Crowdsourcing Collection of Data for Crisis Governance in the Post-2015 World: Potential Offers and Crucial Challenges

Buddhadeb Halder
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University, P.O. Box 90153, 5000 LE Tilburg, Netherlands
+31134663515
b.halder@uvt.nl

ABSTRACT

The practice of 'crowdsourcing' under the new technological regime has opened doors of huge data repositories. In recent 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. Crowdsourcing has the potentiality to offer smart governance by gathering and analyzing massive data from citizens. As data is a key enabler to proper public governance, this paper aims to provide a picture of potential offers that 'crowdsourcing' could make in support of crisis governance in the Post-2015 World, while it illustrates some critical challenges of data protection and privacy in different service sectors. Lastly, with a brief analysis on privacy, online data protection; and safety level of some crowdsourcing tools, this paper proposes brief guidelines for different stakeholders and some future works to avoid some mismanagement of crowdsourced data to protect data, privacy and security of end users.

Categories and Subject Descriptors

K.4.1. [**Public Policy Issues**]: *Abuse and crime involving computers, Ethics, Human safety, Privacy, Regulation, Transborder data flow Use/abuse of power*; H.3.5 [**Online Information Services**]: *Web-based services, Data sharing*.

General Terms

Documentation, Human Factors, Legal Aspects, Management, Measurement, Security, Standardization, Verification

Keywords

Data; Big Data; Public Governance; Crisis Governance; Privacy; Policy; Online Data Protection; PET

1. INTRODUCTION

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" [17]. However, the phenomenon of crowdsourcing is really an old one. The process of crowdsourcing was used as early as 1714. The British Government offered a Longitude Prize [39] of £20,000 for a simple and practical method of calculating a ship's longitude in 1714 [31]. Since then, crowdsourcing has helped creating some of the world's greatest inventions and biggest brands. In last 300 years- starting from 1714, the concept of 'crowdsourcing' process has been using for scientific innovation (i.e. Longitude Prize, 1714; Alkali from sea-salt, 1983; Canned food i.e. long-term food preservation, 1793; Margarine, 1869), design of buildings (i.e. Sydney Opera House, 1957) and logos of different brands (i.e. Planters Peanuts, 1916; Toyota Logo, 1936), fundraising (i.e. Just Giving, 2010); election monitoring (i.e. Kenya, 2007), asking for little help, developing / or amending constitutions (i.e. constitution amendment in Iceland, 2011) and coordinating disaster response activities and mapping of political conflicts (i.e. Syria 2011; Libya conflict, 2011) etc. However, over the last few years, crowdsourcing has expanded rapidly in the business world (i.e. web-based crowdsourcing- Amazon Mechanical Turk, 2005) and in the area of disaster response work (i.e. Haiti, 2010; Hurricane Sandy, 2012, Yolonda 2013), in active participation and discussion on public issues and etc.

The present 'New Media Age' helps citizens to exchange information, forming like-minded groups and coordinate actions with the help of low cost digital tools and services. 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 to use crowdsourcing for policy advocacy or amendment of the constitution; in e-government[1] and in e-democracy[2] [32]. The use of crowdsourcing in these sectors has grown exponentially across the planet. It has been identified that crowdsourcing approaches like the Knowledge Discovery and Management approach[3], the Distributed Human Intelligence

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICEGOV2014, October 27 - 30 2014, Guimaraes, Portugal
Copyright 2014 ACM 978-1-60558-611-3/14/10...$15.00
http://dx.doi.org/10.1145/2691195.2691208

[1] "E-Government" refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions. For more information, visit http://go.worldbank.org/M1JHE0Z280

[2] E-democracy is the use of information and communication technologies and strategies by "democratic sectors" within the political processes of local communities, states, regions, nations, and the global stage. See Reference [8].

[3] Example: SeeClickFix; USGS's Did You Feel It?; USPTO's Peer to Patent; and Possible Uses: Reporting conditions and use of public parks and hiking trails; tracking use of public transit;

Tasking approach[4], the Broadcast Search approach[5], and the Peer-Vetted Creative Production approach[6] are some suitable crowdsourcing approaches for public governance [4].

As in this research, which was based on secondary data, a special attention has been given on Crisis Governance in the Post 2015 World. Some real opportunities have been found in using crowdsourcing for crisis governance. It has been identified that at this moment using crowdsourcing process in crisis governance has three main types of benefits:

a) Reducing Reaction Time[7]

b) Enhancing Information Accuracy[8] and

c) Economic, Social and Human Benefits[9]

Crowdsourcing process has the potentiality to play significant roles in public governance while it has also been noticed that crowdsourcing is being used for 'illegal' surveillance purpose by different government departs in different parts of the world. For example, crowdsourcing has been used by the Law Enforcement Agencies to collect data on potential protest campaigns like Occupy Wall Street,[10] man-made crisis like London riot.[11] Different Law Enforcement Agencies in developed countries have the technical infrastructure to use crowdsourcing process to collect personal data. Sometimes they collect personal data of citizens who contribute in a different crowdsourcing platform for a different purpose hosted by third parties. The disclosures by NSA contractor Edward Snowden confirmed that governments are collecting personal data of citizens on regular basis.

Thus, concepts of different corwdsourcing process allow citizens to connect with each other, skilled and semi-skilled workers to get paid by doing jobs from remote, 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 questions arise from ethical and legal points of view. Thus, the main objective of this paper is to analyze different legal and ethical aspects of crowdsourcing process for various governance initiatives. It has been identified that there is a need of a regulatory framework for crowdsourcing as different important issues related to security and privacy, data ownership, and data protection etc. need to be dealt with proper measurement from legal and ethical aspects.

On this background, this paper will identify a possible way to overcome different legal and ethical challenges in crowdsourcing process for Crisis Governance in the Post-2015 world. In this paper, we intend to give a clear picture of how crowdsourcing could contribute in future Crisis Governance. Finally, a short Regulatory Framework for Post-2015 Crisis Governance will be developed while highlighting some beast practices in crowdsourcing for humanitarian crisis governance.

2. STATE OF THE ART

The explosive growth of information technologies across the world has given enormous power to the hands of common people. Earlier, in this paper, different potential offers of crowdsourcing process have been mentioned while serious concerns have been raised on issues like privacy, security and personal data protection in crowdsourcing process. In this section of this paper, some real world examples will be analyzed to understand different ethical and legal issues of crowdsourcing in crisis governance work.

