Weekly Science
International Research Journal

ISSN: 2321-7871 Impact Factor : 2.4210(UIF) [Yr.2014] Volume - 3 | Issue - 48 | (9 June 2016)

PRIVACY, SECURITY AND DATA PROTECTION IN CROWDSOURCING PLATFORMS:ISSUES AND RECOMMENDATIONS

Buddhadeb Halder
Universitat Autònoma de Barcelona, Campus de la UAB, Plaza Cívica, s/n, 08193 Bellaterra, Barcelona, Spain.

ABSTRACT:

Following the birth of 'digital' crowdsourcing for crisis response, numbers of platforms have been developed by different crisis response to address crisis. At present the crisis informatics is based on crowdsourced data analytics - a combination of crowdsourcing retrieval and filtering, situational awareness and decision support systems. 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. 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. This paper aims to present those risks and offer recommendations for crowdsourcing disaster management platforms.

KEY WORDS: Privacy, Security, Data Protection, Crowdsourcing, Regulatory framework.

1. INTRODUCTION

The extensiveness and increasing access to the communication technologies and the growing interest in engaging 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 [1]. At the international level, a recently adopted framework called the Sendai Framework for Disaster Risk Reduction 2015-2030 have not discussed the potential risks of using emerging ICTs and crowdsourcing in disaster management [2]. 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 Meeting in February 2013 discussed about the use of crowdsourcing, issues and potential steps to take to deal with some existing issues [3].

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 analyze 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 [1].

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 and data 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. Thus, there is a need of a regulatory framework for crowdsourcing disaster management. On this background, this paper will identify a possible way to overcome these challenges in crowdsourcing crisis informatics.

2. PROBLEM STATEMENT

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. Research activities were lead to understand different ethical and legal issues in terms of privacy, data protection and security of crowdsourcing during crisis governance work. Thus, a research work was conducted among couple of crowdsourcing crisis management platforms to identify the potential risks and also to find possible solutions.

3. RESEARCH QUESTION

As some privacy and data protection and security concerns had been identified, the following main research question would guide this research article:

- What are the different privacy, security and data protection issues in crowdsourcing platforms?
- How to address these issues i.e. protect privacy, security and data protection in using crowdsourcing for crisis management?

4. RESEARCH METHODOLOGY

The total process of crowdsourcing crisis management could be divided into three different stages. The stages are a) Retrieval and Selection (RS); b) Situational Awareness (SA); and c) Decision Support Systems (DSS). During the literature review, it had been identified that numbers of different security, privacy and data protection components were very much linked when using crowdsourcing for crisis management. To understand those aspects within existing different crowdsourcing crisis management framework, a qualitative research study was conducted among Uhahidi, Digital Humanitarian Network, MicroMappers and Google Crisis Map.

4.1. Identification of crowdsourcing platforms and tools

Ushahidi (USH) was identified for the secondary research as this platform is considered as the pioneer and innovative crowdsourcing platform that paved the way for using ICT based crowdsourcing in crisis management works.Digital Humanitarian Network (DNH) was identified for the secondary research as at the time of conducting secondary research, it was the biggest network of Volunteer & Technical Communities of its' kind to leverage digital networks in support of humanitarian response. MicroMappers (MM) was selected for the research as it had started AI (Artificial Intelligence) for the first time to select data and information by users. Finally, the Google Crisis Map (GCP) was selected for this research to identify, having all latest technological facilities, how does GCP cares about privacy, security and data protection issues of users during any crisis.

5. RESEARCH OUTCOME

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.

Table 1:Risks and recommendations on security and privacy related to 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 information systems authentication and broadcasting norms	NIF	NIF	NIF	NIF	Privacy-preserving information systems 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 access for communication tools	N	PY	Y	Y	Trusted network access for 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 / Data Storage	Encryption technology integration	N	PY	PY	PY	Encryption technology should be 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 be in a locked room	NIF	NIF	NIF	NIF	The device should 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 permission, etc.)	NIF	NIF	NIF	NIF	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	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 at the end of the crisis management project.	NIF	NIF	NIF	NIF	At the end of the crisis management project, data should be destroyed in a proper and consistent manner.
	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-drive, etc.) or on a networked hard disk.	NIF	NIF	NIF	NIF	Backups can be stored offline (CD/DVD, pen-drive, removable hard-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

Table 2:Risks and recommendations related to 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 geolocation identification	N	NIF	NIF	NIF	PET principles should be applied for determination of exact geolocation point 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 database	NIF	NIF	NIF	NIF	User actions at a particular crowdsourcing deployment database should be logged.

	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, storing, re-use or exchange, archiving or data destruction process in accordance with the rules and principles of relevant laws on individual data protection?	NIF	NIF	NIF	NIF	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.
	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 platforms	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.
	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

Table 3: Decision support systems: recommendations on automatic decision-making

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 forinternal and external supervision on regular interval	PY	Y	Y	Y	SST should keep logs available forinternal 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 the developers	N	N	N	N	Tech companies that develop crowdsourcing tools should publicly announce the 'trust' level of the tool.
	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

Four relevant platforms had then been selected to investigate. 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-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 [6]. 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 [6]. 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.

