two steps verification process needs to be done by the expert crowds i.e. volunteers.
- PET principles should be applied for determination of exact geolocation point of incident.
- Trusted network access for communication tools have to be established.

C. Recommendations Information / Data Storage

- Encryption technology should be integrated with the crowdsourcing platform
- PET enabled data backups facilities have to be developed
- Trusted network access for communication tools have to be established
- Additional safeguards must be ensured for sensitive personal data.
- Data should be stored in a locked cabinet.
- Crowdsourced data should be stored on a password protected and encrypted hard drive.

- The device should be in a locked room.
- Check data integrity of stored data files regularly.
- Use different formats of storage (e.g. hard disk/DVD)
- Label stored data in order to facilitating physical accessibility and location.
- Areas and rooms for storage of digital data should fit risk prevention regulations (e.g. flood and fire)
- Only responsible persons of core crisis response team members should have access to data.
- Enable secure remote access to confidential data but avoiding the possibility to download data.
- Publications regarding to the crisis response work must be conducted under the Statistical Disclosure Control carried out by a trained Service Staff.
- Data usage beyond the life of the crowdsourcing crisis management project must be closely supervised.
- Locking computer systems with a password and installing a firewall system are must.
- Servers should be protected through line-interactive uninterruptible power supply systems (UPS).
- Implementing password protection and control access to data files (e.g. no access, read only permission, administrator-only permission, etc.)
- Controlling access to restricted materials with encryption.
- Imposing non-disclosure agreements for managers or users of confidential data.

- Data transmitted should be encrypted, avoiding non-encrypted methods as e-mail, FTP protocol and so on.
- At the end of the crisis management project, data should be destroyed in a proper and consistent manner.
- Computers that contain sensitive data should not be shifted (e.g. a knock in a hard disk may provoke a failure causing a breach of security).
- Confidential data must be stored in a server without access to the Internet.
- Operating systems and anti-virus software in crowdsourcing platforms should be updated in order to avoid viruses and malicious codes.
- Backups can be stored offline (CD/DVD, pen-drive, removable hard-drive, etc.) or on a networked hard disk.
- If needed, devices that contain a backup can be moved to another place to keep it safe.
- Critical and sensitive data files should be backed-up daily, using an automated back-up process, preferably stored offline.
- Master copies of critical and sensitive files should be made in open formats which facilitate long-term usage.
- All back-up files should be validated regularly.

5.5.2. Recommendations for Situational Awareness: Coordination with volunteers and collaboration among agencies

Crisis management agencies must develop guidelines for the general users, crisis reporters and other users including journalists. A

common coordination platform between government agencies and NGOs should be developed to deal with in humanitarian crisis. Crowdsourcing reporters in humanitarian crisis must ask for options to be ‘anonymous’; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as reporters will be able to apply these options if needed.

A. Coordination with volunteers

- Crowdsourcing reporters in humanitarian crisis must ask for options to be ‘anonymous’; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as reporters will be able to apply these options if needed.

- PET principles should be applied for determination of exact geolocation point of crisis reporters.

- Trusted network access for communication tools have to be established.

- Need to maintain a detailed log of actions related to user accounts plus regular audits regarding their validity, access rights and roles.

- User actions at a particular crowdsourcing deployment database should be logged.

- Crisis governance coordinators must collect and handle information containing personal details in accordance with the rules

and principles of international law and other relevant regional or national laws on individual data protection.

- Crisis governance coordinators should establish standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection.

- Crisis governance coordinators must not use any digital tool that has potential risk of security breach.

- Crisis governance coordinators must develop guidelines for the crisis reporters and other users including journalists.

B. Collaboration among agencies

- Trusted network access for communication tools have to be established.
- PET should be applied for common coordination platform
- Establish and document a personal data breach handling procedure.
- Private companies should not be allowed to illegally collect data in the form of online survey, using third party apps etc. from any online platforms including crowdsourcing platforms. Such type of illegal collection of personal data should be punishable by laws.

- Disclosing of real names, locations of victims in man-made crisis should be banned by the law and should be applicable for all forms of media.

C. Collaboration between volunteers and different agencies

- A common coordination platform between government agencies and NGOs should be developed to deal with in humanitarian crisis.
- Media should develop their own 'Media Ethics' for crisis reporting with keeping in mind the privacy and security issues of victims.
- Trusted network access for communication tools have to be established.
- A specific procedure for the secure destruction of personal data should be established.
- Law enforcement agencies should not monitor crowdsourcing process for crisis governance to identify 'evidences' illegally in the suspicion of future terrorist attack or conflict (in man-made crisis).
- For counter-terrorism purpose governments could do so with prior judicial authorizations.
- The reuse will require quality control on the crowdsourced data.
- Some legal validation of the procedure will be required to reuse data.
- Internal and independent supervisory bodies should be implemented.

5.5.3. Recommendations for Decision Support Systems

Crisis coordinators should use tools with PET integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as 'anonymous'. On the other hand, crowdsourcing reporters in humanitarian crisis must ask for options to be 'anonymous'; not to disclose their location; and to

choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as users will be able to apply these options if needed.

A. Decision-making by human intelligence

- Solution Support Teams (SST) should be formed for every crisis response work.
- First response team should validate all information properly.
- Cross-Checking methodology should be in place to make decisions in a consistent manner.
- SST should keep logs available for internal and external supervision on regular interval.

B. Automatic decision-making

- Automatic cross-checking methodology should be in place.
- First response team monitoring and cross-checking tasks are must.
- Purpose limitation (only for disaster management) procedure have to be applied.
- A specific plan for upgrading hardware and software should be implemented.
- The use of system integrity tools should enable deletion and reporting of changes applied on servers.
- Automatic system alerts generating facilities need to be integrated
- Tech companies that develop crowdsourcing tools should publicly announce the 'trust' level of the tool.

- Tech companies should develop tools with PET integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as ‘anonymous’.

We presented potential solutions of various identified risks in form of general recommendations for crowdsourcing crisis management. These recommendations involved legal, ethical and technical aspects for crowdsourcing disaster management. In the next chapter i.e. Chapter VI, we would analyse some crowdsourcing platforms to understand how these platforms address various risk factors in compliance with the Priority Action 1 and Priority Action 2 of Sendai Framework for Disaster Risk Reduction 2015-2030.

VI. Crisis Management Platforms' Evaluation

In previous chapters we have provided detail risk scenarios and also potential solutions to those risks. Disaster risk reduction and data protection risks have been described, and general legal and ethical concerns and concrete recommendations have been suggested. In this chapter we are going to provide the result of research conducted on four different crowdsourcing platforms. As we mentioned chapters that this research work was conducted with two specific aims – how the Priority Action 1 of the Sendai Framework can be enhanced and how to contribute in fulfilling partially the Priority Action 2 of the Sendai Framework. So, in this chapter, we provide analytical information to see how various risk factors in acquiescence with the Priority Action 1 and Priority Action 2 of Sendai Framework for Disaster Risk Reduction 2015-2030 are addressed.

Though it has been mentioned earlier in detail the reason of selection of four[48] platforms, we are again providing the reasons in brief. Ushahidi (USH) has been selected because it is a pioneer in crowdsourcing platform, and many other platforms have used it as a reference for their own project. Digital Humanitarian Network (DHN) was also interesting due to the fact it was at the time of conducting the research the biggest network of volunteer and technical communities of its' kind to leverage digital networks in support of humanitarian response. On the other hand, MicroMappers (MM) was also relevant for its use of artificial intelligence to select data and information by users. Finally, the Google Crisis Map (GCP) was a good example of how some of these

[48] Uhahidi (USH), Digital Humanitarian Network (DHN), MicroMappers (MM) and Google Crisis Map (GCM)

platforms care about privacy, security and data protection issues of users during any crisis.

During the research, numbers of privacy, security and data protection issues were identified under these three stages i.e. a) Retrieval and Selection (RS); b) Situational Awareness (SA); and c) Decision Support Systems (DSS) of crowdsourcing. Some risks were common in all stages while others were not. Total 71 privacy, security and data protection risks were identified in three different stages. Total 40 risks in the stage one, total 20 risks in the stage two and in the stage three, total 11 risks were identified. As the research study was conducted among four different crowdsourcing crisis management platforms, numbers of tables will be presented in next pages to show the nature of potential risks associated with four crowdsourcing platforms; and at least one recommendation per risks will also be there in the tables.

6.1 Evaluation of the recommendations concerning retrieval, selection and storage

6.1.1 Information and data retrieval

It has been identified that no platform had the presence of encryption technology integrated properly. It is suggested that the encryption technology should be integrated with the all crowdsourcing platforms contributing in disaster management activities. Two of the four platforms studied used standard verification process and the other two used verification process partially. However, it is recommended to establish standard verification process.

- Three platforms had data filtering facilities and the other one had partially data filtering facilities. It is recommended that all crowdsoucing platforms should have data filtering facilities.
- In terms of privacy-preserving information systems authentication and broadcasting norms endorsement, no information found in any of the four platforms. Thus, it is recommended that 'privacy-preserving information systems authentication and broadcasting norms have to be applied in all crowdsourcing platforms.
- Privacy preserving data mining procedures were not available in two platforms and in two platforms the privacy preserving data mining procedures were present partially. It is recommended that the privacy preserving data mining procedures needs to be in place for all crowdsourcing platforms.
- No crowdsourcing platforms were using different tools those trust level were announced publicly by the developers. Thus it is recommended to tech companies that develop crowdsourcing tools should publicly announce the 'trust' level of the tool.
- PET principles in terms of geolocation identification were found partially in all platforms. It is highly suggested that PET principles should be applied for determination of exact geolocation point of crisis reporters.
- Three platforms were using trusted network access for communication tools and one was using partially. So, it recommended for all crowdsourcing platforms to use trusted network access for communication tools.

6.1.2 Information and data selection

When analysed risk scenarios in information and data selection process, we identified that out of four crowdsourcing platforms, two were using the procedure to cross-check data and information. Two of them were using two steps verification process and two of them were not using the two steps verification processes. All crowdsourcing platforms were using partially PET Principles in terms of geolocation identification and two platforms were using trusted network access for communication tools.

In terms of suggestions to secure data and communications in four platforms, it is proposed that the authenticity of data needs to be identified by cross-checking available information; two steps verification process needs to be done by the expert crowds i.e. volunteers; PET principles should be applied for determination of exact geolocation point of incident and finally, trusted network access for communication tools have to be established.

6.1.3 Information and data storage

When analyzing the risk scenarios, we identified that three platforms partially used encryption technology integration when they store data and information. Two platforms had PET enabled data backups; used trusted network access for communication tools and also used additional safeguards for sensitive personal data. One platform used all partially and one did not use a single safeguards. All four platforms used non-disclosure agreements for managers or users of confidential data. Two platforms partially used data beyond the life of the crisis. One of the four

platforms did not use and one used data beyond the life the crisis.

Most importantly, during the research no information found among any of the platforms on:

- Whether data stored in a locked cabinet or in a locked room;
- Whether data stored on a password protected and encrypted hard drive;
- Whether checking data integrity of stored data files happening regularly;
- Whether, using different formats of storage (e.g. hard disk/DVD);
- Whether in order to facilitating physical accessibility and location, the labeling of stored data is available;
- Whether areas and rooms for storage of digital data are fit with risk prevention regulations (e.g. flood and fire);
- Whether, only responsible persons have access to stored data;
- Whether, secure remote access to confidential data enabled but avoided the possibility to download data;
- Whether any research works are conducted under the Statistical Disclosure Control carried out by a trained Service Staff;
- Whether computer systems are locked with a password and installing a firewall system;
- Whether servers are protected through line-interactive uninterruptible power supply systems (UPS);
- Whether, implementation of password protection and control access to data files (e.g. no access, read only permission, administrator-only permission, etc.) are in place;

- Whether controlling access to restricted materials with encryption are in place;
- Whether, encrypted data transmission, avoiding non-encrypted methods as e-mail, FTP protocol and so on are present;
- Whether data destruction happening in a proper and consistent manner at the end of the crisis management project;
- Whether, confidential data stored in a server without access to the Internet;
- Whether, operating systems and anti-virus software in crowdsourcing platforms regularly updated in order to avoid viruses and malicious codes;
- Whether, backups stored offline (CD/DVD, pen-drive, removable hard-drive, etc.) or on a networked hard disk;
- Whether critical and sensitive data files backed-up daily, using an automated back-up process, preferably stored offline;
- Whether, master copies of critical and sensitive files made in open formats which facilitate long-term usage and finally
- Whether all back-up files validated regularly?

In terms of solutions it is proposed –

- Data should be stored in a locked cabinet.
- Crowdsourced data should be stored on a password protected and encrypted hard drive.
- The device should be in a locked room.
- Check data integrity of stored data files regularly.
- Use different formats of storage (e.g. hard disk/DVD)

- Label stored data in order to facilitating physical accessibility and location.
- Areas and rooms for storage of digital data should fit risk prevention regulations (e.g. flood and fire)
- Only responsible persons of core crisis response team members should have access to data.
- Enable secure remote access to confidential data but avoiding the possibility to download data.
- Publications regarding to the crisis response work must be conducted under the Statistical Disclosure Control carried out by a trained Service Staff.
- Data usage beyond the life of the crowdsourcing crisis management project must be closely supervised.
- Locking computer systems with a password and installing a firewall system are must.
- Servers should be protected through line-interactive uninterruptible power supply systems (UPS).
- Implementing password protection and control access to data files (e.g. no access, read only permission, administrator-only permission, etc.)
- Controlling access to restricted materials with encryption.
- Imposing non-disclosure agreements for managers or users of confidential data.
- Data transmitted should be encrypted, avoiding non-encrypted methods as e-mail, FTP protocol and so on.