2.1 What is in Offer for Crisis Governance in Post-2015 World?

The first well-known crowdsourcing process for crisis governance has been used in Kenya in 2008. Ushahidi[12] used mobile phones and the Internet to report violence following the 2007 presidential election in Kenya [19]. The Nairobi People's Settlement Network used mobiles and the Internet to get organised against evictions. They used what we would call 'flashmobbing' to call people from across the many different and rival settlements together where big evictions were planned, and threatened to sit down in front of the bulldozers [24]. Pakistani civil society organisations and activists used FrontlineSMS (an SMS-based system) to co-ordinate peace rallies and candlelight vigils against martial law.[13] The Women of Uganda Network's used social networking tools such as websites, email, SMS and mobile phones to reduce violence against women [26]. They used a variety of crowdsourcing process, tools and methods to receive reports and generate public awareness on several social issues. After the horrific rape incident on 16th December 2012 in Delhi, India, the 'Justice Verma Committee' was constituted by the Government of India Notification Number SO(3003)E, dated 23 December to look into possible amendments of the Criminal Law to provide for quicker trial and enhanced punishment for criminals committing sexual assault of extreme nature against women. Then the Committee directed the Ministry

cataloguing public art projects and murals for historical boards. See Reference [4].

[4] Example: Transcribing digital scans of old handwritten census records; Possible Uses: Language translation for documents and websites; data entry; behavioral modeling. See Reference [4].

[5] Example: White House SAVE Award; NASA's use of InnoCentive for a solar flare prediction formula; and Possible Uses: Finding better algorithms for timing traffic signals; improving actuarial formulas for Social Security. See Ref. [4].

[6] Example: Next Stop Design bus stop shelter design competition; ITS Congestion Challenge for alleviating traffic congestion; and Possible Uses: Designs for public structures and art projects; urban plans; transit plans; policy proposals; school redistricting plans. See Reference [4].

[7] For example: Early warning (conflict, other humanitarian crisis); Crowdsourcing helps to start rescue work quickly; It helps to mobilize the crisis response team quickly and it will contribute in quick decision making process during any crisis.

[8] For example: Actual information from the ground – Real time information; Helps to assess the situation time to time; Gaining Intelligence on potential threat of 'man-made disaster' by using Crowdsourcing / Spy Agency; Crowdsourcing will help in finding the source of occurrence / incidents; Crowdsourcing allows to get an idea of citizen's sentiment at the time of occurrence of the incident; Identification of the location (GPS) of reporters / incidents; and Verification of incidents / reports / image verification.

[9] For example: It would reduce the potential cost of crisis management work; It will offer more sustainable crisis response management; and It will protect victims and potential victims.

[10] See 'Los Angeles Law Enforcement Looking To Crowdsource Surveillance' at http://bit.ly/1iqAn5a (accessed on 15/05/14)

[11] B.B.C. News Report,. 26 June 2012. Crowd-sourcing used to trace London riot suspects, Available at http://bbc.in/1tPrtn9

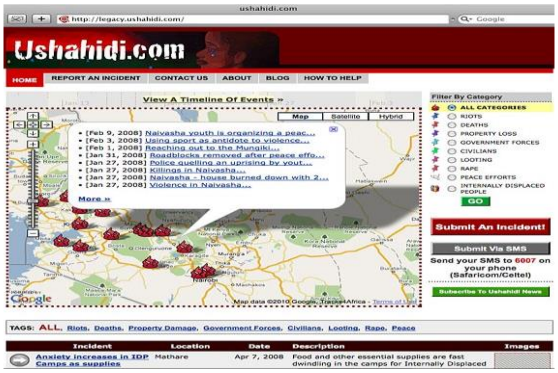
[12] Ushahidi means "testimony" in Swahili language, was a website that was initially developed to map reports of violence in Kenya. For more visit http://ushahidi.com

[13] See 'FrontlineSMS in Pakistan' at https://bit.ly/1gd0lKQ

of Home Affairs, GOI to issue a public notice on behalf of the Committee inviting views and suggestions from the general public. Accordingly a public notice was issued on December 24, 2012 and it called for suggestion to be sent to the Committee by emails, post and fax by 5th January 2013. In response to the said public notice, the Committee received around 80,000 responses from stake-holders, social activists and the general public [37].

2.1.1 *Crowdsourcing Collection of Data in Humanitarian Crisis Governance*

It is believed that 'crowdsourcing' process is the first step of disaster relief focusing on data collection. After preprocessing and cleaning up crowdsourcing collection of data can be used for a variety of situations to give people better insight into events that impact their communities [1]. Liu and Palen (2009) summarize 13 crisis-related mashups to derive some high-level design directions of next generation crisis support tools [23].



- [Feb 9, 2008] Naivasha youth is organizing a peac...
- [Feb 3, 2008] Using sport as antidote to violence...
- [Feb 1, 2008] Reaching out to the Mungiki...
- [Jan 31, 2008] Roadblocks removed after peace effo...
- [Jan 27, 2008] Police quelling an uprising by yout...
- [Jan 27, 2008] Killings in Naivasha...
- [Jan 27, 2008] Naivasha - house burned down with 2...
- [Jan 27, 2008] Violence in Naivasha...

More »

Send your SMS to 6007 on your phone (Safaricom/Celtel)

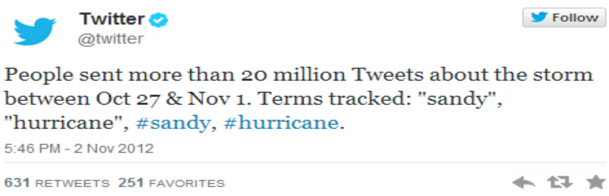
TAGS: ALL, Riots, Deaths, Property Damage, Government Forces, Civilians, Looting, Rape, Peace

Incident	Location	Date	Description	Images
Anxiety increases in IDP Camps as supplies	Mathare	Apr 7, 2008	Food and other essential supplies are fast dwindling in the camps for Internally Displaced	

Figure 1: Post-Election Violence Mapping in Kenya, 2008.

One of the most famous crisis maps is 'Ushahidi' that utilizes web 2.0 technologies to collect and visualize real-time public reports on a map via SMS, email, and the web. It was first developed to track reports of incidents of violence after the election in Kenya in 2008. The original website was used to map incidents of violence and peace efforts throughout the country based on reports submitted via the web and mobile phones. This website had 45,000 users in Kenya.[14]

Again, after the devastating 7.0 magnitude earthquake striking Haiti in January 2010, Ushahidi launched 'Haiti Live'[15] to gather the post-earthquake crisis response and recovery efforts in Haiti and generated over 13,5004 crowdsourced messages [1].