The following recommendations are not fulfilled by platforms, and therefore the detected priorities for a crowdsourced disaster management are in a concrete regulation that would eventually implement this regulatory framework:

- On information and data retrieval, encryption is still not used or not properly used. Privacy preserving data mining 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.

As privacy, security and data protection risks were identified, some recommendations also made in table 1, table 2 and in table 3. The brief recommendations are as follows:

5.1 Retrieval, selection and storage

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 [7]. 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 [8]. 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) [9]. 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 [10]. Geographical Information Systems (GIS) are also becoming GIServices, including sensors, data, processing, portrayal, registry and chaining services [11]. Along with the GIS capabilities, the embedded technology like web and services, semantic web, sensing technologies, data-intensive computing and advanced analytics etc. are imroving. 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 [4]. 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.

5.2. Situational Awareness (SA)

Traditional situational awareness services are mainly focused on the institutional warning response [12]. 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 [13]. Only recently disaster management tries to exploit the active participation of citizens, with mobile data and smart sensors [14]. Smartphone apps and sensors provide new functionalities for emergency management [15].The design of the smartphone is now supposed to be adapted to a new use: emergency sensoring. So, a new field is born for mobile HCI (Human Computer Interaction). "Crowd as sensor" is complementing the previous "crowd as journalist" perspective [16].

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 [17]. 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 [18]. Sentiment analysis in social media is also recently taken into consideration for situation awareness and even for supporting decision making during the crisis [19].

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 [20]. 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 [21]. 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, for example the "contribution profiles"[21]. The data also greatly decrease in quantity andqualitywhenmovingoutsidemajorcities with active mapping communities.

Thus, 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 [5].

5.3 Decision Support Systems (DSS)

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 [22]. 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 [23]. 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 [24], disaster risk management at farms [25] and Climate Risk Management (CRM) [26]. 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 [27]. Multi-agent systems are also envisioned to guide first response teams in the near future [28]. But all these new rolesof 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 [29]. 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 [30]. 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 TomNodcontribute to analyse of post-event imagery. But the digital communities are now involved in off-line analyses to train supervised classification algorithms [31].

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.

6. CONCLUSIONS AND NEXT STEPS

Disasters are no longer viewed as only or mainly natural events, but more as the results of poor governance [32]. Disaster management is also considered a shared responsibility, an investment in humanity [33]. 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. The future work would be to develop general framework for crowdsourcing crisis informatics comprising with potential legal, ethical and technical solutions for the next generation crisis response work.

ACKNOWLEDGEMENTS

This paper is supported through a Doctoral Fellowship LAST-JD PhD program (www.last-jd.eu). The author would like to thank his supervisor Dr. Antoni Roig (IDT-UAB) for his support, guidance and feedback on this manuscript.

REFERENCES

[1] B. Halder, (2014), 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.

[2] 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.

[3] 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.

[4] 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.

[5] Luz N., Silva, N. and Novais, P., A survey of task-oriented crowdsourcing,Artif Intell Rev (2015) 44:187–213.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] Yue, P., Baumann, P., Bugbee, K. and Jiang, L., Towards intelligent GIServices, Earth Sci Inform (2015) 8:463–481.

[12] 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 Soft Computing Systems, Advances in Intelligent Systems and Computing, 397.

[13] Whybark, C.,Co-creation of improved quality in disasterresponse and recovery, International

Journal of Quality Innovation (2015) 1:3.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] Burns, Ryan, Rethinking big data in digital humanitarianism: practices, epistemologies, and social relations, GeoJournal (2015) 80:477–490.

[21] Quinn, S., Using small cities to understand the crowd behind OpenStreetMap, GeoJournal, 09.12-2015, 1-19.

[22] Aitsi-Selmi, A., Murray, V., Wannous, C., Dickinson, C., Johnston, D., Kawasaki, A., Stevance, A.-S.,Yeun, T., Re?ections on a Science and Technology Agenda for 21st Century Disaster Risk ReductionBased on the Scienti?c 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.

[23] Mechler, R., Reviewing estimates of the economic ef?ciency of disaster risk management: opportunities and limitations of using risk-based cost–bene?t analysis, Nat Hazards (2016) 81:2121–2147.

[24] Martel,J.C., Exploring the integration of energy efficiency and disaster management in public policies and program, Energy Efficiency (2016) 9:533–543.

[25] Ullah, R., Shivakoti, G.P., Kamran, A., Zul?qar, F.,Farmers versus nature: managing disaster risks at farm level,Nat Hazards, 14-03-2016.

[26] 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.

[27] 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.

[28] 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.

[29] Soto, A.,Deriving information on disasters caused by natural hazards from limited data: a Guatemalan case study, Nat Hazards (2015) 75:71–94.

[30] Bastian, N.D., Grif?n, 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.

[31] 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.

[32] 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.

[33] Report of the Secretary-General for the World Humanitarian Summit, One humanity: shared responsibility, 2 February 2016.