- At the end of the crisis management project, data should be destroyed in a proper and consistent manner.
- Confidential data must be stored in a server without access to the Internet.
- Operating systems and anti-virus software in crowdsourcing platforms should be updated in order to avoid viruses and malicious codes.
- Backups can be stored offline (CD/DVD, pen-drive, removable hard-drive, etc.) or on a networked hard disk.
- Critical and sensitive data files should be backed-up daily, using an automated back-up process, preferably stored offline.
- Master copies of critical and sensitive files should be made in open formats which facilitate long-term usage.
- All back-up files should be validated regularly.

Crowdsourcing-based disaster platforms get increasing amount of information from social media. For instance, the functions of social media in drought risk management have being described as follows: info-sharing (one way and two ways), situational awareness, rumor control, reconnection and decision-making [163]. Apparently, social media was not active in donation solicitation and volunteer management. Perhaps the reason is that drought disaster is a long-term hazard and not an emergent one. Anyway, the contribution of digital volunteers reporting is now completed with web event data directly retrieved from social networks. Algorithms for social computation and data analysis are therefore crucial to distinguish the web event with

accuracy and precision indicators [164]. The resulting number of web pages and the average clustering coefficient can then be used to detect events.

Crowdsourced-based Geographic Information, the Volunteered Geographic Information (VGI) is used for Landslide Risk Assessment (LRA) [165]. The need of training for involved volunteers and selection and validation of data is often emphasized. The assessment of the accuracy of VGI has led to adopt conceptual quality frameworks of accuracy, granularity, completeness, consistency, compliance and richness [166]. Geographical Information Systems (GIS) are also becoming GIServices, including sensors, data, processing, portrayal, registry and chaining services [167]. Along with the GIS capabilities, the embedded technology like web and services, semantic web, sensing technologies, data-intensive computing and advanced analytics etc. are improving. This will provide intelligent mechanism for discovery, access and use of geospatial data in distributed service environments. These intelligent systems will include perception, reasoning, learning and acting.

Volunteers must collect and handle information containing personal details in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection [168]. Crisis governance volunteers should work under established standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection. Crowdsourcing Coordinators (CCs) and

crisis governance volunteers must not use any digital tool that has potential risks of security breach.

6.2. **Risks and recommendations related to situational awareness**

6.2.1 Coordination with volunteers

When assessing the risks in coordination with volunteers, we identified only two platforms had the option to be 'anonymous' or not to disclose locations. Whereas one platform did not have same options and one platform partially had same options. All platforms offered the option to choose email or phone as the first point of contact. One platform was not using any PET principles in terms of geolocation identification and no information found on the same issue in three platforms. One platform was not using any trusted network access for communication tools, one used the same partially and no information found on the same in other two platforms. However, no information found in any of the platforms while exploring the following:

- Maintaining a detailed log of actions related to user accounts plus regular audits regarding their validity, access rights and roles.
- Logging of user actions at a particular crowdsourcing deployment database.
- Whether handling of information containing personal details is being done in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection?

- Whether standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection?
- No platform had any guidelines for the crisis reporters and other users including journalists.

In terms of minimizing risks, the following recommendations are being proposed.

- Crowdsourcing reporters in humanitarian crisis must ask for options to be ‘anonymous’; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as reporters will be able to apply these options if needed.
- PET principles should be applied for determination of exact geolocation point of crisis reporters.
- Trusted network access for communication tools have to be established.
- Need to maintain a detailed log of actions related to user accounts plus regular audits regarding their validity, access rights and roles.
- User actions at a particular crowdsourcing deployment database should be logged.
- Crisis governance coordinators must collect and handle information containing personal details in accordance with the

rules and principles of international law and other relevant regional or national laws on individual data protection.

- Crisis governance coordinators should establish standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection.
- Crisis governance coordinators must not use any digital tool that has potential risk of security breach.
- Crisis governance coordinators must develop guidelines for the crisis reporters and other users including journalists.

6.2.2 Collaboration among agencies

In terms of using trusted network access for communication tools, we found two platforms were using the trusted network access while one was partially using the same and one platform was not using. Three platforms partially applied PET for common coordination platform and one did not apply the PET. Three platforms fully established and documented and one partially established and documented a personal data breach handling procedure. When analyzing whether private companies can collect data in the form of online survey, using third party apps etc., we identified two crowdsourcing platforms was not allowing third parties to collect data, one partially and one fully allowed third party to collect data. No information found in any of the

platforms whether disclosing of real names, locations of victims in man-made crisis is banned for all forms of media.

For above-mentioned risks related to collaboration among agencies during crisis, the following recommendations are being made:

- Trusted network access for communication tools have to be established.
- PET should be applied for common coordination platform
- Establish and document a personal data breach handling procedure.
- Private companies should not be allowed to illegally collect data in the form of online survey, using third party apps etc. from any online platforms including crowdsourcing platforms. Such type of illegal collection of personal data should be punishable by the Law.
- Disclosing of real names, locations of victims in man-made crisis should be banned by the law and should be applicable for all forms of media.

6.2.3 Collaboration between volunteers and different agencies

While checking whether crowdsourcing platforms are using a common coordination platform between government agencies and NGOs to deal with in humanitarian crisis, we found all four platforms were partially working towards a common coordination platform. Which means all platforms shared some information with government agencies and humanitarian NGOs during any crisis. No information found in any of

the four crowdsourcing platforms on – whether any established procedure for the secure destruction of personal data was available; whether reuse requires quality control on the crowdsourced data or whether there is any option to set up internal and independent supervisory bodies. For two platforms legal validation was required to reuse data. No information was found on this matter in case of one platform and one platform was using legal validation partially to reuse data.

To minimize the following above-mentioned risks, the following general recommendations are being proposed.

- A common coordination platform between government agencies and NGOs should be developed to deal with in humanitarian crisis.
- Trusted network access for communication tools have to be established.
- A specific procedure for the secure destruction of personal data should be established.
- The reuse will require quality control on the crowdsourced data.
- Some legal validation of the procedure will be required to reuse data.
- Internal and independent supervisory bodies should be implemented.

Traditional situational awareness services are mainly focused on the

institutional warning response [169]. While the intensity of disasters is said to increase, the response quality is perhaps decreasing. Some authors also claim for co-creation of improved quality in disaster response and recovery [170]. Only recently disaster management tries to exploit the active participation of citizens, with mobile data and smart sensors [171]. Smartphone apps and sensors provide new functionalities for emergency management [172].The design of the smartphone is now supposed to be adapted to a new use: emergency censoring. So, a new field is born for mobile HCI (Human Computer Interaction). “Crowd as sensor” is complementing the previous “crowd as journalist” perspective [173].

The added value of this information increases the reliability and the efficiency of the services. Semantic tagging, mining and analysis also enhance location and temporal perspectives [174]. Geo-tagged and time-tagged data are then classified into different categories. Indeed, some projects offer situational awareness web services, combining social media data and volunteers’ participation [175]. Sentiment analysis in social media is also recently taken into consideration for situation awareness and even for supporting decision making during the crisis [176].

Nonetheless, this bottom-up contribution also raises some concerns. Digital volunteers working remotely are unaware of the direct experience of the crisis. This information is data-driven and focused on correlations, with an increasing presence of data analysis. So, there might be a lack of qualitative understanding of the situation, in the

sense of misleading situational knowledge [177]. The situational awareness can be more complex than simply asking volunteers to enhance and complete current available information. Context modelling with data analysis requires accounting for its limitations. Social scientists should be involved in situational awareness to enhance the social and political impact assessment.

On the other hand, the unpredictable mix of casual contributions due to crowdsourcing disaster management includes varied influences with effects on the data [178]. As a result, first response teams, when using the OpenStreetMap (OSM) data should be aware of the roles played by contributors that cannot be reduced to "citizen as sensor". A complex typology of roles therefore emergences like the "contribution profiles" [178]. The data also greatly decrease in quantity and quality when moving out side major cities with active mapping communities.

Therefore crisis management agencies must develop guidelines for the general users, crisis reporters and other users including journalists. A common coordination platform between government agencies and NGOs should be developed to deal with in humanitarian crisis. Crowdsourcing reporters in humanitarian crisis must ask for options to be 'anonymous'; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as reporters will be able to apply these options if needed. This is urgent taking into account the multiple task-oriented roles volunteers are developing in current crowdsourcing

disaster platforms [179].

6.3 Evaluation of the recommendations concerning Decision Support Systems

6.3.1 Decision-making by human intelligence

While identifying whether the Solution Support Teams (SST) are available for every crisis response work, we found all platforms had SSTs. Also the procedure of validating by first response team was followed by all platforms. Three platforms partially used cross-checking methodology to make decisions in a consistent manner and one platform fully used the same methodology. Three platforms used to keep logs which were available for internal and external supervision on regular interval and one platform partially kept logs and was available for supervision. Following general recommendations are being made to address risk issues mentioned above:

- Solution Support Teams (SST) should be formed for every crisis response work.
- First response team should validate.
- Cross-Checking methodology should be in place to make decisions in a consistent manner.
- SST should keep logs available for internal and external supervision on regular interval.

6.3.2 Automatic decision-making

We found no platform was using any automatic cross-checking

methodology, no automatic system alerts integrated with any platforms to generate further actions or no crowdsourcing platforms are using different tools those trust level were announced publicly by the developers. No information found while checking whether any purpose limitations procedure were available. All platforms had plans for upgrading hardware and software on regular basis. Three platforms allowed PET integration for crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as ‘anonymous’ and one platform used the same partially. We also found that the first response teams do monitoring and cross-checking in case of two platforms and in case of other two platforms, first response teams partially monitor and cross-check.

However, the following general recommendations are being proposed to avoid above –mentioned risks:

- Automatic cross-checking methodology should be in place.
- First response team monitoring and cross-checking tasks are must.
- Purpose limitation (only for disaster management) procedure have to be applied.
- A specific plan for upgrading hardware and software should be implemented.
- The use of system integrity tools should enable deletion and reporting of changes applied on servers. Automatic system alerts generating facilities need to be integrated
- Tech companies that develop crowdsourcing tools should publicly announce the ‘trust’ level of the tool.

- Tech companies should develop tools with PET integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as ‘anonymous’.

Passive crowdsourcing is a source of intelligence, a tool for situational awareness and it is also increasingly being used for decision support systems. The evolution of the role of science and technology in the policy process is clearly present in the 2015 Sendai Framework [180]. IT tools not only enhance the retrieval of accurate information, enriches the situational awareness and supports the decisions making of first response teams; they also improve the implementation and reporting of the Sendai Framework itself. IT tools are therefore fuelling multi-hazard and multidisciplinary approaches to disaster management. Indeed, even if cost-benefit analysis continues to be important in Disaster Risk Reduction, multi-criteria analysis and robust decision-making approaches seem to adapt better to preparedness and systemic interventions [181]. More, disaster management shares some benefits and challenges with other public policies, like energy efficiency, that could perhaps converge in the near future for greater positive impact on society [182], disaster risk management at farms [183] and Climate Risk Management (CRM) [184]. Moreover, disasters are highly unpredictable, and extensive assessments are difficult in situ. That’s the reason why simulation is increasingly being used to test the software solutions for natural disaster responses [185]. Multi-agent systems are also envisioned to guide first response teams in the near future [186]. But all these new roles of technology related to disaster management

need new safeguards.

With a combination of databases, the response teams now have the possibility to describe disasters over time and space in one area. This allows local-scale disaster management for areas where no direct information is available [187]. By doing so, actions can be adopted and disaster risk-reduction management can be properly implemented. Data analysis is thus eventually allowing decision support systems. Military humanitarian assistance, for instance by means of disaster relief aerial delivery operations, has also developed multi-criteria logistics modelling [188]. Some limitations of these decision support systems are worth mentioning. First, parameter estimation for rare events is difficult since in this case historical data are sparse. On the other hand, in case of lack of information, average values are usually used. The results might change with accurate field data. Finally, the assumption that the decision-makers are risk neutral might not be realistic in concrete scenarios.

Rapid mapping is also becoming an interesting decision support tool for disaster management. Disaster platforms systematically evaluate with both efficiency and accuracy. Collaborative mapping and crowdsourcing initiatives like HOT-OSM and TomNod contribute to analyse of post-event imagery. But the digital communities are now involved in off-line analyses to train supervised classification algorithms [189].

Crisis coordinators should use tools with Privacy Enhancing Technologies integration to allow crisis reporters to have control over

their location disclosure and to be given the capacity to choose to be recorded as ‘anonymous’. On the other hand, crowdsourcing reporters in humanitarian crisis must ask for options to be ‘anonymous’; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as users will be able to apply these options if needed.

VII. Conclusions

The role of crowdsourcing for disaster management is constantly evolving. Its initial contribution was to help collecting information as it has been noticed in the case of Ushahidi. Since 2005, crowdsourcing has allowed citizens to connect with each other, governments to connect with common mass, acquiring information quickly and participating in issues that affect citizens. We noticed the better use of crowdsourcing platforms and the positive development of crowdsourcing help common people to become more active and informed citizens. The information gathered from social networks and also volunteers' reports contributed to modify the first crowdsourcing platforms. Accurate information retrieval was one of the important responsibilities during early days of digital crowdsourcing.