Twitter
@twitter

People sent more than 20 million Tweets about the storm between Oct 27 & Nov 1. Terms tracked: "sandy", "hurricane", #sandy, #hurricane.

5:46 PM - 2 Nov 2012

631 RETWEETS 251 FAVORITES

Figure 2: Twitter tracked #sandy and #hurricane.

Just before, during and after the devastating hurricane Sandy in USA, people sent more than 20 million tweets between October 27 and November 01, 2010.

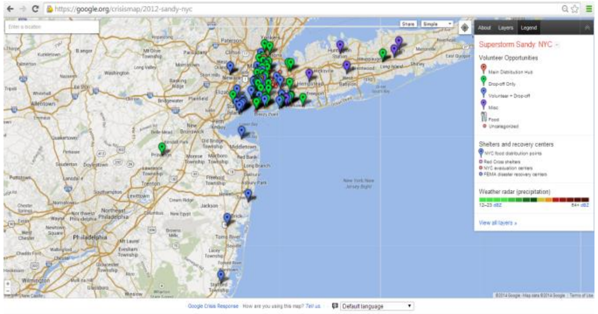


Figure 3: Deployment on Google Crisis Map for Hurricane Sandy 2012.

Howe describes crowdsourcing, in part, as leveraging the "latent talent of the crowd" [17] to accomplish something. In any crisis response work, developing crisis map is a common practice. In last couple of years Google has deployed more than 30 Crisis Maps.[16]

From 2007 to the present, several crowdsourcing platforms[17] have been used to deploy in a variety of situations such as human and natural disasters, elections monitoring and observation, tracking incidents of crime and civil unrest, promoting peace initiatives, documenting the impact of the "Deepwater Horizon" oil-spill disaster, crowdsourcing citizen response to Russian wildfires, visualizing the urban landscape in Prague and New York City or mapping the disruptions caused by the London tube strikes [14]. In two years, from 2009 to 2011, there were about 40 key deployments only on Ushahidi platform. Some recent Ushahidi deployments and statistics are given bellow.

Table 1: Crowdsourcing crisis map deployments on Ushahidi

Deployments	No of Reports	Deployments	No of Reports
Sinsai.info	4,000	Libya Crisis Map	697
Christchurch Recovery Map	1,729	Queensland Flood	99,772
EveryMap	1,300	U-Shahid	2,462
HarassMap	319	VacantNYC	11,523
Prague Watch	80	Tubestrike Crowdmap	55
PakReport	1,140	Help Map (Russian Fires)	1,600+
Louisiana Bucket Brigade	3,297	Elecciones Transparentes	815
Eleitor2010	230	Ushahidi Haiti	3,584

Source: Information gathered from George, S., 2011.

During the horrific terrorist attack in Mumbai in 2008, 70 tweets posted in every five seconds[18] and recently couple of months ago, during the Typhoon Yolanda in November 2013, the Digital

[14] See 'About Us' of Ushahidi at https://bit.ly/1lMYL1P

[15] See http://haiti.ushahidi.com/

[16] See http://bit.ly/1sSuY9K for more.

[17] Different crowdsourcing platforms are Ushahidi, SwiftRiver, Crowdmap, Eden (Sahana), CrowdCrafting, CrisisTracker, OpenIR, ArcGIS, Recovers, PADDDtracker, Google Crisis Map, GeoChat, Souktel, InaSAFE, Geofeedia, Geopictures, OpenStreetMap and etc.

[18] See 'Mumbai attacks: Twitter and Flickr used to break news' at https://bit.ly/1nUsVmN

Humanitarian Network collected 182,000+ tweets in just 14 hours.[19] There are more examples like above.

Thus, crowdsourcing has potential to generate huge amount of data. This data provides useful insights and at the same time, the data can be even more valuable after pre-processing [1]. Crowdsourcing process for crisis governance is not only limited to economically developed countries but also in developing countries. Crowdsourcing is already having a strong impact in developing countries, where it is being applied for crisis mapping and other tactical mappings as well as to track, report, and coordinate relief efforts. For example, in Haiti and Pakistan it has been used to coordinate crisis governance work after of natural disasters; in Libya it has been used to coordinate humanitarian response work during political conflicts and in Kenya it has been used to report human rights abuses and violence [3].

Crowdsourcing is the easiest way to gather huge data on something that can be used to monitor the well-being of high-risk communities without requiring significant investment in human resources or infrastructure. Through the use of a crowdsourcing process, it is possible to gather private data and sensitive personal data on sensitive issues. Interestingly, law enforcement officials are increasing their attention on the process as, such type technology has tremendous potential for situations in which rapid response is critical success factor [40]. Thus, the odd condition arises in which others have access to one’s personal affairs, including personal information, the intimacies of one’s life, one’s thoughts and one’s feelings. Such type of condition could be described as the ‘violation of privacy’, while the process of monitoring someone and his activities for accessing his personal and other confidential data could be described as ‘surveillance’. At this point, it is important to understand that both privacy and surveillance are in many ways each other’s counterpart [6].

As law enforcement agencies are giving more attention on crowdsourcing process and using it increasingly, it is better to know how they have used crowdsourcing for surveillance earlier and how are they using crowdsourcing at present. So, the next part of the paper would be dedicated to the history of crowdsourcing process in surveillance. Some recent examples of (mis)using crowdsourcing initiatives for data collection aiming for surveillance would be given as well.

2.2 Surveillance Using Crowdsourcing Process

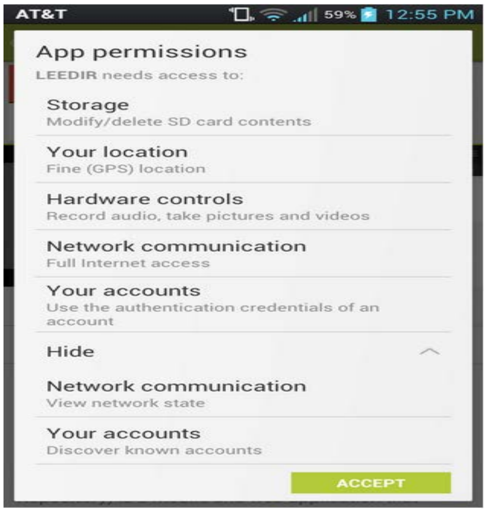
The history of surveillance using crowdsourcing process is rather interesting. The ‘traditional’ crowdsourcing process was used to spy on citizens in UK back in 1937. Officially, the Mass Observation project was developed in UK, aimed to create a “people’s anthropology” to redress the relative neglect of the perspective of ordinary people in social science [2]. Following public appeals by the founders of Mass-Observation, several hundred ordinary people across Britain volunteered to keep daily dairies about their personal lives and their communities and to respond regular surveys (called “directive replies”) [42]. In this project investigators got paid who anonymously recorded people's conversation and behavior at work, on the street and at various public occasions including public meetings and sporting and religious events. For example, one of the reporters wrote ‘I am mass observing the forces’ love affairs’ [42]. For such type reasons, some people felt it was just an invasion of privacy.[20] Interestingly, the London Metropolitan Police is still collecting reports on ‘suspicious behaviors’ of residents using crowdsourcing process under the ‘Safer Neighborhood’ project that have been noticed by this researcher.

