International Journal of Information Systems for Crisis Response and Management
Volume 9 • Issue 3 • July-September 2017

Metrics for Ensuring Security and Privacy of Information Sharing Platforms for Improved City Resilience:
A Review Approach

Jaziar Radianti, Centre for Integrated Emergency Management UiA, Grimstad, Norway
Terje Gjøsæter, Oslo Metropolitan University, Oslo, Norway

ABSTRACT

City resilience is a pressing issue worldwide since the majority of the population resides in urban areas. When disaster strikes, the consequences will be more severe in the cities. To achieve resilience, different organizations, agencies and the public should share information during a disaster. ICT-based community engagement is used for strengthening resilience. The authors propose a set of metrics for assessing the security and privacy of information sharing tools for resilience. They then apply the selected metrics to a selection of information sharing tools. The authors' main finding is that most of them are reasonably well-protected, but with less than private default settings. They discuss the importance of security and privacy for different important categories of users of such systems, to better understand how these aspects affect the willingness to share information. Security and privacy is of particular importance for whistle-blowers that may carry urgent information, while volunteers and active helpers are less affected by the level of security and privacy.

KEYWORDS

Crowdsourcing, Evaluation, Information Sharing, Metrics, Privacy, Resilience, Resilience Tools, Security

1. INTRODUCTION

The UNDESA projection shows that the proportion of the world's population living in urban areas will increase from 54% (2014) to 66% by 2050 (UN, 2014). Thus, it is evident why city resilience has been emphasized globally due to cities becoming more vulnerable as more people will be affected when unexpected events occur. Information sharing is an important way to enhance resilience in a disaster (Palen et al., 2010; Yang & Maxwell, 2011), with the help of information and communication technology (ICT) tools that are becoming acceptable for facilitating crisis communication (Pipek, Liu, & Kerne, 2014). Interpreting further the spirit of the Hyogo Framework Action (UNISDR, 2005), the overall capability to cope with hazards is not solely authority responsibility, but is a combination of the self-organizing capability of the individuals, communities, public and private organizations in affected areas. Furthermore, the Sendai Framework for Disaster Risk Reduction 2015-2030 outlines

DOI: 10.4018/IJISCRAM.2017070103

the importance of building resilience into policies, plans and programmes. Sendai Framework encourages the use of information and communications technology to enhance measurement tools and the collection, analysis and dissemination of data, as well as to collaborate with people at the local level through the involvement of both community-based and non-governmental organizations.

In brief, the role of ICT tools to enable the society in general to adapt and recover from hazards and stresses is evident (Trnka & Johansson, 2011), especially to ensure that the right information flows smoothly to the intended audience.

What is resilience? UNISDR (2004) defines resilience as "the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure". We adopt this definition, and suggest that resilience should include the ability of individuals and communities to absorb and prepare to make use of the different crisis management communication technologies, so that they can engage and share information better with each other and with public authorities. The definition should also include the capacity for learning practical security and privacy knowledge for better use of ICT-based engagement tools.

The recent trend of ubiquitous computing allows people to share information by using day-to-day technologies surrounding them. The presence of social media in combination with the powerful trend of crowdsourcing for obtaining data shared by citizens (Liu, 2014; Liza, 2011), has to some extent been accepted as a part of crisis communication, apart from the data quality weaknesses that may arise from social media information (Tapia & Moore, 2014). Sharing information using various means arguably improves resilience as individuals can contribute information faster to the authorities, as well as to the circle of family and friends they care about and improve the way responders manage the crisis (Lindsay, 2011; Trnka & Johansson, 2011).

However, the crucial questions that should be addressed are: how thoroughly are the privacy and security concerns considered in line with the encouragement of the information sharing among different components of a resilient society? Does information sharing increase the resilience, or could it in some situations weaken the resilience when a focus on security and privacy emerge?

Information security concerns protecting information in different contexts: its confidentiality, integrity and availability (Avižienis, Laprie, Randell, & Landwehr, 2004). Security of information is essential to some organizations and actors before they are willing to share it (Liu & Chetal, 2005). For private citizens, trust concerning privacy protection is crucial, covering personal sensitive information (PSI) and personally identifiable information (PII, information that can identify them) (Schwartz & Solove, 2011). Part of the resilience is that our information is verifiably unmodified, confidential, available when needed, and accessible to authorized personnel only. These may in some cases seem to be sacrificed or at least prioritized down in a disaster situation, but should not be, and indeed does not need to be. On the contrary, the negligence of security and privacy could in fact harm the information sharing by making some actors reluctant to share potentially important information.

This article discusses a selection of techniques, technologies and tools that are used for information sharing in some countries, or general tools that are used worldwide such as social media. We discuss how individuals and communities can be more resilient in a crisis, in terms of the way they share information, by addressing security and privacy concerns.