Since 2008, a new 'digital' crowdsourcing for crisis response is replacing the old one. Numbers of platforms have been developed by different communities and tech companies to address crisis. Initiatives like DHN were established during this time. Although use of crowdsourcing allows a higher availability of information, inaccurate reports provided by volunteers were an increasing problem. Platforms therefore realized some filtering and proper selections from experts were both needed. Present crisis response work is more affordable, more accurate and more trustworthy than the initial stage of digital crowdsourcing. A new layer of trusted volunteers is coordinating and selecting relevant information from the rest of volunteers. It also complements and fulfils the experts or first response teams' decision making.

But, this enhanced crowdsourcing is also currently been replaced by data analysis. In recent initiatives, data analysis improves digital humanitarian activities. This sudden move toward social media channels and Big Data changes the role of volunteers and trusted volunteers. They are not only source of relevant updated information; they are also training algorithms. And perhaps one day, the resulting decision support system will work independently from its crowdsourcing origins. Like some big stars, crowdsourcing might collapse and disappear into a decision support system's black hole.

Meanwhile, both contributions –information accuracy and complement by trusted volunteers and algorithms training- are evolving in parallel. For example, at the earlier stage of using crowdsourcing for crisis management, the main contribution of digital volunteers was crisis mapping. This is still going on. Nonetheless, current crisis mapping platforms also use sophisticated tools and technologies i.e. machine learning, artificial intelligence, use of drones to gather crisis information etc. MicroMappers is the pioneer example of using machine learning, artificial intelligence in disaster response activities.

Thus, some platforms using data analysis like Digital Humanitarian Network (DHN) are becoming meta-communities, offering real-time estimation of reliability and relevance of incidents for digital communities and crisis response coordinators. Indeed, data analytics adds a new layer to final data mapping, with sensors, UVA or satellite images;

and it replaces volunteers' relevance selection with algorithms. Visual analytics and risk estimation fuel situational awareness services.

These platforms with data analysis are not only meta-communities for other more traditional disaster management communities; they directly support first responde teams decision-making. In this research, it has been identified that first response teams are usually reluctant to let non-experts participate in the decision-making process. Nonetheless, the emerging automatic support systems based on simulation, geomatics and emotion classification might soon directly be part of an hypothetic quick-reponse decision-making. Similarly to many other fields, experts should not decide solely based on automatic tools. First response teams should also check those tools, and limit their use to recurrent and clear cases. In more complex cases, confirmation from skilled experts is necessary.

The coordination of OCHA and DHN can be an alternative decision support, not only based on automatic tools. Indeed, OCHA-DHN can offer external supervision to automatic decision support systems. Obviously, like in other emerging technology fields –nanotechnology, biotechnology…- the risk of capture of the law maker is always there. But the alternative of completely automatic decision support systems is, in our opinion, even worse.

Crisis management and Disaster Risk Reduction need a legal framework to enhance this evolving crisis governance.

7.1 Summary and Analysis of Various Old and New Risk Scenarios relevant to Law and Policies

We identified different stage-wise risk scenarios in crowdsourcing. For example, in retrieval and selection' stage, security breach, cyber-attacks, nuisance attacks, Mass surveillance, Quality and accuracy of data, Personal Information Disclosure, Location management, Sensitive data are most important concerns in terms of data analysis by volunteers. The other concerns during data analysis are profiling with data mining, geolocation using sensors and user ranking and content classification.

During the stage of 'situational analysis', we identified issues related to Geo-referenced information, lack of coordination between experts and volunteers, lack of collaboration between agencies, Non-acceptance of SA services by users, Information collection and storage, reliability, decision adversely affecting humans solely based on automatic decision-making support system and traceability of the automatic decision are most important.

7.2 Summary and Analysis of Privacy and Data Protection Risk Assessment and Recommendations for Crowdsourcing Crisis Management Platforms

Inclusive governance is very challenging to current thinking and practice in crisis management. Though, present crisis governance arrangements

are still very government-centric, emerging blend of ‘community-driven’ and ‘technology-driven’ crisis management framework could be the model of third generation crowdsourcing crisis governance regulatory framework.

Developing more inclusive regulatory framework for crowdsourcing crisis management is not, of course, a magic bullet for achieving more legitimate and effective responsibility-sharing among citizens, humanitarian organisations and the State in disaster management.

Our main aims were to identify how the Priority Action 1 of the Sendai Framework for Disaster Risk Reduction 2015-2030 can be enhanced more by highlighting the importance of ‘data protection’ in using crowdsourcing process in any disaster / crisis management event; and to contribute in fulfilling partially the Priority Action 2 of the Sendai Framework by offering recommendations for Crowdsourcing Crisis Management Platforms. To fulfil the aim, we identified crowdsourced-based disaster management platforms’ risk scenarios, and later proposed existing ways to preserve privacy, security and data protection in crowdsourcing crisis management. Doing this part of the work, we have described the three different roles crowdsourcing plays in these platforms: retrieval and selection of data, context enhancement or situational awareness, and data or training for automatic support systems. This classification of roles is a contribution beyond the state-of-the-art in crowdsourcing disaster management.

7.3 Summary and Analysis of different Safeguards

7.3.1 Disaster Risk Reduction

In terms of regulations, policies and laws, at the international level, the *Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters (HFA)*[49] was developed and agreed on with the many partners needed to reduce disaster risk - governments, international agencies, disaster experts and many others - bringing them into a common system of coordination. However, this framework did not highlight anything about the privacy, online security and data protection during the emergency.

The *Hyogo Framework for Action 2005-2015* was replaced by the Sendai Framework for Disaster Risk Reduction (2015-2030). This international framework adopted in 2015 did not talk on the potential risks of using emerging ICTs and crowdsourcing in disaster management. However, we identified that some Sendai principles could be directly linked to crowdsourcing disaster management.

7.3.2 General Data Protection

On the other hand, the general principles of Privacy and Data Protection apply to the personal information involved in the disaster management platforms. For instance the International Committee of the Red Cross has adopted some rules on Personal Data Protection and includes these basic principles[50]. Recent EU data protection rules adopted in April 2016 aim to give citizens back control of their personal data and create a high,

[49] The Hyogo Framework endorsed by the UN General Assembly in the Resolution A/RES/60/195 following the 2005 World Disaster Reduction Conference.
[50] ICRC Rules on Personal Data Protection, The ICRC Data Protection Reference Framework, adopted by the Directorate of the ICRC on 24 February 2015 and updated on 10 November 2015.

uniform level of data protection across the EU that fit for present digital era.[51]

7.4 Summary and Analysis of Various individual concerns and Summary Recommendations

We also identified various individual concerns in terms of information / data retrieval, selection, storage, coordination with volunteers, collaboration among agencies, collaboration between volunteers and agencies, decision-making by human intelligence, automatic decision – making in crowdsourcing crisis management. Finally, we also provided potential recommendations to various concerns identified during the research work.

7.5 Evaluation of Four Platforms

Among these four platforms i.e. Ushahidi, DHN, MicroMappers and Google Crisis Map, information regarding a good number of privacy, security and data protection components were not found during the research. We also identified number of drawbacks in all four platforms. In general, there was no common coordination crowdsourcing platform that makes all communication more vulnerable. Among others, none of the platforms used proper and trustworthy encryption technology; none of the four platforms had announced trustworthiness of different tools publicly; there was no automatic cross-

[51] Regulation (EU) 2016/679, Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), will come into force on 25 May 2018.

checking methodology in place and there was no reporting guideline for the crisis news reporters, including journalists. And finally, out of four crowdsourcing platforms, Ushahidi had less security and data protection measurement for users.

Data analyses contribute to threaten the informed consent principle. According to it, users should be able to self- manage their privacy. As a rule of thumbs, the use of social networks is reducing the capacity of people to preserve their intimate information. In the context of crisis, the situation is even worse: data protection might be much lower priority than obtaining help or locating a friend or loved people [190]. Location, food and water needs in one event are now reused and held in databases for further data analyses. The predictive capabilities might help managing more efficiently the next crisis. But, for the concrete data user, it might be the occasion for discrimination in other contexts like employment, health insurance or property [190]. The duty to participate replaces the informed consent right of the user, and an unbalanced general interest prevails. Data tagged as private by users might, nonetheless, be published through crowdsourcing efforts. There is no proportionality in this case, and during crisis victims and users have absolutely no power to shape the use of their data by the platforms. In the event of a disaster, on the contrary, user rights should be more preserved than on ordinary cases. It is a sensitive situation to protect, and like health, gender and political opinions, a special effort is here needed.

Disasters are no longer viewed as only or mainly natural events, but

more as the results of poor governance [191]. Disaster management is also considered a shared responsibility, an investment in humanity [192]. As numbers of crowdsourcing crisis informatics risks were identified and also numbers of recommendations were made in this paper, the future work would be to execute those recommendations. Based on different scenarios, it has been identified that trusted network access, authentication, encryption, data backups, privacy-preserving information systems, authentication broadcasting, filtering, cross-checking, verification by the crowd, mask up, forwarding, obfuscation, perturbation, additional safeguards for sensitive data, privacy preserving data mining, Privacy Enhancing Technologies (PET), PET for geolocation, Context-aware multi-party coordination systems, proper Solution Support Teams, Purpose limitation (only for disaster management), first response team monitoring and cross-checking etc. are needed to solve present risks associated with crowdsourcing crisis management. Media should develop their own 'Media Ethics' for crisis reporting with keeping in mind the privacy and security issues of victims. Law enforcement agencies should not monitor crowdsourcing process for crisis governance to identify 'evidences' illegally in the suspicion of future terrorist attack or conflict (in man-made crisis). For counter-terrorism purpose governments could do so with prior judicial authorizations. Crowdsourcing crisis coordinators, and different online platforms that provide support during any crisis event, need to address privacy, security and data protection issues associated with the platform.

7.6 Proposed Future Work

We divided our proposed future work in two levels. The first one is at policy level i.e. for law makers and the second one is at practice level i.e. for other relevant stakeholders.

7.6.1 Proposed Future Work at Policy Level

As we wanted to contribute to the Sendai Framework Priority Actions 1 and 2, we believe that integrating of the following articles of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) would fulfil various issues related to privacy and security in crowdsourcing crisis management.

- Art. 5.2 Accountability principle – 'the controller shall be responsible for, and be able to demonstrate compliance with lawfulness, fairness and transparency' in relation to data subject.
- Implement data protection by design and by default according to Article 25.
- Implement data protection impact assessment and prior consultation according to the Article 35 of General Data Protection Regulation.
- The Sendai Framework should also state the importance of having a Data Protection Officer as mentioned in Article 37 of General Data Protection Regulation.

- It is also proposed that the Sendai Framework to issue ‘Codes of Conduct’ according to Article 40 of the General Data Protection Regulation.
- According to the Article 43, the Sendai Framework should create a ‘Certification Body’ to have an appropriate level of expertise in relation to crowdsourced data protection.

As the mentioned recommendations are not fulfilled by platforms investigated in this research, and therefore the detected priorities for law-makers are to contribute in developing regulatory frameworks at national, regional and international level.

7.6.2 Proposed future work at practice level

The following recommendations are also not fulfilled by platforms investigated in this research, and therefore the detected priorities for various stakeholders related to crowdsourcing crisis management platforms are to follow the following at practice level:

- On information and data retrieval, encryption is still not used or not properly used. Privacy preserving datamining procedures should also be in place. The “trust” level of the tool should also be available.
- On data selection, the two steps verification process needs to be fulfilled by expert crowds (volunteers).
- On storage, encryption is not yet integrated with the platform.
- On coordination, crisis governance coordinators must develop guidelines for the crisis reporters and other users like journalists. Third party reuse of data is a clear risk not yet tackled.

- On decision support systems, the use of system integrity tools should enable deletion and reporting of changes applied on servers. Here too the “trust” level of the tool should be available for users.

References

1. Howe, J. ‘The Rise of Crowdsourcing’. Wired, 14 June 2006.
2. Howe, J. Crowdsourcing: A Definition. Crowdsourcing, 02 June 2006.
3. Estelles – Arolas, e et al. Towards an integrated crowdsourcing definition. Journal of Information Science, v. 38, n. 2, p. 189–200, 2012.
4. Windt, P. V. D. From Crowdsourcing to Crowdseeding: The Cutting Edge of Empowerment? 20132.
5. Howe, J. ‘Crowdsourcing: why the power of the Crowd is driving the Future of Business’. New York: Crown Business, 2008.
6. Ess, H. V. Harvesting Knowledge: Success Criteria and Strategies for Crowdsourcing. 2010.
7. Grier, D. A. Crowdsourcing for Dummies. Hoboken, New Jersey: John Wiley & Sons, 2013.
8. Brabham, D C. Crowdsourcing. Massachusetts: The MIT Press, 2013.
9. Poblet et al. Crowdsourcing Tools for Disaster Management: A Review of Platforms and Methods. In: Lecture Notes in Artificial Intelligence Series, Berlin, Heidelberg: Springer Verlag, 2014.
10. Hetmank, L. Components and Functions of Crowdsourcing Systems: a Systematic Literature Review. In: International Conference on Wirtschaftsinformatik, 11., 2013., Leipzig. Proceedings… . Leipzig: University Leipzig, 2013. p 55-69.
11. Halder, B., Crowdsourcing collection of data for crisis governance in the post-2015 world: potential offers and crucial challenges, Proceeding ICEGOV '14 Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance. ACM New York, NY, USA. 2014.
12. Casal, D. P. Crowdsourcing the Corpus: Using Collective Intelligence as a Method for Composition. Leonardo Music Journal, n. 21, p. 25-28, 2011.