2.2.1 Some Recent Examples: Using the Process of Crowdsourcing for Surveillance

With the advancement of science and technology, different security agencies- equipped with up-to-date tools are continuing the same ‘tradition’ of spying on citizens. They also use different web 2.0 tools those are externally available.

In 2008, the United States launched a project called the ‘Texas Virtual Border Watch Program’[21], which allows anyone in the world to log on via the Internet and watch a live feed of the Texas border to supposedly report suspicious activities [13]. A British private company designed Internet Eyes[22] in 2009 to ‘crowdsource’ digital surveillance. The UK approved the company to launch the digital tool. There have been other citizen spy pilots in the U.K. Farrier mentions, ‘the cable TV channel in East London that showed live feeds of CCTV cameras in the area. All of these seek to outsource surveillance monitoring to members of the public, making members of the public the watchers and consequently part of the surveillance state’ [13].

Recently, the Los Angeles County Sheriff’s Department unveiled a crowd control software program called LEEDIR (Large Emergency Event Digital Information Repository)[23] that allows US law enforcement agencies who adopt it to solicit and gather videos and photos of "emergency events" from the public.[24] In early April 2014 after the riot in Isla Vista, California where over where over 100 arrests were made and 44 people injured, including five police officers, police were seeking to identify several subjects wanted for violent felonies that occurred during the evening.[25]



AT&T 59% 12:55 PM

App permissions

LEEDIR needs access to:

Storage
Modify/delete SD card contents

Your location
Fine (GPS) location

Hardware controls
Record audio, take pictures and videos

Network communication
Full Internet access

Your accounts
Use the authentication credentials of an account

Hide

Network communication
View network state

Your accounts
Discover known accounts

ACCEPT

Figure 4: Providing GPS data is mandatory in LEEDIR App

[19] See ‘Typhoon Yolanda: UN Needs Your Help Tagging Crisis Tweets for Disaster Response (Updated)’ at http://bit.ly/1p1ovYI

[20] Please visit http://bit.ly/1zYPEQ5 for more information.

[21] Visit http://www.texasborderwatch.com/ for more information http://www.youtube.com/watch?v=LHHJtjW--Tc..

[22] Visit http://www.interneteyes.co.uk/ for more information.

[23] See http://www.leedir.us/ accessed 01/05/2013

[24] See http://bit.ly/1pvMHGn accessed 01/05/2013

[25] See http://alj.am/1nMhXeG accessed 01/05/2013

Apparently, LEEDIR looks potentially useful tool, but there are some definite concerns. 'For one, there's no real way to submit anything anonymously. You aren't required to input your name, but the app itself demands access to GPS data and any other communications-related metadata is likely hoovered up by LEEDIR when images and video are uploaded' [10]. Apart from these, Law Enforcement Agencies might retain collected content via LEEDIR app for a while and then delete it. But there's no requirement to delete gathered different types of data in LEEDIR.

2.3 Some Crucial Challenges

No wonder that the crowdsourcing tool like LEEDIR, which is a government initiative, will certainly ask for some private data of users, while governments might try to gather information from crowdsourcing platforms without having a formal relationship with the project. The recent disclosures by NSA contractor Snowden proves such type of activities by governments.

It has been identified that crowdsourcing has huge potential for Crisis Governance and with the expansion of science and technology; it will have several positive dimensions in the Post-2015 world. However, as of now, all crowdsourcing process, tools and methods for crisis governance work are not fully secured both technically and legally.

Crowdsourcing process can reveal important and helpful data during any crisis but sometimes it lacks the ability to efficiently handle privacy and personal data. One of the pioneer and most popular crowdsourcing platforms i.e. Ushahidi is being used by many humanitarian volunteers. However, this platform has some security holes that have been identified in 2012 by the Stand By Task Force (SBTF).[26] According to Meier, one UN practitioner who was not 'techie' was able to 'scrape Ushahidi's entire Kenya election monitoring data form March 2013, which included some personal identifying information' [25].

In addition to this, it has become much easier for governments to gather information from crowdsourcing platforms, which might happen without even needing to establish any formal cooperation with crowdsourcing projects. The 'excellent' combination of social networking tools, government's own tools and 'pro-active' audience allows any government, private companies and other spying agencies to gather reports and other data outside of a formal agreement among parties.

Generally, government information systems do not interface with external information systems due to security and reliability concerns while some civil society organisations or NGOs may not want a government organization to access their information systems [35]. During the 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 (NGOs) 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 [1].

Crowdsourced applications also have lacked the ability to efficiently provide a mechanism to help coordinate a response during a crisis [15]. The process of crowdfeeding[27] 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 [28]. 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.

Sometimes governments develop (i.e. LEEDIR in the U.S.) or allow private companies to develop citizen-monitoring tools (Internet Eyes in the UK). In the name of national security, governments also use different laws to monitor or to access data from such type of digital platforms. For example, the UK Government initiated surveillance of communications (it includes online communication and mobile as well.) under two separate regimes in UK law. Under Part I Chapter 1 and Part I Chapter 2 of the Regulation of Investigatory Powers Act 2000 (RIPA), the Home Secretary can authorize 'Interception of content for three or six months' or 'access to data related to the use of communications service' may be self-authorised by a wide range of government bodies respectively. It is to be noted that the both sections of RIPA were amended by the Serious Organised Crime and Police Act 2005 to replace references to the National Criminal Intelligence Service with the Serious Organised Crime Agency[7].

Sometimes private companies gather different types of personal information of online active individuals for their business promotion. They use different methods of data collection including data mining, crowdsourcing, online surveying process etc. Thus, this type of act by private companies might constitute gross privacy risks for citizens.