13. Belleflamme, P. et al. Crowdfunding: Tapping the Right Crowd. In: (July 9, 2013). Journal of Business Venturing, Forthcoming; CORE Discussion Paper No. 2011/32. 2011.
14. Bommert, B. Collaborative innovation in the public sector. International Public Management Review, v. 11, n. 1, p. 15–33, 2010.
15. Fitt, V. A. Crowdsourcing the News: News Organization Liability for iReporters. William Mitchell Law Review, v. 37, n. 4, p. 1839-1867, 2011.
16. Norman, T. C. et al. Leveraging Crowdsourcing to Facilitate the Discovery of New Medicines. Science Translational Medicine, v. 3, n. 88, p. 88mr1, june/2011.
17. Cox, L.P. Truth in Crowdsourcing. IEEE Journal on Security and Privacy, v. 9, n. 5, p. 74-76, 2011.
18. Meier, P. AIDR: Artificial Intelligence for Disaster Response. Published in iRevolutions.org. 2013.
19. United Nations, (2015), Preamble of the Sendai Framework for Disaster Risk Reduction 2015-2030', (A/CONF.224/L.2) the final outcomes of the Third United Nations World Conference on Disaster Risk held in March 2015.
20. United Nations, (2013), 'Report on the International Expert Meeting on Crowdsource Mapping for Disaster Risk Management and Emergency Response carried out in the framework of the United Nations Platform for Space-based Information for Disaster Management and Emergency Response' (UN-SPIDER) Report No. A/AC.105/C.1/2013/CRP.5 presented by the Committee on the Peaceful Uses of Outer Space Scientific and Technical Subcommittee at Fiftieth Session in Vienna during 11-22 February 2013.
21. Robert, M.: Crowdsourcing and the crisis-affected community. Lessons learned and looking forward from Mission 4636. Information Retrieval, v. 16, n. 2, p. 210-266, apr. 2013.
22. Halder, B. Crowdsourcing for Social Change in the Global South: Challenges and Possibilities. In: International Conference for e-

Democracy and Open Government, 2. Krems. Proceedings… Krems: Edition Donau-Universität Krems, 2013. p. 473-474.
23. Fisher, L. How Crowdsourcing Is Tackling Poverty In The Developing World. Forbes, 21 mar. 2012.
24. Chunara, R et al. Social and News Media Enable Estimation of Epidemiological Patterns Early in the 2010 Haitian Cholera Outbreak. The American Journal of Tropical Medicine and Hygiene, v. 86, n. 1, p. 39-45, 2012.
25. ACCESS. Privacy & Data Protection on Social Networks. In: EDRI and Digital Courage (Germany) (Eds.). An Introduction to Data Protection. v. 6. Brussels: European Digital Rights, 2013. p. 14-15.
26. Chamales, G. Et al. Securing crisis maps in conflict zones. In: GLOBAL HUMANITARIAN TECHNOLOGY CONFERENCE, 2011, Seattle. In Proceedings. Los Alamitos: IEEE, 2011. p. 426–430.
27. Stecklow, S. et al. Mideast Uses Western Tools to Battle the Skype Rebellion. The Wall Street Journal, 1 sept. 2011.
28. Morrows, N., et al. Independent evaluation of the Ushahidi Haiti project. Medford, MA. ALNAP, 2011.
29. Strohmeyer, K. Not alone in a crowd: Crowdsourcing for healthcare. Level 3 Communications Blog, Healthcare, 2013.
30. World Bank. Information and Communications for Development 2012: Maximizing Mobile. Washington: World Bank, 2012.
31. Gallagher, L. Experts: mHealth poses privacy challenge. Healthcare IT News, 2013.
32. Karnin, et al. Crowdsourcing in the Document Processing Practice. In: DANIEL, F.; FACCA, F. M. (Eds). Current Trends in Web Engineering. Lecture Notes in Computer Science Series, v. 6385. Berlin, Heidelberg: Springer, 2010. p 408-411.
33. Wang, Y et al. Respecting User Privacy in Mobile Crowdsourcing. Science Journal, v. 2, n. 2, p. 1-15, 2013.

34. Heinzelman, J et al. Crowdsourcing Crisis Information in Disaster- Affected Haiti. Special Report 252. Washington: United States Washington Institute of Peace, 2010.
35. William, E. Defending users against smart-phone apps: techniques and future directions. In: International Conference on Information Systems Security, 7, Berlin. Proceedings…Berlin, Heidelberg: Springer-Verlag, 2011.p. 49-70. 2011.
36. Grubmuller, V et al. Social media analytics for future oriented policy making. European Journal of Futures Research, v. 1, n. 1, p. 1-9, 2013.
37. Omand, D et al. A balance between security and privacy online must be struck. London: Demos, 2012.
38. Toch, E. Crowdsourcing privacy preferences in context-aware applications. London: Springer-Verlag, 2012.
39. Van, V. E. B. Obstacles to European research projects with data and tissue: solutions and further challenges. European Journal of Cancer, v. 44, n. 10, p. 1438–50, 2008.
40. Martens, R. IOM Data Protection Manual. International Organisation for Migration, Geneva. Switzerland, 2010.
41. Halder, B., Measuring Security, Privacy and Data Protection in Crowdsourcing. Published in SSRN, 2014.
42. Halder B: Crowdsourcing Collection of Data for Crisis Governance in the Post-2015 World: Potential Offers and Crucial Challenges. 8th International Conference on Theory and Practice of Electronic Governance, Guimaraes, Portugal, 2014. Proceedings by Association for Computing Machinery, ACM Press (ISBN 978-1-60558-611-3). 2014.
43. Temnikova I,, Biyikli D, and Boon F: First Steps towards Implementing a Sahana Eden Social Media Dashboard. SMERST 2013: Social Media and Semantic Technologies in Emergency Response, 2013, p 6.
44. Gao H, Wang X, Barbier G, and Liu H: Promoting Coordination for Disaster Relief– From Crowdsourcing to Coordination in J.

Salerno et al. (Eds.) Springer-Verlag, Berlin Heidelberg. 2011, pp. 197–204.
45. Abbasil M, Kumar S, Filho A, et al.: Lessons Learned in Using Social Media for Disaster Relief - ASU Crisis Response Game in S.J. Yang, A.M. Greenberg, and M. Endsley (Eds.). Springer-Verlag Berlin Heidelberg. 2012, pp. 282–289.
46. Ortmann J, Limbu M, Wang D et al.: Crowdsourcing Linked Open Data for Disaster Management, Institute for Geoinformatics. University of Muenster, Germany, 2011.
47. Imran M, Castillo C, Lucas J, et al.: AIDR: Artificial Intelligence for Disaster Response. WWW'14 Companion, Seoul, Kore, April 7–11, 2014.
48. Ezequiel CAF, Cua M, Libatique NC, et al.: UAV Aerial Imaging Applications for Post-Disaster Assessment, Environmental Management and Infrastructure Development. 2014 International Conference on Unmanned Aircraft Systems (ICUAS). May 27-30, 2014. Orlando, FL, USA. 2014, pp. 274-283.
49. Meier P: On UAVs for Peacebuilding and Conflict Prevention. Blog published in irevolution.net. 2014.
50. Vieweg S, Hughes AL, Starbird K, et al.: Microblogging during Two Natural Hazards Events: What Twitter May Contribute to Situational Awareness. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, GA. New York: ACM Press. 2010, pp. 1079–1088.
51. Meier, P. (2013). AIDR: Artificial Intelligence for Disaster Response. Published in irevolution.net.
52. Blum JR, Eichhorn A, Smith S, et al.: Real-time emergency response: improved management of real-time information during crisis situations. J Multimodal User Interfaces. 2014; 8: 161–173.
53. Liu SB: Crisis Crowdsourcing Framework: Designing Strategic Configurations of Crowdsourcing for the Emergency

Management Domain published in Computer Supported Cooperative Work (CSCW). 2014; 23: 389-443.
54. Starbird K: Crowdwork, Crisis and Convergence: How the Connected Crowd Organizes Information During Mass Disruption Events. University of Colorado at Boulder, Colorado: Alliance for Technology, Learning, and Society (ATLAS) Institute. 2012.
55. Hemus, J (2013). Crisis management planning: why a new reality demands a fresh approach. Published in International Public Relations Association. London. UK.
56. Small SG, and Medsker L: Review of information extraction technologies and applications in Neural Computing and Applications. Springer-Verlag London. 2013; 25: 533–548.
57. Weaver AC, Boyle JP, and Besaleva LI: Applications and Trust Issues when Crowdsourcing a Crisis. Proceesings of ICCCN, IEEE. 2012, pp 1-5.
58. Meier, P (2014). Presentation at the Advanced Technology Conference Series by TTI Vanguard.
59. Meier, P. (2013). How Online Gamers Can Support Disaster Response. Published in irevolution.net.
60. Meier. P (2013): Live Crisis Map of Disaster Damage Reported on Social Media. Published in irevolution.net.
61. Rajiv A: Analyzing User Behavior On Facebook's "Hurricane Sandy Lost and Found Pets" Page to Improve Support for Pet Matching in Crisis Informatics Applications. A thesis submitted to the Faculty of the Graduate School of the University of Colorado in partial fulfillment of the requirement for the degree of Master of Science Department of Computer Science, 2013.
62. Gupta A, Kumaraguru P, Castillo C, et al.: TweetCred: Real-Time Credibility Assessment of Content on Twitter, In: Social Informatics. L.M. Aiello and D. McFarland (Eds.): SocInfo. 2014, pp. 228–243.

63. Ajmar A, Boccardo P, Disabato F, et al.: Mapping: geomatics role and research opportunities. Rend. Fis. Acc. Lincei. 2015; 26: 63-73.
64. Chae J, Thomb D, Jang Y, et al.: Public behavior response analysis in disaster events utilizing visual analytics of microblog data. Computers and Graphics. 2014; 38:51-60.
65. Poblet M (ed.): Mobile Technologies for Conflict Management: Online Dispute Resolution, Governance, Participation, Law, Governance and Technology Series 2. 2011.
66. Meier, P. (2011). OpenStreetMap's New Micro-Tasking Platform for Satellite Imagery Tracing. Published in irevolution.net.
67. Naderpour, M. and Guangquan Zhang, J.L., An intelligent situation awareness support system for safety-critical environments, Decision Support Systems, 59, 325-340 (2014).
68. Artés T, Cencerrado A, Cortés A, et al.: Enhancing computational efficiency on forest fire forecasting by time-aware Genetic Algorithms. J Supercomput. 2015; 71:1869–1881.
69. Foresti G, Farinosi M, and Vernier M: Situational awareness in smart environments: socio-mobile and sensor data fusion for emergency response to disasters. J Ambient Intell Human Comput. 2015; 6: 239–257.
70. United Nations, 2015. Preamble of the Sendai Framework for Disaster Risk Reduction 2015-2030, (A/CONF.224/L.2) the final outcomes of the Third United Nations World Conference on Disaster Risk held in March 2015.
71. OCHA, 2014. Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies, Occasional Policy Paper, OCHA Policy and Studies Series 2014.
72. Gao, H., Wang, X.. Barbier, G. and Liu, H (2011). Promoting Coordination for Disaster Relief– From Crowdsourcing to

Coordination in J. Salerno et al. (Eds.): SBP 2011, LNCS 6589, pp. 197–204, 2011. Springer-Verlag Berlin Heidelberg 2011.

73. United Nations, 2013. Report on the International Expert Meeting on Crowdsource Mapping for Disaster Risk Management and Emergency Response carried out in the framework of the United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER) Report No. A/AC.105/C.1/2013/CRP.5 presented by the Committee on the Peaceful Uses of Outer Space Scientific and Technical Subcommittee at Fiftieth Session in Vienna during 11-22 February 2013.
74. Gao, H., Barbier, G., Goolsby, R. (2011). Harnessing the crowdsourcing power of social media for disaster relief. IEEE Intelligent Systems 26(3), 10–14 (2011).
75. Tapia, A. H., and Moore, K., Good Enough is Good Enough: Overcoming Disaster Response Organizations' Slow Social Media Data Adoption, Computer Supported Cooperative Work (CSCW) (2014) 23:483–512.
76. Gilman, D. 2014. Cyber-Warfare and Humanitarian Space, in Llorente, R. V. and Wall, I. (eds.) Communications Technology and Humanitarian Delivery Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF).
77. Byrne, R. 2014. Trends in Intelligence Gathering by Governments, in Llorente, R. V. and Wall, I. (eds.) Communications Technology and Humanitarian Delivery Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF).
78. Fisher, M. 2013. Syria's Pro-Assad Hackers Infiltrate Human Rights Watch Web Site and Twitter Feed, The Washington Post, 17 March, 2013. Available at http://wapo.st/1xSz3T7
79. Kiyomoto, S., Fukushima, K., and Miyake, Y., Security issues on IT systems during disasters: a survey, J Ambient Intell Human Comput (2014) 5:173–185.

80. Wu,S.-Y., Wang, M.-H., and Chen, K.-T., Privacy Crisis due to Crisis Response on the Web, 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST.
81. Saito, Y., Progress or repetition? Gender perspectives in disaster management in Japan, Disaster Prevention and Management Vol. 23 No. 2, 2014 pp. 98-111
82. Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers, 22(5), 428-438.
83. Halder, B. 2014. Crowdsourcing collection of data for crisis governance in the post-2015 world: potential offers and crucial challenges. In Proceeding ICEGOV '14 Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance. ACM New York, NY, USA ©2014.
84. Slonecker, E. T., Shaw, D. M., and Lillesand, T. M.: Emerging Legal and Ethical Issues in Advanced Remote Sensing Technology. Photogrammetric Engineering & Remote Sensing, Vol. 64, No. 6, June 1998, pp. 589-595.
85. Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M. (2011). A survey on privacy in mobile participatory sensing applications. Journal of Systems and Software, 84(11), 1928– 1946.
86. Lievrouw, L. A., & Farb, S. E. (2003). Information and social equity. In Cronin, B. & Shaw, D. (Eds.), Annual review of information science and technology, Volume 37 (pp. 499–540).
87. Ginige, A., Paolino, L., Romano, M., Sebillo, M., Tortora, G., & Vitiello, G. (2014). Information Sharing Among Disaster Responders - An Interactive Spreadsheet-Based Collaboration Approach. Computer Supported Cooperative Work (CSCW) (2014) 23:547–583. DOI 10.1007/s10606-014-9207-0.
88. Poblet, M. (ed.), (2011) Mobile Technologies for Conflict Management: Online Dispute Resolution, Governance, Participation, Law, Governance and Technology Series 2, DOI 10.1007/978-94-007-1384-0_4, © Springer Science+Business Media B.V. 2011.

89. Ajmar, A.,Boccardo, P., Disabato, F. and Tonolo, F.G. (2015). Mapping: geomatics role and research opportunities, Rend. Fis. Acc. Lincei, Springerlink.com.
90. Chae J., Thomb, D., Jang Y., Kim S.Y., Ertl, T. And Ebert D.,S., Public behavior response analysis in disaster events utilizing visual analytics of microblog data, Computers and Graphics, 38, 51-60 (2014).
91. Cushing, T., 2014. Los Angeles Law Enforcement Looking To Crowdsource Surveillance, (Mis)Uses of Technology. Published at http://bit.ly/S4d6wE. Accessed on 12/05/14
92. Berlin, J. M. and Carlstro, E. D.: (2014). Collaboration Exercises—The Lack of Collaborative Benefits. International Journal of Disaster Risk Science (2014) 5:192–205 www.ijdrs.com. DOI 10.1007/s13753-014-0025-2.
93. N. Kapucu, The American Review of Public Administration 36 (2006) 207-225.
94. Purohit, H., Hampton, A., Bhatt, S., Shalin, V.L., Sheth, A. P. & Flach, J. M. (2014). Identifying Seekers and Suppliers in Social Media Communities to Support Crisis Coordination. Computer Supported Cooperative Work (CSCW) (2014) 23:513–545. DOI 10.1007/s10606-014-9209-y.
95. Sweta, L.O. 2014.: Early Warning Systems and Disaster Management using Mobile Crowdsourcing . International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 . Volume 3 Issue 4, April 2014.
96. V.G. Duffy (Ed.) (DHM 2014). HCI Challenges for Community-Based Disaster Recovery. LNCS 8529, pp. 637–648, 2014. Springer International Publishing Switzerland 2014.
97. L.M. Aiello and D. McFarland (Eds.): Integrating Social Media Communications into the Rapid Assessment of Sudden Onset Disasters. SocInfo 2014, LNCS 8851, pp. 444–461, 2014. Springer International Publishing Switzerland 2014.

98. Verity, A., Mackinnon, K., Link, Y.: OCHA information management guidance for sudden onset emergencies. Tech. rep., UN OCHA (Feb 2014).
99. Way, S., Yuan, Y. (2013). Transitioning From Dynamic Decision Support to Context-Aware Multi-Party Coordination: A Case for Emergency Response. Group Decis Negot (2014) 23:649–672. DOI 10.1007/s10726-013-9365-3.
100. Patterson, E. Crowdfunding Sites Grapple with Fraud, Better Business Bureau. 2013.
101. Larrauri, H. P. 2014. Drones, ethics and conflict. Accessed on 10/11/2014 andavailable at http://bit.ly/1qUwRER
102. Naderpour, M. and Guangquan Zhang, J.L., 2014: An intelligent situation awareness support system for safety-critical environments, Decision Support Systems, 59, 325-340 (2014).
103. Gao, H., Wang, X.. Barbier, G. and Liu, H (2011). Promoting Coordination for Disaster Relief– From Crowdsourcing to Coordination in J. Salerno et al. (Eds.): SBP 2011, LNCS 6589, pp. 197–204, 2011. Springer-Verlag Berlin Heidelberg 2011.
104. Abbasil, M., Kumar, S., Filho, A, and Liu, H. (2012). Lessons Learned in Using Social Media for Disaster Relief - ASU Crisis Response Game in S.J. Yang, A.M. Greenberg, and M. Endsley (Eds.): SBP 2012, LNCS 7227, pp. 282–289, 2012. Springer-Verlag Berlin Heidelberg 2012.
105. Ortmann, J., Limbu, M., Wang, D. and Kauppinen, T. (2011). Crowdsourcing Linked Open Data for Disaster Management, Institute for Geoinformatics, University of Muenster, Germany.
106. Halder, B. 2013. SMS2FAX: A Tool to Enhance Public Service in Emergency Situation. International Journal of Computer and Communication Technology, ISSN (PRINT): 0975 - 7449, Volume-4, Issue-3, 2013. p 16-21.
107. Halder, B. 2014. CrowdCriMa - a complete Next Generation Crowsourced Crisis Management Platform. Accessed on 07/06/2015 and available at http://bit.ly/1WjOyuW

108. Imran, M., Castillo, C., Lucas, J., Meier, P. and Vieweg, S. (2014). AIDR: Artificial Intelligence for Disaster Response presented at WWW'14 Companion, April 7–11, 2014, Seoul, Korea. ACM 978-1-4503-2745-9/14/04. http://dx.doi.org/10.1145/2567948.2577034.
109. Amnesty International, (2013). Aleppo satellite images show devastation, mass displacement one year on. Accessed on 08/10/2014 and available at http://bit.ly/1PjlRJ3
110. Meier, P. (2014). On UAVs for Peacebuilding and Conflict Prevention. Available at http://bit.ly/1t6ueAD and Accessed on 10/11/2014
111. Robinson. A. C. (2014). Emerging Theme: UAVs and DIY Drones, Planning GIS for Emergency Management. Penn State University, 2014. Accessed on 08/10/2014. Available at https://www.e-education.psu.edu/geog588/l2_p5.html
112. Ezequiel, C A F., Cua, M., Libatique, N. C., Tangonan, G. L., Alampay, R., Labuguen, R. T., Favila, C. M., Honrado, J.L.E., Ca˜nos, V., Devaney, C., Loreto, A. B., Bacusmo, J. and Palma, B. (2014). UAV Aerial Imaging Applications for Post-Disaster Assessment, Environmental Management and Infrastructure Development. 2014 International Conference on Unmanned Aircraft Systems (ICUAS). May 27-30, 2014. Orlando, FL, USA. p. 274-283.
113. Glasscoe, M.T., Wang,J., Pierce, M.E., Yoder, M.R., Parker, W., Burl, M. C., Stough, T.M., Granat, R.A., Donnelan, A., Rundle, J.B., Ma, Y., Bawden, G. W., and Yuen, K., E-DECIDER: Using Earth Science Data and Modeling Tools to Develop Decision Support for Earthquake Disaster Response, Pure Appl. Geophys., April 2014.
114. Susaki, J., Region-based automatic mapping of tsunami-damaged buildings using multi-temporal aerial images, Nat Hazards (2015) 76:397–420.
115. Mancini, F., Capra, A., Castagnetti,C., Ceppi, C., Bertacchini, E., and Rivola, R., Contribution of Geomatics Engineering and VGI

Within the Landslide Risk Assessment Procedures, O. Gervasi et al. (Eds.): ICCSA 2015, Part II, LNCS 9156, pp. 635–647, 2015.
116. Radianti, J., Granmo, O.C, Sarshar, P., Goodwin, M., Dugdale, J, Gonzalez, J.J., A spatio-temporal probabilistic model of hazard- and crowd dynamics for evacuation planning in disasters, Appl Intell (2015) 42:3–23.
117. Tehrany, M.S., Lee, M.J., Pradhan, B., Jebur, M.N., Lee, S., Flood susceptibility mapping using integrated bivariate and multivariate statistical models, Environ Earth Sci (2014) 72:4001–4015.
118. Chou, J.S. and Lee, C.M., Integrating the geographic information system and predictive data mining techniques to model effects of compound disasters in Taipei, Nat Hazards (2014) 70:1385–1415.
119. Sadiq, F.I., Selamat, A. and Ibrahim, R., Human Activity Recognition Prediction for Crowd Disaster Mitigation, N.T. Nguyen et al. (Eds.): ACIIDS 2015, Part I, LNAI 9011, pp. 200–210, 2015.
120. Mahdipour, E. and Dadkhah, C., Automatic fire detection based on soft computing techniques: review from 2000 to 2010, Artif Intell Rev (2014) 42:895–934.
121. Konev, A., Waser, J.,Sadransky,B., Cornel, D., Perdigão, R.A.P., Horváth, Z., and Gröller, M.E., Run Watchers: Automatic Simulation-Based Decision Support in Flood Management, IEEE Transactions on Visualization and Computer Graphics, Vol. 20, no. 12, December 2014.
122. Foresti, G.,L., Farinosi, M. and Vernier, M., Situational awareness in smart environments: socio-mobile and sensor data fusion for emergency response to disasters, J Ambient Intell Human Comput, 6:239–257 (2015).
123. Kefalas, P., Sakellariou,I., Basakos, D. and Stamatopoulou, I, A Formal Approach to Model Emotional Agents Behaviour in Disaster Management Situations, A. Likas, K. Blekas, and D. Kalles (Eds.): SETN 2014, LNAI 8445, pp. 237–250, 2014.

124. Opinion 01/2015 of the Article 29 data Protection Working Party on Privacy and Data Protection Issues relating to the utilisation of Drones, 16 June 2015 (01673/15/EN, WP 231).
125. United Nations, (2015), Preamble of the Sendai Framework for Disaster Risk Reduction 2015-2030', (A/CONF.224/L.2) the final outcomes of the Third United Nations World Conference on Disaster Risk held in March 2015.
126. United Nations, (2013), 'Report on the International Expert Meeting on Crowdsource Mapping for Disaster Risk Management and Emergency Response carried out in the framework of the United Nations Platform for Space-based Information for Disaster Management and Emergency Response' (UN-SPIDER) Report No. A/AC.105/C.1/2013/CRP.5 presented by the Committee on the Peaceful Uses of Outer Space Scientific and Technical Subcommittee at Fiftieth Session in Vienna during 11-22 February 2013.
127. Kiyomoto, S., Fukushima, K. and Miyake, Y. (2014), 'Security issues on IT systems during disasters: a survey', Journal of Ambient Intelligence and Humanized Computing (2014) 5:173–185.
128. The LifeNet Project (2011) LifeNet. Accessed on 12/07/2015 from http://www.thelifenetwork.org/about.html.
129. Basu, S., Bhattacharjee, S., Roy, S. and Bandyopadhyay, S. (2015), 'SAGE-PRoPHET: A Security Aided and Group Encounter based PRoPHET Routing Protocol for Dissemination of Post Disaster Situational Data', ICDCN'15 January 04 – 07-2015, Goa, India.
130. Hughes, A.L. Peterson, S., and Palen, L. (2014), 'Social media in emergency management. In Issues in Disaster Science and Management: A Critical Dialogue Between Scientists and Emergency Managers'. FEMA in Higher Education Program.
131. Tapia, A. H and Moore, K., (2014), 'Good Enough is Good Enough: Overcoming Disaster Response Organizations' Slow

Social Media Data Adoption', Computer Supported Cooperative Work (CSCW) (2014) 23:483–512.

132. Cuijpers, C., Nadezhda, N. and Eleni, K., (2014), 'Data Protection Reform and the Internet: The Draft Data Protection Regulation'. Forthcoming in Savin, A., Trzaskowski, J., (eds) Research Handbook on EU Internet Law (Edward Elgar 2014); Tilburg Law School Research Paper No. 03/2014. Available at SSRN: http://bit.ly/1qrLePx
133. Article 29, Data Protection Working Party. European Commission. Directorate C (Fundamental Rights and Union Citizenship). Available at http://ec.europa.eu/justice/data-protection/index_en.htm; Accessed on 12/07/2015.
134. Pan, R.K., Sarama, J., Jo, H., Mitrovic, M., and Palchykov, V. (2014). Inferring human mobility using communication patterns. www.nature.com/scientificreports. DOI: 10.1038/srep06174.
135. Oguri, H. and Sonehara, N. (2014), A k-anonymity method based on search engine query statistics for disaster impact statements, 9th International Conference on Availability, Reliability and Security, 2014.
136. Pham T.T.H., Apparicio P., Gomez C., Weber C. and Mathon, D. (2014), 'Towards a rapid automatic detection of building damage using remote sensing for disaster management', Disaster Prevention and Management, Vol. 23 Iss 1 (2014) pp. 53-66.
137. 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 (2014) 167–179.
138. Lue, E., Wilson J.P. and Curtis, A. (2014),'Conducting disaster damage assessments with Spatial Video, experts, and citizens', Applied Geography 52 (2014) 46-54.
139. Thomson, R., Ito, N., Suda, H., Lin, F., Liu, Y. Hayasaka, R., Isochi, R., and Wang, Z. (2012), 'Trusting tweets: The Fukushima disaster and information source credibility on Twitter'. In Proceedings of ISCRAM. 2010.