So, for different reasons like, government initiatives to access personal data illegally; private company initiatives to gather personal data; security holes in crowdsouricng platforms and apps; introducing laws to access personal data in the name of national 'security' but in an unethical way etc. really generate question- how to minimize the gap in trust among governments, private companies, security agencies and citizens.

Someone can predict after analyzing the above issues that there would be some crucial challenges in using crowdsourcing process for crisis governance in the Post-2015 World as well. As, no proper ethical or legal safeguards for crowdsourcing collection of data are available at any level; a brief legal analysis has been carried out on data protection and online privacy condition in some countries and regions.

3. DATA PROTECTION AND ONLINE PRIVACY FRAMEWORKS FOR CRISIS MANAGEMENT CROWDSOURCING

Modern crowdsourcing in the New Media Age is totally based on digital environment. As at present there are no particular laws just to deal with crowdsourced data, which is not seem to be logical as well, an analysis will be done on some existing online privacy and data protection laws and government programs from different parts of the world. Thus, this desk research has been performed to understand the safety level of crowdsourcing process by analyzing online privacy and data protection in seven different countries all

[26] The Standby Task Force was founded in October 2010 to support the information management needs of formal humanitarian organizations. To know more information, visit http://blog.standbytaskforce.com/

[27] Crowdfeeding is when information sourced from the "crowd" is fed back into the population to improve collective knowledge and decision-making.

over the world along with the European Union. Based on different 'open ended'[28] factors, the following countries and region have been chosen for the research on online privacy and data protection to have a general idea of 'safety' in crowdsourcing process. Thus, a short analysis has been completed on important issues related to Data Protection, Online Privacy and Freedom of Online Expression. The outcome of the analysis is given here.

3.1 BRICS Countries:

3.1.1 Brazil

Brazil's long-debated bill the "Internet Bill of Rights" has become law recently. The legislation, which passed the Brazilian Senate unanimously and signed by the president on April 2014, is intended to secure equality of access to the Internet in Brazil. It provides the protection of privacy for Brazilian Internet users. The legislation states that the disclosure of personal data to third parties generally requires the informed consent of an Internet user, except under a valid court order. Organisations that collect personal data from residents of Brazil will be subject to Brazil's laws and courts in cases involving information on Brazilians, even if the data is stored on servers abroad. In addition to these, Internet Service Providers (ISP) will be required to retain Internet access logs for one year [41].

3.1.2 Russia

Russian law does not specifically regulate online privacy. The definition of personal data under the Data Protection Act No. 152 FZ dated 27 July 2006 ('DPA') is rather broad and there are views that information on number, length of visits of particular web-sites and IP address (in combination with other data allowing the user to be identified) could be considered personal data.

Just couple of weeks ago, on May 5, 2014, President Putin singed the new law on bloggers. The law will enter into force on August 1, 2014. This law will be included to the counter-terrorism legislation. This new "Internet users called bloggers" law requires bloggers with more than 3,000 daily visitors online to register with the state body for media monitoring named Roskomnadzor. After registration, bloggers with daily more than 3,000 visitors 'will have the same legal constraints and responsibilities as mass media outlets, including verifying information for accuracy, indicating the minimal age for users, protecting information pertaining to people's privacy, and being subject to restrictions on propaganda in support of electoral candidates. Bloggers could also be held responsible for any comments posted by third parties on their website or social media page'.[29]

3.1.3 India

There is no specific legislation on privacy and data protection in India. However, India's most comprehensive data protection standards are found in the Information Technology Act (ITA) 2000 and are known as "Reasonable security practices and procedures and sensitive personal data or information" Rules 2011 [11]. In the name of national security, the ITA also allows law enforcement and security agencies as well as the government to intercept, monitor, and decrypt digital communication.[30]

The structure of different provisions and the lack of safeguards incorporated in ITA 2000, serve as a dilution to user privacy. In addition, the provisions place huge security and technical obligations on the service provider – as 'they are required to extend all facilities necessary to security agencies for interception and decryption, and hold the service provider liable for imprisonment up to seven years for non-compliance'. Thus, the government creates such an environment where service providers would unlikely challenge any request for access or interception from law enforcement agencies.[31]

The Government of India 'lawfully' intercepts communications. However, there have been a number of instances of unauthorized interceptions that have taken place as well [18]. It was found that in 2013, in Himachel Pradesh 1371 phones were tapped based on verbal approval, while the Home Ministry had only authorized interception of 170 [36]. This fact proves that there are instances of when existing safeguards for interception and surveillance are undermined and thus, these exercises also challenge existing safeguards for online privacy and security. Recently, the Government of India implemented the Central Monitoring System [33]. The system allows security agencies to bypass service providers and directly intercept communications of citizens.

3.1.4 China

There is no comprehensive data protection law in China. However, provisions relating to personal data protection are found in various laws and regulations. A draft Personal Data Protection Law has been under review by the government for many years, but there is still no indication as to if and when such law will be passed [27]. The Standing Committee of the National People's Congress took the 'Decision on Strengthening Online Information Protection' on 28th December 2012.[32] China developed the 'Guidelines for Personal Information Protection under the National Standard of Information Security Technology that came into force on 01 Feb 2013 [23]. Both, collectively referred to as 'General Data Protection Law'.

In the middle of 2011, China Police told cafes, hotels and other businesses in central Beijing to install surveillance technology for Wi-Fi users or face fines and possible closure, in a further tightening of Internet controls [5].

[28] Factors behind choosing **BRICS** (Brazil, Russia, India, China and South Africa) Countries: AS the BRICS countries are emerging as economic powers and it is expected that these countries will take the lead role in Post-2015 governance. As technological environment is boosting in these countries, they have to cope up with widespread aspirations in the area of online privacy and data protection; **European Union** (EU): In terms of safeguarding the privacy of its citizens, the EU is the pioneer example. Recent development in data protection initiative by the European Court of Justice also supports its supremacy in protecting personal data and privacy of citizens and also to highlight EU's real interest in protecting the privacy and data of individuals that could be a good example for others; **United States** (US): The US-NSA snooping revelations stoked fears around privacy, data protection. US is collecting information from everywhere in the name of National Security and protection of US Business etc. Because of such type of aggressiveness in collecting data unethically, it was interesting to know more about US data protection and online privacy laws and different programs they run to gather personal data; and **United Arab Emirates (UAE)**: Most of the Middle Eastern countries are very conservative in both offline and online environment. It was appealing to know the real picture of online environment in any Middle Eastern conservative country.