140. Imran, M., Carlos, C., Diaz, F., and Vieweg, S. (2015), 'Processing social media messages in mass emergency: A survey'. ACM Comput. Surv. 47, 4, Article 67 (June 2015), DOI: http://dx.doi.org/10.1145/2771588
141. Gupta, A., Kumaraguru, P., Castillo, C., and Meier, P. (2014), 'TweetCred: Real-time credibility assessment of content on Twitter'. In Proceedings of SocInfo. Springer, 228–243.
142. Ludwig, T., Reuter, C., and Pipek, V. (2015), 'Social haystack: Dynamic quality assessment of citizen-generated content during emergencies', ACM Trans. Comput.-Hum. Interact. 22, 4, Article 17 (June 2015).
143. Popoola, A., Krasnoshtan, D., Toth, A., Naroditskiy, V., Castillo, C., Meier, P. and Rahwan, I. (2013), Information verification during natural disasters. In Proceedings of WWW (Companion). IW3C2, 1029–1032.
144. Ludwig, T., Siebigteroth, T., and Pipek, V. (2015), 'CrowdMonitor:Monitoring physical and digital activities of citizens during emergencies'. In Proceedings of CHI. 421–428.
145. Ludwig, T., Reuter, C., Siebigteroth, T., Pipek, V. (2015), 'CrowdMonitor: Mobile Crowd Sensing for Assessing Physical and Digital Activities of Citizens during Emergencies', CHI 2015, April 18 – 23, 2015, Seoul, Republic of Korea. ACM 978-1-4503-3145-6/15/04.
146. McCreadie, R., Kappler, K., Kardara, M., Kaltenbrunner, A., Macdonald, C., Soldatos, J. and Ounis, J. (2015). SUPER: Towards the use of Social Sensors for Security Assessments and Proactive Management of Emergencies. In Proceedings of International World Wide Web Conference Committee (IW3C2). WWW 2015 Companion, May 18–22, 2015, Florence, Italy. ACM 978-1-4503-3473-0/15/05.
147. Veil, R.V., Buehner, T., and Palenchar, M. J. (2011), A work-in-process literature review: Incorporating social media in risk and crisis communication. Journal of Contingencies and Crisis Management 19, 2, 110–122.

148. Varga, I., Sano, M., Torisawa, K., Hashimoto, C., Ohtake, K., Kawai, T., Oh, J.H. and Saeger, S.D. (2013), 'Aid is out there: Looking for help from tweets during a large scale disaster'. In Proceedings of ACL. 1619–1629.
149. Purohit, H., Castillo, C., Diaz, F., Sheth, A., and Meier, P. (2013), 'Emergency-relief coordination on social media: Automatically matching resource requests and offers. FirstMonday (2013).
150. Pipek, V., Liu, S., and Kerne, A. (Eds.) (2014), 'Special Issue: Crisis Informatics and Collaboration. Computer Supported Cooperative Work', Vol. 23, Issue 4-6 (2014).
151. Bruns. A. (2014), 'Crisis communication. The Media and Communications in Australia', 351–355.
152. Boin, A. and Bynander, F. (2015), 'Explaining success and failure in crisis coordination'. Geografiska Annaler: Series A, Physical Geography, 97, 123–135. doi:10.1111/geoa.12072
153. Velásquez, C.A, Cardona, O.D.,Mora, M.G.,Yamin, L.E.,Carreño, M.l. and Barbat, H.A. (2014), 'Hybrid loss exceedance curve (HLEC) for disaster risk assessment', Nat Hazards (2014) 72:455–479.
154. Novelo-Casanova, D.A. and Suárez, G. (2015), 'Estimation of the Risk Management Index (RMI) using statistical analysis', Nat Hazards (2015) 77:1501–1514.
155. Jeon,S.-S. (2014), 'Areas vulnerable to natural disasters and damage estimation of infrastructure'. In Busan, Korea, J. Central South University. (2014) 21: 1499−1507.
156. Satake, K. (2014), 'Advances in earthquake and tsunami sciences and disaster risk reduction since the 2004 Indian ocean tsunami', Geoscience Letters 2014, 1:15.
157. Avvenuti, M., Cresci, S., Marchetti, A., Meletti, C., Tesconi, M. (2014), 'EARS (Earthquake Alert and Report System): a Real Time Decision Support System for Earthquake Crisis Management', KDD'14, August 24–27, 2014, New York, NY, USA.

158. Song,X., Zhang, Q., Sekimoto Y. and Shibasaki R. (2014), 'Prediction of Human Emergency Behavior and their Mobility following Large-scale Disaster', KDD'14, August 24–27, 2014, New York, NY, USA.
159. Ben Othman, S., Zoghlami, N., Hammadi, S. and Zgaya, H. (2014), 'Adaptive Collaborative Agent-based System for Crisis Management', 2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT).
160. Chandler, D. (2015), 'A World without Causation: Big Data and the Coming of Age of Posthumanism', Millennium: Journal of International Studies 2015, Vol. 43(3) 833–851.
161. Lindskov Jacobsen, K. (2015), 'Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees', Security Dialogue, 2015, Vol. 46(2) 144–164.
162. Meier, P. (2013), 'Data Protection Protocols for Crisis Mapping'. Available at http://irevolution.net/2013/04/11/data-protection-for-crisis-mapping/. Accessed 12/05/2015.
163. Tang,Z., Zhang, L. and Xu, F. and Vo, H., Examining the role of social media in California's drought risk management in 2014, Nat Hazards (2015) 79:171–193.
164. Xu, Z., Liu, Y., Xuan, J., Chen, H., and Mei1, L., Crowdsourcing based social media data analysis of urban emergency events, Multimed Tools Appl, 27-06-2015, 1-18.
165. Mancini, F., Capra1, A., Castagnetti1, C., Ceppi, C., Bertacchini, E., and Rivola, R., Contribution of Geomatics Engineering and VGI Within the Landslide Risk Assessment Procedures, O. Gervasi et al. (Eds.): ICCSA 2015, Part II, LNCS 9156, pp. 635–647, 2015.
166. Ballatore, A. and Zipf, A. A Conceptual Quality Framework for Volunteered Geographic Information, S.I. Fabrikant et al. (Eds.): COSIT 2015, LNCS 9368, pp. 89–107, 2015.
167. Yue, P., Baumann, P., Bugbee, K. and Jiang, L., Towards intelligent GIServices, Earth Sci Inform (2015) 8:463–481.

168. Meier, P. (2013), ‘Data Protection Protocols for Crisis Mapping’. IrevolutionBlog.
169. Chandrasekaran, V., Rajan, S.V., Vasani, R.K., Menon, A., Bagavathi Sivakumar P. and Shunmuga Velayutham, C., A Crowdsourcing - Based Platform for Better Governance, L.P. Suresh and B.K. Panigrahi (eds.), Proceedings of the International Conference on S oft Computing Systems, Advances in Intelligent Systems and Computing, 397.
170. Whybark, C., Co-creation of improved quality in disaster response and recovery, International Journal of Quality Innovation (2015) 1:3.
171. Foresti, G. L., Farinosi, M. and Vernier, M., Situational awareness in smart environments: socio-mobile and sensor data fusion for emergency response to disaster, J Ambient Intell Human Comput (2015) 6:239–257.
172. Sarshar, P., Nunavath, V. and Radianti, J., On the Usability of Smartphone Apps in Emergencies. An HCI Analysis of GDACSmobile and SmartRescue Apps, M. Kurosu (Ed.): Human-Computer Interaction, Part II, HCII 2015, LNCS 9170, pp. 765–774, 2015.
173. García-Santa, N., García-Cuesta, E., and Villazón-Terrazas, B., Controlling and Monitoring Crisis, F. Gandon et al. (Eds.): ESWC 2015, LNCS 9341, pp. 46–50, 2015.
174. Xu, Z., Zhang, Hui, Sugumaran, V., Choo, K.-K. R., Mei, L. and Zhu, Y,, Participatory sensing-based semantic and spatial analysis of urban emergency events using mobile social media, Xu et al. EURASIP Journal on Wireless Communications and Networking (2016) 2016:44.
175. Ludwig, T., Siebigteroth, T. and Pipek, V., CrowdMonitor: Monitoring Physical and Digital Activities of Citizens during Emergencies, L.M. Aiello and D. McFarland (Eds.): SocInfo 2014 Workshops, LNCS 8852, pp. 421–428, 2015.
176. Beigi, G., Hu, X., Maciejewski, R., and Liu, H., An Overview of Sentiment Analysis in Social Media and Its Applications in

Disaster Relief, in W. Pedrycz and S.-M. Chen (eds.), Sentiment Analysis and Ontology Engineering, Studies in Computational Intelligence, 639, 2016.
177. Burns, Ryan, Rethinking big data in digital humanitarianism: practices, epistemologies, and social relations, GeoJournal (2015) 80:477–490.
178. Quinn, S., Using small cities to understand the crowd behind OpenStreetMap, GeoJournal, 09.12-2015, 1-19.
179. Luz N., Silva, N. and Novais, P., A survey of task-oriented crowdsourcing, Artif Intell Rev (2015) 44:187–213.
180. Aitsi-Selmi, A., Murray, V., Wannous, C., Dickinson, C., Johnston, D., Kawasaki, A., Stevance, A.-S.,Yeun, T., Reflections on a Science and Technology Agenda for 21st Century Disaster Risk Reduction Based on the Scientific Content of the 2016 UNISDR Science and Technology Conference on the Implementation of the Sendai Framework for Disaster Risk Reduction 2015–2030, Int J Disaster Risk Sci (2016) 7:1–29.
181. Mechler, R., Reviewing estimates of the economic efficiency of disaster risk management: opportunities and limitations of using risk-based cost–benefit analysis, Nat Hazards (2016) 81:2121–2147.
182. Martel,J.C., Exploring the integration of energy efficiency and disaster management in public policies and program, Energy Efficiency (2016) 9:533–543.
183. Ullah, R., Shivakoti, G.P., Kamran, A., Zulfiqar, F., Farmers versus nature: managing disaster risks at farm level, Nat Hazards, 14-03-2016.
184. Schinko, T., Mechler, R., and Hochrainer-Stigler, S., A methodological framework to operationalize climate risk management: managing sovereign climate-related extreme event risk in Austria, Mitig Adapt Strateg Glob Change, 19-04-2016.
185. Rosas, E., Hidalgo, N., Gil-Costa, V.,, Bonacic, C., Marin, M., Senger, H., Arantes, L., Marcondes, C., and Marin, O., Survey on Simulation for Mobile Ad-Hoc Communication for Disaster

Scenarios, Journal of Computer Science And Technology 31(2): 326–349 Mar. 2016.
186. Ramchurn, S.D., Wu, F., Jiang, W., Fischer, J.E., Reece, S., Roberts, S., Rodden, T., Greenhalgh, C., and Jennings, N.R., Human–agent collaboration for disaster response, Auton Agent Multi-Agent Syst (2016) 30:82–111.
187. Soto, A., Deriving information on disasters caused by natural hazards from limited data: a Guatemalan case study, Nat Hazards (2015) 75:71–94.
188. Bastian, N.D., Griffin, P.M., Spero, E., and Fulton, L.V., Multi-criteria logistics modeling for military humanitarian assistance and disaster relief aerial delivery operations, Optim Lett, 11-04-2015.
189. Ajmar, A., Boccardo, P., Disabato, F. and Tonolo F. G., Rapid Mapping: geomatics role and research opportunities, Rend. Fis. Acc. Lincei (2015) 26 (Suppl 1):S63–S73.
190. Crawford, K. and Finn, M., The limits of crisis data: analytical and ethical challenges of using social and mobile data to understand disasters, GeoJournal (2015) 80:491–502.
191. Hapuarachchi, A. B., Hughey, K., Rennie1, H., Effectiveness of Environmental Impact Assessment (EIA) in addressing development- induced disasters: a comparison of the EIA processes of Sri Lanka and New Zealand, Nat Hazards (2016) 81:423–445.
192. Report of the Secretary-General for the World Humanitarian Summit, One humanity: shared responsibility, 2 February 2016.

ANNEXES

List of published papers

(PhD Chapters)

1. Evolution of Crowdsourcing: Potential Data Protection, Privacy and Security Concerns under the New Media Age published in Democracia Digital e Governo Eletrônico, Florianópolis. Available at http://www.buscalegis.ccj.ufsc.br/revistas/index.php/observatoriodoegov/article/viewFile/34341/33195
2. Crisis Informatics: From Crowdsourcing to Crowdsourced Data analytics, published in Indian Streams Research Journal available http://isrj.org/ViewPdf.aspx?ArticleID=8500
3. Crowd-sourced Crisis Data: Ethical and Legal Concerns, published in European Academic Research available at http://euacademic.org/UploadArticle/2670.pdf
4. Privacy, Security and Data Protection in Crowdsourcing Platforms: Issues and Recommendations published in Weekly Science- International Research Journal available at http://weeklyscience.org/UploadedArticle/248.pdf

Other Publications:

5. Halder B: Crowdsourcing Collection of Data for Crisis Governance in the Post-2015 World: Potential Offers and Crucial Challenges. 8th International Conference on Theory and Practice of Electronic Governance, Guimaraes, Portugal, 2014. Proceedings by Association for Computing Machinery, ACM Press (ISBN 978-1-60558-611-3). 2014.

6. Halder, B. 2013. SMS2FAX: A Tool to Enhance Public Service in Emergency Situation. International Journal of Computer and Communication Technology, ISSN (PRINT): 0975 - 7449, Volume-4, Issue-3, 2013. p 16-21.
7. Halder, B. 2014. Crowdsourcing collection of data for crisis governance in the post-2015 world: potential offers and crucial challenges. In Proceeding ICEGOV '14 Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance. ACM New York, NY, USA ©2014.
8. Halder, B. Crowdsourcing for Social Change in the Global South: Challenges and Possibilities. In: International Conference for e-Democracy and Open Government, 2. Krems. Proceedings. Krems: Edition Donau-Universität Krems, 2013. p. 473-474.
9. Halder, B., Crowdsourcing collection of data for crisis governance in the post-2015 world: potential offers and crucial challenges, Proceeding ICEGOV '14 Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance. ACM New York, NY, USA. 2014.
10. Halder, B., Measuring Security, Privacy and Data Protection in Crowdsourcing. Published in SSRN, 2014.