[29] Visit http://bit.ly/1qWp0WW for more information.

[30] See Section 43, 66, 66F, 67 and 84A of ITA 2000 available at http://bit.ly/1qRpDNG

[31] Visit http://bit.ly/1ovlgXh

[32] Visit http://1.usa.gov/1vXSkgw

China's online regulations and legislation are aimed to ‘preserve the economic benefits of new information and communications technologies while guarding against foreign economic domination and the use of technology to coordinate anti-government activity’. [38]. One of the most important steps was to recruit thousands of students and fresh graduates with computer science background and Internet skills as ‘Cyber Police’. The main activity of the cyber police is to monitor and control the Internet [29]. They continuously search web sites, personal blogs, social networking sites and other discussion forum and ‘block or shut them down whenever they come across content the government disapproves of, including potential state secrets, "anti-Party and anti-socialist speech" and criticism of the country's leadership’ [30].

3.1.5 South Africa

South Africa does not have a Data Protection Act or Online Privacy Act. However, under the Section 14 of the Constitution of the Republic of South Africa guarantees the right to privacy. It declares that the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.[33]

The Protection of Personal Information Act[34] ('PPI Act') came into force on 26 November 2013 is wide in application and will, subject to certain exclusions detailed therein, impact all persons processing personal information. The Electronic Communications and Transactions Act [34], which covers personal information that has been obtained through electronic transactions, which defines a set of rules between the person the information is about and the person/organisation (“data controller”) who is holding that information.[35]

3.2 European Union

The EC Data Protection Directive- also known as Directive 95/46/EC was adopted to protect the processing of personal data and on the free movement of such data.[36] The Directive 95/46/EC set a milestone in the history of personal data protection. It has now become a truly international standard for data protection [9]. However, each EU country has its own way of implementations the law that has led to an uneven level of protection for personal data, depending on where an individual lives and use services. It is also that fact that in the ‘New Media Age’, fast technological expansion has brought new challenges for data protection. With social networking sites, cloud computing, location-based services and smart cards, people leave digital traces with every move they make. So, the European Commission has proposed a comprehensive reform of the Directive 95/46/EC to strengthen online privacy rights and boost Europe's digital economy. The EU expects that ‘the EU data protection reform will make sure the EU rules are future-proof and fit for the digital age’ [12]. Let us now have a look about the proposed changes. [37]

- ‘A ‘right to be forgotten’ will help people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed.
- Easier access to one’s own data and the right of data portability, i.e. easier transfer of personal data from one service provider to another.
- Companies and organisations will have to notify serious data breaches without undue delay, where feasible within 24 hours.
- A single set of rules on data protection, valid across the EU.
- Companies will only have to deal with a single national data protection authority – in the EU country where they have their main establishment.
- Individuals will have the right to refer all cases to their home national data protection authority, even when their personal data is processed outside their home country.
- EU rules will apply to companies not established in the EU, if they offer goods or services in the EU or monitor the online behaviour of citizens.
- Increased responsibility and accountability for those processing personal data.
- Unnecessary administrative burdens such as notification requirements for companies processing personal data will be removed.
- National data protection authorities will be strengthened so they can better enforce the EU rules at home.’

3.3 United Arab Emirates (UAE)

In the UAE, there is no specific data protection legislation. However, there are several UAE Federal Laws[38] that contain various provisions in relation to privacy and the protection of personal data. The UAE Penal Code does not contain direct provisions to the Internet governance, but its provisions related to privacy are broadly drafted and therefore could apply to online matters. Apart from these, ‘under certain circumstances, online privacy is protected through Articles 21 and 22 of the Cyber Crime Law and Clause 3 of the Privacy of Consumer Information Policy’ [27].

3.4 United States

The United States has about 20 sector specific or medium specific national privacy or data security laws, and hundreds of such laws among its 50 states. For example, California alone has more than 25 state privacy and data security laws [27].

The Foreign Intelligence Surveillance Act of 1978[39] prescribes procedures for the physical and electronic surveillance and collection of “foreign intelligence information” between “foreign powers” and “agents of foreign powers” (which may include American citizens and permanent residents suspected of

[33] The Preamble of the Protection of Personal Information Bill available at http://bit.ly/1tPnSWp

[34] Visit http://bit.ly/1tPnSWp for more information.

[35] See the Chapter VIII (Protection of Personal Information) of Electronic Communications and Transactions Act, 2002. available at http://bit.ly/VZprmV

[36] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050

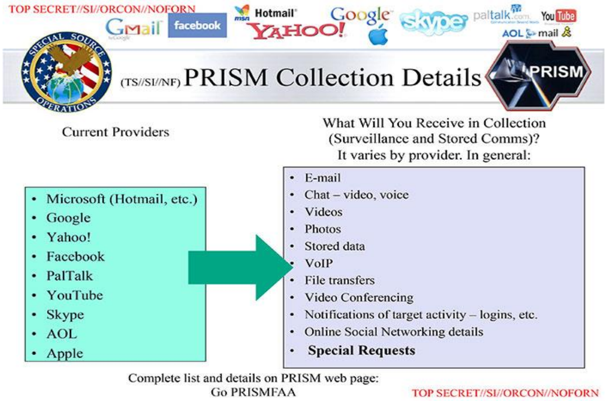
[37] Visit to know why the EU needs data protection reform at http://bit.ly/VXhWxo

[38] For example, Constitution of the UAE (Federal Law 1 of 1971); Penal Code (Federal Law 3 of 1987 as amended); Cyber Crime Law (Federal Law 5 of 2012 regarding Information Technology Crime Control); Regulating Telecommunications (Federal Law by Decree 3 of 2003 as amended)

[39] The full Act is available at http://1.usa.gov/1u11hFv

espionage or terrorism). Following the September 11, 2001 attacks, the Act was amended by the USA Patriot Act to protect liberty of the American people from the challenges posed by a global terrorist network. The Patriot Act 'allows victims of computer hacking to request law enforcement assistance in monitoring the "trespassers" on their computers.'[40] Thus, the Act allows using the crowdsourcing process (as it suggests common people to seek assistance from the law enforcement agencies) to identify online threats by "trespassers".

After the revelation of NSA-PRISM program, no further discussion on online privacy, security and data protection is needed to understand the US approach towards these issues.[41] The PRISM program began in 2007 in the wake of the passage of the Protect America Act [21] under the Bush Administration [20].