List of Tables:

Identification of Risks

Retrieval and Selection (RS)

Table 1: Information / Data Retrieval

Sl No	Privacy, Security and Data Protection components	USH	DHN	MM	**GCM**
1	Presence of Encryption technology	N	PY	PY	PY
2	Standard verification process	PY	Y	Y	PY
3	Data filtering facilities	PY	Y	Y	Y
4	Privacy-preserving information systems authentication and broadcasting norms	NIF	NIF	NIF	NIF
5	Privacy preserving data mining procedures	N	PY	PY	N
6	Whether crowdsourcing platforms are using different tools those trust level were announced publicly by the developers	N	N	N	N
7	PET[52] principles in terms of geolocation identification	PY	PY	PY	PY
8	Trusted network access for communication tools	N	PY	Y	Y

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

[52] Privacy Enhancing Technologies

Table 2: Information / Data Selection

Sl No	Privacy, Security and Data Protection components	USH	DHN	MM	GCM
1	Cross-checking data and information	PY	Y	Y	N
2	Two steps verification process	N	Y	Y	N
3	PET principles in terms of geolocation identification	PY	PY	PY	PY
4	Trusted network access for communication tools	N	PY	Y	Y

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Table 3: Information / Data Storage

Sl No	Privacy, Security and Data Protection components	USH	DHN	MM	GCM
1	Encryption technology integration	N	PY	PY	PY
2	PET enabled data backups	N	PY	Y	Y
3	Trusted network access for communication tools	N	PY	Y	Y
4	Additional safeguards for sensitive personal data.	N	PY	Y	Y
5	Data stored in a locked cabinet	NIF	NIF	NIF	NIF
6	Data stored on a password protected and encrypted hard drive	NIF	NIF	NIF	NIF
7	The device should be in a locked room	NIF	NIF	NIF	NIF
8	Checking data integrity of stored data files regularly	NIF	NIF	NIF	NIF

9	Using different formats of storage (e.g. hard disk/DVD)	NIF	NIF	NIF	NIF
10	Labelling of stored data in order to facilitating physical accessibility and location	NIF	NIF	NIF	NIF
11	Areas and rooms for storage of digital data should fit risk prevention regulations (e.g. flood and fire)	NIF	NIF	NIF	NIF
12	Only responsible persons have access to stored data	NIF	NIF	NIF	NIF
13	Enable secure remote access to confidential data but avoiding the possibility to download data	NIF	NIF	NIF	NIF
14	Research works are conducted under the Statistical Disclosure Control carried out by a trained Service Staff	NIF	NIF	NIF	NIF
15	Data usage beyond the life of the crisis closely supervised	Y	PY	PY	N
16	Locking computer systems with a password and installing a firewall system	NIF	NIF	NIF	NIF
17	Servers are protected through line-interactive uninterruptible power supply systems (UPS)	NIF	NIF	NIF	NIF
18	Implementation of password protection and control access to data files (e.g. no access, read only permission, administrator-only permission, etc.)	NIF	NIF	NIF	NIF
19	Controlling access to restricted materials with encryption	NIF	NIF	NIF	NIF

20	Using non-disclosure agreements for managers or users of confidential data.	Y	Y	Y	Y
21	Encrypted data transmission, avoiding non-encrypted methods as e-mail, FTP protocol and so on.	NIF	NIF	NIF	NIF
22	Data destruction in a proper and consistent manner at the end of the crisis management project.	NIF	NIF	NIF	NIF
23	Confidential data stored in a server without access to the Internet.	NIF	NIF	NIF	NIF
24	Operating systems and anti-virus software in crowdsourcing platforms regularly updated in order to avoid viruses and malicious codes.	NIF	NIF	NIF	NIF
25	Backups stored offline (CD/DVD, pen-drive, removable hard-drive, etc.) or on a networked hard disk.	NIF	NIF	NIF	NIF
26	Critical and sensitive data files backed-up daily, using an automated back-up process, preferably stored offline	NIF	NIF	NIF	NIF
27	Master copies of critical and sensitive files made in open formats which facilitate long-term usage	NIF	NIF	NIF	NIF
28	All back-up files validated regularly	NIF	NIF	NIF	NIF

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Situational Awareness (SA)

Table 4: Coordination with volunteers

Sl No	Privacy, Security and Data Protection components	USH	DHN	MM	GCM
1	Options to be ‘anonymous’; not to disclose locations	PY	Y	Y	N
2	Choosing email or phone as the first point of contact	Y	Y	Y	Y
3	PET principles in terms of geolocation identification	N	NIF	NIF	NIF
4	Trusted network access for communication tools	N	PY	Y	Y
5	Maintaining a detailed log of actions related to user accounts plus regular audits regarding their validity, access rights and roles.	NIF	NIF	NIF	NIF
6	Logging of user actions at a particular crowdsourcing deployment database	NIF	NIF	NIF	NIF
7	Whether handling of information containing personal details is being done in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection?	NIF	NIF	NIF	NIF
8	Whether standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or data	NIF	NIF	NIF	NIF

	destruction process in accordance with the rules and principles of relevant laws on individual data protection?				
9	Guidelines for the crisis reporters and other users including journalists.	N	N	N	N

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Table 5: Collaboration among agencies

Sl No	Privacy, Security and Data Protection components	USH	DHN	MM	GCM
1	Trusted network access for communication tools	N	PY	Y	Y
2	PET applied for common coordination platform	N	PY	PY	PY
3	Establish and document a personal data breach handling procedure.	PY	Y	Y	Y
4	Private companies can collect data in the form of online survey, using third party apps etc. from any online platforms including crowdsourcing platforms	PY	N	N	Y
5	Disclosing of real names, locations of victims in man-made crisis is banned for all forms of media	NIF	NIF	NIF	NIF

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Table 6: Collaboration between volunteers and different agencies

Sl No	Privacy, Security and Data Protection components	USH	DHN	MM	GCP
1	Common coordination platform between government agencies and NGOs to deal with in humanitarian crisis	PY	PY	PY	PY
2	Trusted network access for communication tools	N	PY	Y	Y
3	Any established procedure for the secure destruction of personal data	NIF	NIF	NIF	NIF
4	Whether reuse requires quality control on the crowdsourced data.	NIF	NIF	NIF	NIF
5	Whether legal validation of the procedure is required to reuse data.	NIF	PY	Y	Y
6	Any option to set up internal and independent supervisory bodies	NIF	NIF	NIF	NIF

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Decision Support Systems (DSS)

Table 7: Decision- making by human intelligence

Sl No	Privacy, Security and Data Protection components	USH	DHN	MM	GCP
1	Solution Support Teams (SST) for every crisis response work.	Y	Y	Y	Y
2	Validation by first response team	Y	Y	Y	Y
3	Cross-Checking methodology in place to make decisions in a consistent manner	PY	PY	Y	PY
4	SST keeps logs available for internal and external supervision on regular interval	PY	Y	Y	Y

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Table 8: Automatic decision-making

Sl No	Privacy, Security and Data Protection components	USH	DHN	MM	GCP
1	Whether any automatic cross-checking methodology is in place	N	N	N	N

2	Whether first response team does monitoring and cross-checking	N	PY	Y	PY
3	Any purpose limitation (only for disaster management) procedure available	NIF	NIF	NIF	NIF
4	Whether plans for upgrading hardware and software in regular basis	Y	Y	Y	Y
5	Whether any automatic system alerts integrated to generate further actions	N	N	N	Y
6	Whether crowdsourcing platforms are using different tools those trust level were announced publicly by the developers	N	N	N	N
7	Whether PET integration allows crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as ‘anonymous’.	Y	Y	Y	PY

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Ethical and Legal Concerns

Security and Privacy-preserving Data Retrieval and Selection

Table 9: Risk-solution general guidelines

Risks	Possible Solutions
Security breaks: cyber-attacks, nuisance attacks, Mass surveillance	Trusted network access, authentication, encryption, data backups, privacy-preserving information systems authentication broadcasting
Quality and accuracy of data	Filtering, cross-checking, verification by the crowd
Personal Information Disclosure, location management, sensitive data	Mask up, forwarding, obfuscation, perturbation; Additional safeguards for sensitive data
Profiling with data mining	Privacy preserving data mining; Privacy Enhancing Technologies (PET)
Geolocation using sensors	PET for geolocation
User ranking and content classification	Cross-checking
Geo-referenced information	PET for geolocation
Lack of coordination between experts	Solution Support Teams

and volunteers	
Lack of collaboration between agencies	Context-aware multi-party coordination systems
Non-acceptance of SA services by users	Purpose limitation (only for disaster management)
Information collection and storage	PET
Reliability	Cross-Checking
Decision adversely affecting humans solely based on automatic DSS	First response team monitoring and cross-checking
Traceability of the automatic decision	Logs and internal and external supervision

Table 10: **Retrieval, selection and storage: recommendations on security and privacy**

Tasks	**Recommendations**
Information / Data Retrieval	• Encryption technology should be integrated with the crowdsourcing platform • Standard verification process by the crowd need to be established • Data filtering facilities should be integrated with the crowdsourcing platform • Privacy-preserving information systems authentication and broadcasting norms have to be applied • Privacy preserving data mining procedures needs to be in place • Tech companies that develop crowdsourcing tools that should publicly announce the

	'trust' level of the tool. • PET principles should be applied for determination of exact geolocation point of crisis reporters. • Trusted network access for communication tools have to be established.
Information / Data Selection	• The authenticity of data needs to be identified by cross-checking available information. • Two steps verification process needs to be done by the expert crowds i.e. volunteers. • PET principles should be applied for determination of exact geolocation point of incident. • Trusted network access for communication tools have to be established.
Information / Data Storage	• Encryption technology should be integrated with the crowdsourcing platform • PET enabled data backups facilities have to be developed • Trusted network access for communication tools have to be established • Additional safeguards must be ensured for sensitive personal data. • Data should be stored in a locked cabinet. • Crowdsourced data should be stored on a password protected and encrypted hard drive. • The device should be in a locked room.

	• Check data integrity of stored data files regularly. • Use different formats of storage (e.g. hard disk/DVD) • Label stored data in order to facilitating physical accessibility and location. • Areas and rooms for storage of digital data should fit risk prevention regulations (e.g. flood and fire) • Only responsible persons of core crisis response team members should have access to data. • Enable secure remote access to confidential data but avoiding the possibility to download data. • Publications regarding to the crisis response work must be conducted under the Statistical Disclosure Control carried out by a trained Service Staff. • Data usage beyond the life of the crowdsourcing crisis management project must be closely supervised. • Locking computer systems with a password and installing a firewall system are must. • Servers should be protected through line-interactive uninterruptible power supply systems (UPS). • Implementing password protection and control access to data files (e.g. no access, read only permission, administrator-only permission, etc.) • Controlling access to restricted materials with encryption.

	• Imposing non-disclosure agreements for managers or users of confidential data. • Data transmitted should be encrypted, avoiding non-encrypted methods as e-mail, FTP protocol and so on. • At the end of the crisis management project, data should be destroyed in a proper and consistent manner. • Computers that contain sensitive data should not be shifted (e.g. a knock in a hard disk may provoke a failure causing a breach of security). • Confidential data must be stored in a server without access to the Internet. • Operating systems and anti-virus software in crowdsourcing platforms should be updated in order to avoid viruses and malicious codes. • Backups can be stored offline (CD/DVD, pen-drive, removable hard-drive, etc.) or on a networked hard disk. • If needed, devices that contain a backup can be moved to another place to keep it safe. • Critical and sensitive data files should be backed-up daily, using an automated back-up process, preferably stored offline. • Master copies of critical and sensitive files should be made in open formats which facilitate long-term usage. • All back-up files should be validated regularly.

Table 11: **Coordination with volunteers and collaboration among agencies: recommendations on coordination**

Tasks	Recommendations
Coordination with volunteers	• Crowdsourcing reporters in humanitarian crisis must ask for options to be 'anonymous'; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as reporters will be able to apply these options if needed. • PET principles should be applied for determination of exact geolocation point of crisis reporters. • Trusted network access for communication tools have to be established. • Need to maintain a detailed log of actions related to user accounts plus regular audits regarding their validity, access rights and roles. • User actions at a particular crowdsourcing deployment database should be logged. • Crisis governance coordinators must collect and handle information containing personal details in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection.

	• Crisis governance coordinators should establish standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection. • Crisis governance coordinators must not use any digital tool that has potential risk of security breach. • Crisis governance coordinators must develop guidelines for the crisis reporters and other users including journalists.
Collaboration among agencies	• Trusted network access for communication tools have to be established. • PET should be applied for common coordination platform • Establish and document a personal data breach handling procedure. • Private companies should not be allowed to illegally collect data in the form of online survey, using third party apps etc. from any online platforms including crowdsourcing platforms. Such type of illegal collection of personal data should be punishable by the Law. • Disclosing of real names, locations of victims in man-made crisis should be banned by the law and should be applicable for all forms of media.
Collaboration between	• A common coordination platform between government agencies and NGOs should be developed to deal with in humanitarian crisis.

volunteers and different agencies	• Media should develop their own 'Media Ethics' for crisis reporting with keeping in mind the privacy and security issues of victims. • Trusted network access for communication tools have to be established. • A specific procedure for the secure destruction of personal data should be established. • Law enforcement agencies should not monitor crowdsourcing process for crisis governance to identify 'evidences' illegally in the suspicion of future terrorist attack or conflict (in man-made crisis). • For counter-terrorism purpose governments could do so with prior judicial authorizations. • The reuse will require quality control on the crowdsourced data. • Some legal validation of the procedure will be required to reuse data. • Internal and independent supervisory bodies should be implemented.