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Figure 5: The PRISM program collects a wide range of data from the nine companies. Source: The Washington Post.[42]

Since then nine companies joined the program to 'co-operate' with the NSA. Under the PRISM program, the NSA collects enormous personal and sensitive personal data.

4. REGULATORY FRAMEWORK: CROWDSOURCING COLLECTION OF DATA FOR CRISIS GOVERNANCE

Based on earlier discussions and brief analysis on online privacy, data protection, security and freedom of online expression, it has emerged that different countries have different approach to these issues. It becomes more depressing when Internet and tech companies join hands with programs like PRISM and hand over or help to track personal data and sensitive personal data of their customers.

As the online world is not really safe to roam around leaving your online footprint, crowdsourcing collection of data is also risky in terms of privacy, data protection and security aspects. The main threat comes from authoritarian administrations while the service providers / different crowdsourcing tools suppliers do not give proper attention in maintaining high level privacy and security for those crowdsourcing tools. Existing legal instruments in some countries are really very good to protect privacy of citizens in online environment. However, it is rare to find proper implementation of the 'Rule of Law'. Some countries like India, China, Russia, US really don't care about personal privacy. Thus, there is no reason to believe that these countries are not monitoring crowdsourcing collection of data in the time of crisis governance.

So, a set of suggestions on how to deal privacy, security and data protections issues in crowdsourcing process for crisis governance in the Post-2015 World will be provided here. Different stakeholders must follow some common and some independent best practices during any crowdsourcing process for crisis governance.

4.1 Governments

- Proper implementation of rule of law is needed in countries where some privacy and data protection laws are available.
- Countries without any data protection and online privacy laws need to start discussion on how to improve the privacy, security and data protection level of citizens and start the process of introducing new laws.
- Governments must respect the right to privacy; right to freedom of expression; and right to personal data protection.
- Governments should formulate acceptable legal safeguards for not monitoring crowdsourcing process during humanitarian crisis governance work.
- Governments should seek for the judicial authorization to access crowdsourcing information, if any need arise.
- A common coordination platform between government agencies and NGOs should be developed to deal with in humanitarian crisis.

4.2 Law Enforcement Agencies

- 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.

4.3 Crisis Governance Coordinators

- 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. [43]
- 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.
- A common coordination platform between government agencies and NGOs should be developed to deal with in humanitarian crisis.

[40] Visit http://www.justice.gov/archive/ll/highlights.htm for more.

[41] Visit http://1.usa.gov/1u11hFv for more about US surveillance.

[42] Information available at http://wapo.st/1nMiBZU

[43] Visit http://bit.ly/1u11vfN for more.

4.4 Developers of Crowdsourcing Tools

- Tech companies who develop crowdsourcing tools should publicly announce the 'trust' level of the tool.
- Tech companies should develop tools with PET[44] 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'.

4.5 Media

- Media should develop their own 'Media Ethics' for crisis reporting with keeping in mind the privacy and security issues of victims.
- 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.

4.6 Private Companies

- Private companies 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.

4.7 Users / Contributors

- 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.

5. CONCLUSION AND FUTURE WORK

Good governance is just impossible without the active support of common citizens. However, at the same time governments need to ensure that protecting citizens from any type of harm as it is one of the moral duties for governments. Crowdsourcing can be an excellent way to collect data on ongoing man-made crisis i.e. conflict between two groups, violence and abuses; and its impacts on citizens and communities. For a coordinated crisis governance work, a common crowdsourcing platform can gather different sets of data that help to coordinate the crisis work properly and effectively. The potential of crowdsourcing process for crisis governance cannot be underestimated, especially in developing countries where mobile network is growing very rapidly. Thus, crowdsourcing process is increasingly seen as the new paradigm of crisis governance and mobile-based crowdsourcing platforms [16] could be the potential answer to crisis governance in the Post-2015 World.

It is important to keep in mind that some real challenges exist and some new challenges are being added to those existing challenges. Governments, some security agencies, terrorist groups, private companies and other unnamed groups are scrutinizing the online world for 24X7 hours. The issue of personal safety and security of mass reporters in crowdsourcing process for any type of crisis governance must be taken care properly.

It has been noticed that in the name of national security several countries are engaged in illegal and unethical activities while some other countries do have a proper legal safeguards to protect online privacy and security of their citizens. The disclosures by NSA contractor Edward Snowden confirmed that governments are collecting personal data of citizens in an unethical way and the privacy of common people is really in danger. On the other hand, some online crowdsourcing platforms are not trusted; the absence for a common platform for coordinated crisis response work; some users are not really concerned about the consequences of sharing personal data and sensitive personal data during online reporting etc.; and all these factors constitute a real danger for people who engage in such type of crowdsourcing activities. All these factors along with the disclosers by Snowden would have huge impact on our society and also on communication platforms, tools and software produced by different tech companies.

So, an especial attention with innovative approach should be taken when developing new communication tools, as users in crowdsourcing process look for guaranteed quality, anonymity, privacy, and security and also it is suggested to use Privacy Enhancing Technology during the development of any communications tools. Countries from developing world should take necessary steps to use emerging ICTs to ensure better and smart governance for their citizens. At the same time they have to ensure protecting online privacy, security and data protection of their citizens with proper legal safeguards.

6. ACKNOWLEDGMENTS

The paper is one of the end results that has been partially developed under the Ph.D. Research title 'Crowdsourcing Processes to Manage Humanitarian Crisis: Towards a New Paradigm?' in partial fulfillment of the requirements for the Erasmus Mundus Joint International Doctoral (Ph.D) Degree in Law, Science and Technology (LAST-JD). I am grateful to the entire Doctoral Board headed by Prof. Monica Palmirani of Bologna University; and especially to Prof. Antoni Roig of UAB Law School, Barcelona, Spain who has helped me to understand some crucial issues during the development of this paper. I am also grateful to my main supervisor for Ph.D. Prof. Pompeu Casanovas of the Institute of Law and Technology, Faculty of Law, Universitat Autònoma de Barcelona, Barcelona, Spain for his kind support and advise towards my Ph.D. research.

7. REFERENCES

[1] Barbier, G., Zafarani, R., Gao, H., Fung, G. and Liu, H. 2012. Maximizing benefits from crowdsourced data, In Computational and Mathematical Organization Theory, September 2012, Volume 18, Issue 3, pp 257-279 DOI: 10.1007/s10588-012-9121-2

[2] Bloome D, Sheridan D, Street BV (1993) Reading mass-observation writing. University of Sussex Library, Brighton.