Table 12: **Decision support systems: recommendations on automatic decision-making**

Tasks	**Recommendations**
Decision-making by human intelligence	• Solution Support Teams (SST) should be formed for every crisis response work. • First response team should validate.

	• Cross-Checking methodology should be in place to make decisions in a consistent manner. • SST should keep logs available for internal and external supervision on regular interval.
Automatic decision-making	• Automatic cross-checking methodology should be in place. • First response team monitoring and cross-checking tasks are must. • Purpose limitation (only for disaster management) procedure have to be applied. • A specific plan for upgrading hardware and software should be implemented. • The use of system integrity tools should enable deletion and reporting of changes applied on servers. • Automatic system alerts generating facilities need to be integrated • Tech companies that develop crowdsourcing tools should publicly announce the 'trust' level of the tool. • Tech companies should develop tools with PET integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as 'anonymous'.

Evaluation of the recommendations concerning retrieval, selection and storage

Table 13: General Recommendations on retrieval, selection and storage

Tasks	**Privacy, Security and Data Protection components**	**Different Crowdsourcing Platforms**				**General Recommendations**
		USH	**DHN**	**MM**	**GCM**	
Information / Data Retrieval	Presence of Encryption technology	N	PY	PY	PY	Encryption technology should be integrated with the crowdsourcing platform
	Standard verification process	PY	Y	Y	PY	Standard verification process by the crowd need to be established
	Data filtering facilities	PY	Y	Y	Y	Data filtering facilities should be integrated with the crowdsourcing platform
	Privacy-preserving	NIF	NIF	NIF	NIF	Privacy-preserving information systems

	information systems authentication and broadcasting norms					authentication and broadcasting norms have to be applied
	Privacy preserving data mining procedures	N	PY	PY	N	Privacy preserving data mining procedures needs to be in place
	Whether crowdsourcing platforms are using different tools those trust level were announced publicly by the developers	N	N	N	N	Tech companies that develop crowdsourcing tools that should publicly announce the 'trust' level of the tool.
	PET principles in terms of geolocation identification	PY	PY	PY	PY	PET principles should be applied for determination of exact geolocation point of crisis reporters.
	Trusted network	N	PY	Y	Y	Trusted network access for

	access for communication tools					communication tools have to be established.
Information / Data Selection	Cross-checking data and information	PY	Y	Y	N	The authenticity of data needs to be identified by cross-checking available information.
	Two steps verification process	N	Y	Y	N	Two steps verification process needs to be done by the expert crowds i.e. volunteers.
	PET principles in terms of geolocation identification	PY	PY	PY	PY	PET principles should be applied for determination of exact geolocation point of incident.
	Trusted network access for communication tools	N	PY	Y	Y	Trusted network access for communication tools have to be established.
Information /	Encryption	N	PY	PY	PY	Encryption technology should be

Data Storage	technology integration					integrated with the crowdsourcing platform
	PET enabled data backups	N	PY	Y	Y	PET enabled data backups facilities have to be developed
	Trusted network access for communication tools	N	PY	Y	Y	Trusted network access for communication tools have to be established
	Additional safeguards for sensitive personal data.	N	PY	Y	Y	Additional safeguards must be ensured for sensitive personal data.
	Data stored in a locked cabinet	NIF	NIF	NIF	NIF	Data should be stored in a locked cabinet.
	Data stored on a password protected and encrypted hard drive	NIF	NIF	NIF	NIF	Crowdsourced data should be stored on a password protected and encrypted hard drive.
	The device should	NIF	NIF	NIF	NIF	The device should be in a locked room.

	be in a locked room					
	Checking data integrity of stored data files regularly	NIF	NIF	NIF	NIF	Check data integrity of stored data files regularly.
	Using different formats of storage (e.g. hard disk/DVD)	NIF	NIF	NIF	NIF	Use different formats of storage (e.g. hard disk/DVD)
	Labeling of stored data in order to facilitating physical accessibility and location	NIF	NIF	NIF	NIF	Label stored data in order to facilitating physical accessibility and location.
	Areas and rooms for storage of digital data should fit risk prevention regulations (e.g. flood and fire)	NIF	NIF	NIF	NIF	Areas and rooms for storage of digital data should fit risk prevention regulations (e.g. flood and fire)

	Only responsible persons have access to stored data	NIF	NIF	NIF	NIF	Only responsible persons of core crisis response team members should have access to data.
	Enable secure remote access to confidential data but avoiding the possibility to download data	NIF	NIF	NIF	NIF	Enable secure remote access to confidential data but avoiding the possibility to download data.
	Research works are conducted under the Statistical Disclosure Control carried out by a trained Service Staff	NIF	NIF	NIF	NIF	Publications regarding to the crisis response work must be conducted under the Statistical Disclosure Control carried out by a trained Service Staff.
	Data usage beyond the life of the crisis closely supervised	Y	PY	PY	N	Data usage beyond the life of the crowdsourcing crisis management project must be closely supervised.

	Locking computer systems with a password and installing a firewall system	NIF	NIF	NIF	NIF	Locking computer systems with a password and installing a firewall system are must.
	Servers are protected through line-interactive uninterruptible power supply systems (UPS)	NIF	NIF	NIF	NIF	Servers should be protected through line-interactive uninterruptible power supply systems (UPS).
	Implementation of password protection and control access to data files (e.g. no access, read only permission, administrator-only	NIF	NIF	NIF	NIF	Implementing password protection and control access to data files (e.g. no access, read only permission, administrator-only permission, etc.)

	permission, etc.)					
	Controlling access to restricted materials with encryption	NIF	NIF	NIF	NIF	Controlling access to restricted materials with encryption.
	Using non-disclosure agreements for managers or users of confidential data.	Y	Y	Y	Y	Imposing non-disclosure agreements for managers or users of confidential data.
	Encrypted data transmission, avoiding non-encrypted methods as e-mail, FTP protocol and so on.	NIF	NIF	NIF	NIF	Data transmitted should be encrypted, avoiding non-encrypted methods as e-mail, FTP protocol and so on.
	Data destruction in a proper and consistent manner	NIF	NIF	NIF	NIF	At the end of the crisis management project, data should be destroyed in a proper and consistent manner.

	at the end of the crisis management project.					
	Confidential data stored in a server without access to the Internet.	NIF	NIF	NIF	NIF	Confidential data must be stored in a server without access to the Internet.
	Operating systems and anti-virus software in crowdsourcing platforms regularly updated in order to avoid viruses and malicious codes.	NIF	NIF	NIF	NIF	Operating systems and anti-virus software in crowdsourcing platforms should be updated in order to avoid viruses and malicious codes.
	Backups stored offline (CD/DVD, pen-drive, removable hard-	NIF	NIF	NIF	NIF	Backups can be stored offline (CD/DVD, pen-drive, removable hard-drive, etc.) or on a networked hard disk.

	drive, etc.) or on a networked hard disk.					
	Critical and sensitive data files backed-up daily, using an automated back-up process, preferably stored offline	NIF	NIF	NIF	NIF	Critical and sensitive data files should be backed-up daily, using an automated back-up process, preferably stored offline.
	Master copies of critical and sensitive files made in open formats which facilitate long-term usage	NIF	NIF	NIF	NIF	Master copies of critical and sensitive files should be made in open formats which facilitate long-term usage.
	All back-up files validated regularly	NIF	NIF	NIF	NIF	All back-up files should be validated regularly.

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Evaluation of the recommendations concerning retrieval, selection and storage

Table 14: General Recommendations on situational awareness

Tasks	**Privacy, Security and Data Protection components**	**Different Crowdsourcing Platforms**				**General Recommendations**
		USH	**DHN**	**MM**	**GCM**	
Coordination with volunteers	Options to be 'anonymous'; not to disclose locations;	PY	Y	Y	N	Crowdsourcing reporters in humanitarian crisis must ask for options to be 'anonymous'; not to disclose their location; and to choose email or phone as the first point of contact to minimize the risk to be targeted. Providing options for these would be rally helpful as reporters will be able to apply these options if needed.
	Choosing email or phone as the first point of contact	Y	Y	Y	Y	
	PET principles in terms of	N	NIF	NIF	NIF	PET principles should be applied for determination of exact geolocation point

	geolocation identification					of crisis reporters.
	Trusted network access for communication tools	N	PY	Y	Y	Trusted network access for communication tools have to be established.
	Maintaining a detailed log of actions related to user accounts plus regular audits regarding their validity, access rights and roles.	NIF	NIF	NIF	NIF	Need to maintain a detailed log of actions related to user accounts plus regular audits regarding their validity, access rights and roles.
	Logging of user actions at a particular crowdsourcing deployment	NIF	NIF	NIF	NIF	User actions at a particular crowdsourcing deployment database should be logged.

	database					
	Whether handling of information containing personal details is being done in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection?	NIF	NIF	NIF	NIF	Crisis governance coordinators must collect and handle information containing personal details in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection.
	Whether standard procedures on the crowdsourcing collection of data,	NIF	NIF	NIF	NIF	Crisis governance coordinators should establish standard procedures on the crowdsourcing collection of data, storing, re-use or exchange, archiving or

	storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection?					data destruction process in accordance with the rules and principles of relevant laws on individual data protection. Crisis governance coordinators must not use any digital tool that has potential risk of security breach.
	Guidelines for the crisis reporters and other users including journalists.	N	N	N	N	Crisis governance coordinators must develop guidelines for the crisis reporters and other users including journalists.
Collaboration among agencies	Trusted network access for communication tools	N	PY	Y	Y	Trusted network access for communication tools have to be established.

	PET applied for common coordination platform	N	PY	PY	PY	PET should be applied for common coordination platform
	Establish and document a personal data breach handling procedure.	PY	Y	Y	Y	Establish and document a personal data breach handling procedure.
	Private companies can collect data in the form of online survey, using third party apps etc. from any online platforms including crowdsourcing	PY	N	N	Y	Private companies should not be allowed to illegally collect data in the form of online survey, using third party apps etc. from any online platforms including crowdsourcing platforms. Such type of illegal collection of personal data should be punishable by the Law.

	platforms					
	Disclosing of real names, locations of victims in man-made crisis is banned for all forms of media	NIF	NIF	NIF	NIF	Disclosing of real names, locations of victims in man-made crisis should be banned by the law and should be applicable for all forms of media.
Collaboration between volunteers and different agencies	Common coordination platform between government agencies and NGOs to deal with in humanitarian crisis	PY	PY	PY	PY	A common coordination platform between government agencies and NGOs should be developed to deal with in humanitarian crisis.
	Trusted network access for communication tools	N	PY	Y	Y	Trusted network access for communication tools have to be established.

	Any established procedure for the secure destruction of personal data	NIF	NIF	NIF	NIF	A specific procedure for the secure destruction of personal data should be established.
	Whether reuse requires quality control on the crowdsourced data.	NIF	NIF	NIF	NIF	The reuse will require quality control on the crowdsourced data.
	Whether legal validation of the procedure is required to reuse data.	NIF	PY	Y	Y	Some legal validation of the procedure will be required to reuse data.
	Any option to set up internal and independent supervisory bodies	NIF	NIF	NIF	NIF	Internal and independent supervisory bodies should be implemented.

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found

Evaluation of the recommendations concerning Decision Support Systems

Table 15: General Recommendations on Decision support systems

Tasks	**Privacy, Security and Data Protection components**	**Different Crowdsourcing Platforms**				**General Recommendations**
		USH	**DHN**	**MM**	**GCM**	
Decision-making by human intelligence	Solution Support Teams (SST) for every crisis response work.	Y	Y	Y	Y	Solution Support Teams (SST) should be formed for every crisis response work.
	Validation by first response team	Y	Y	Y	Y	First response team should validate.
	Cross-Checking methodology in place to make decisions in a consistent manner	PY	PY	Y	PY	Cross-Checking methodology should be in place to make decisions in a consistent

						manner.
	SST keeps logs available for internal and external supervision on regular interval	PY	Y	Y	Y	SST should keep logs available for internal and external supervision on regular interval.
Automatic decision-making	Whether any automatic cross-checking methodology is in place	N	N	N	N	Automatic cross-checking methodology should be in place.
	Whether first response team does monitoring and cross-checking	N	PY	Y	PY	First response team monitoring and cross-checking tasks are must.
	Any purpose limitation (only for disaster management) procedure available	NIF	NIF	NIF	NIF	Purpose limitation (only for disaster management) procedure have to be applied.

	Whether plans for upgrading hardware and software in regular basis	Y	Y	Y	Y	A specific plan for upgrading hardware and software should be implemented.
	Whether any automatic system alerts integrated to generate further actions	N	N	N	Y	The use of system integrity tools should enable deletion and reporting of changes applied on servers. Automatic system alerts generating facilities need to be integrated
	Whether crowdsourcing platforms are using different tools those trust level were announced publicly by	N	N	N	N	Tech companies that develop crowdsourcing tools should publicly announce the ‘trust’ level of the tool.

	the developers					
	Whether PET integration allows crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as ‘anonymous’.	Y	Y	Y	PY	Tech companies should develop tools with PET integration to allow crisis reporters to have control over their location disclosure and to be given the capacity to choose to be recorded as ‘anonymous’.

Y= Yes, PY=Partially Yes; N = No, NIF= No Information found