[3] Bott, M., Gigler, B., and Young, G., 2014. The Role of Crowdsourcing for Better Governance in Fragile State Contexts. 2014 International Bank for Reconstruction and Development / The World Bank. 1818 H Street NW, Washington DC 20433.

[4] Brabham, D C., 2013. Using Crowdsourcing In Government, pp 10-20. Collaboration Across Boundaries Series, IBM Center for The Business of Government, Washington, DC 20005.

[5] Branigan, T., 2011. China boosts internet surveillance. Available at http://bit.ly/1lCnU2T

[6] Brey, P., 2006. Editorial introduction – Surveillance and privacy in Ethics and Information Technology (2005) 7:183–184. DOI 10.1007/s10676-006-0015-1

[44] PET stands for Privacy Enhancing Technologies.

[7] Brown, I., 2012. Government Access to Private-Sector Data in the United Kingdom. International Data Privacy Law 2, no. 4: 230-238.

[8] Clift, S. 2003. "E-Democracy, E-Governance and Public Net-Work." Publicus, September. http://www.publicus.net

[9] 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

[10] 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

[11] Dharmakumar, R., 2013. India's Internet Privacy Woes. Available at http://bit.ly/1qfRIlM accessed on 12/05/2014.

[12] Fact Sheet, EC., 2012. Why do we need an EU data protection reform' in Factsheets on data protection reform. Available http://bit.ly/1pXq1hM accessed on 14/05/2014.

[13] Farrier, C., 2010. Internet Eyes Citizen Spy Game – The New Stasi? Available at http://bit.ly/1gGVvpM

[14] George, S., 2011. Key Deployment Report – March 2011. Ushahidi 1100 North Glebe Rd. 22201 http://ushahidi.com

[15] Goolsby, R., 2010. Social media as crisis platform: The future of community maps/crisis maps. ACM Trans. Intell. Syst. Technol. 1(1), 1–11 (2010). DOI: http://bit.ly/1vzmsS0

[16] Halder, B. 2013. Mobile-based Crowdsourcing Platform for Post-2015 Governance: Possibilities for Developing Countries available at http://bit.ly/1vzmwRE

[17] Howe, J.: The Rise of Crowdsourcing accessed on 20/10/13 from http://wrd.cm/1rH4vjv

[18] Jain, B., 2011. 8,736 phone and e-mail accounts tapped by different government agencies in July. Available at: http://bit.ly/1lCo8qw

[19] Jeffery, S., 2011, Ushahidi: crowdmapping collective that exposed Kenyan election killings. Available from: http://bit.ly/1vXT7Ot accessed on 21/11/2012

[20] Johnson, L., 2013. George W. Bush Defends PRISM: 'I Put That Program in Place to Protect the Country'. The Huffington Post. Retrieved on May 25, 2014 and Available at http://huff.to/1wVgE6O

[21] Lee, T.B., 2013. How Congress Unknowingly Legalized PRISM in 2007. Wonkblog (blog of The Washington Post). Available at http://wapo.st/1pXqPDd Accessed on 25/05/14.

[22] Linklaters., 2013. China – Progress towards national privacy regulation in Technology, Media & Telecommunications News. pp 10-14. Available at http://bit.ly/1lCoiym

[23] Liu, S. & Palen, L., (2009) Spatiotemporal Mashups: a survey of current tools to inform next generation crisis support. In: Proceedings of the 6th international ISCRAM conference, Gothenburg, Sweden.

[24] Mason, P., 2007. Kenya in crisis, BBC News Report accessed on 12/05/2014 from http://bbc.in/1tle73o

[25] Meier, P., 2013. Data Protection Protocols for Crisis Mapping available at http://bit.ly/1u11vfN

[26] OECD/International Telecommunication Union (2011), *M-Government: Mobile Technologies for Responsive Governments and Connected Societies*, p 36, OECD Publishing. http://dx.doi.org/10.1787/9789264118706-en

[27] Paul McCormack and Kate Lucente,. 2014. Data Protection Laws of World Handbook. DLA Piper, London. http://bit.ly/VXjIP4

[28] 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

[29] Privacy International., 2012. Chapter: II. Surveillance policy in 'Country Report- China' under the 'Privacy in the Developing World'. Available at http://bit.ly/1lpq85f

[30] Qinglian, H., 2006. The Hijacked Potential of China's Internet in China's Right's Forum. Special Book Review. pp 33-35.

[31] Roberts, A. 2014. A true sea shanty: the story behind the Longitude prize. Accessed on 19/05/2014 from http://bit.ly/1ndqO9m

[32] Shirky, C. 2008. Here Comes Everybody: The Power of Organizing without Organizations. New York: Penguin Press.

[33] Singh, S., 2013. Govt. violates privacy safeguards to secretly monitor Internet traffic. Available at http://bit.ly/1tleESR

[34] South African Government. 2002. Electronic Communications and Transactions Act, 2002, No. 25 of 2002 [Online]. Accessed on 25/05/2014 and available from: http://www.internet.org.za/ect_act.html

[35] Spellman, J., 2010. Heading off disaster, one tweet at a time. http://bit.ly/1tleESR Turner Broadcasting System, Inc.

[36] The Economic Times. 2013. Action to be taken in 'phone tapping' during BJP rule: Virbhadra Singh. Available at: http://bit.ly/1ovmH7W

[37] Verma, J.S., 2013. Report of the Commmittee on Amendments to Criminal Law. Available at http://bit.ly/1wVi7df

[38] Walton, G., 2001. China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China 9 (Rights and Democracy, 2001). Available at http://www.totse.com/en/privacy/pucc.html

[39] Wepster, S. A., 2010. Between Theory and Observations; pp 34-37. ISBN 978-1-4419-1313-5; DOI: 10.1007/978-14419-1314-2; Springer New York Dordrecht Heidelberg London.

[40] Young. C., 2014. HarassMap: Using Crowdsourced Data to Map Sexual Harassment in Egypt. Available at http://bit.ly/1qfTd39

[41] Zimmermann, D. and Costa, J., 2014. Brazil: Brazil Is Passing Legislation Aimed At Guaranteeing The Protection And Privacy Of Internet Users. Accessed on 21/05/2012 and available at http://bit.ly/1tx1fEz

[42] Zittoun, T., Alex, G., Flora, C. and Aveling, E. 2008. Using Social Knowledge: A Case Study of a Diarist's Meaning Making During World War II, 163-179. DOI: 10.1007/978-4-431-74680-5_10