The article is divided into 6 sections. In *Related Works,* we describe the relevant literature for our case. *Scope and Methodology* describes our scope, research questions and methodology. In *Results and Analysis*, we report the result and analysis from our study. Discussion and lessons learnt from our research and implications for disaster resilience is presented in *Discussion, Solutions and Implications for Resilience*. *Conclusion* is a summary of the main findings of this study and its limitations.

2. RELATED WORKS

The literature review targets answering the following questions: How is the resilience generally defined, and then, linked to the community engagement, security and privacy in the context of a city as a unit analysis? How does information sharing to increase resilience appear in the literature, and how are security and privacy discussed in the resilience context? What kinds of gaps exist when discussing community engagement, the use of technologies, security, and privacy?

2.1. Resilience

Resilience is an elusive concept as it has been used for specific disaster contexts elsewhere without resulting in a consensus among researchers, even far before this term was made popular through the issuance of the Hyogo Framework for Action (HFA) (UNISDR, 2005). UNISDR (2004) has provided the definition of resilience as the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. HFA pays attention to the efforts for strengthening of institutions, mechanisms and capacities at all levels, in particular at the community level, that can systematically contribute to building resilience to hazards (UNISDR, 2005). While the technology and information system admittedly can support for enhancing resilience, surprisingly, none of privacy and security issues that often follows the adoption of communication technologies are addressed in HFA. Likewise, while the intention is to reframe the resilience, no technology aspect is discussed in any of the three storylines of resilience proposed by Aldunce, Beilin, Handmer, and Howden (2014): mechanistic/technocratic, community-based and sustainability. Accordingly, no security and privacy issues exist in the article. The technology aspect is mentioned only for pointing out its irrelevance as it is in favour of two other aspects that are believed more relevant and significant for building community: community self-resilience and participation.

Rogers (2013) suggests the concept of resilience as the organisational and technological resilience. In fact, when it comes to the technology dimension of resilience, this aspect is interpreted as "critical infrastructure", and thus, when the technology is linked to the organisations, it becomes "a mechanism for governing infrastructure from a distance and eliciting obedience"—a state-centric one. Such notions exclude the community participation. In principle, Rogers advocates the community resilience idea and urges the shift from warning and informing to increased personal preparedness and responsibility needed in public participation. It should be re-articulated in such way that it does not appear as a reproduction of passive engagement entrenched in the state-centric model. However, how technology can contribute to this proposed shifting is missing from this proposal.

Another comprehensive review on resilience is conducted by Bhamra, Dani, and Burnard (2011) and Manyena (2006). In Bhamra, Dani, and Burnard (2011), while the focus is resilience in organisational level context, the authors are conducting a general resilience survey in the literature. The authors point out that the general definition of resilience is closely related to the capability and ability of an element to return to a pre-disturbance state after a disruption. In fact, according to the authors, applying the notion of resilience to communities and the wider context of organisations does not change this broad definition. Finally, Bhamra et al. (2011) suggest a number of areas for advancing resilience research, in particular: the relationship between human and organisational resilience, understanding interfaces between organisational and infrastructural resilience. Again, the role of technology is presented vaguely as "infrastructural resilience" without supplementary explanation.

In Manyena's work (2006), the researchers' challenge to achieve consensus on definition of resilience are addressed. Resilience, is admittedly having a variety in the meaning. The vagueness of the concept is even explicitly mentioned in this article. Manyena (2006) suggests not making a problem of having multiple definitions of resilience as long as they do not harm conceptualisation, because reaching consensus is not an end itself. At the same time, the author proposes resilience definition as "…capacity of a system, community or society predisposed to a shock or stress to adapt and survive by changing its non-essential attributes and rebuilding itself…" Equally, the role of the physical aspects of resilience such as technology and infrastructure are not completely neglected, but they are secondary, as the need to mainstream resilience building through people is a key of disaster risk reduction and recovery. Not to mention security and privacy aspects and how they could relate to city resilience, which are clearly out of scope of the abovementioned studies. Albeit the recent emergency management system is unduly relying on new and often unproven hardware, computing technology, systems of intelligence gathering, and the like, to predict, prevent, or mitigate future threats (Birkland, 2009), how resilience with respect to security and privacy can come into the overall resilience picture remains blurred.

Given these points, there is a clear gap in the general definition of resilience where the role of technology in improving resilience is, to some extent, inadvertently neglected. It could also be because of the difficulties to capture the resilience details, if the effort in the literature is to find a general definition of resilience that works for all, or simply such technological roles does not fit within the community, organisational or city resilience framework.

Specific keywords search in SCOPUS using the combination of the following words: ICT, community, engagement, resilien, city, privacy, security in the journals and social science field, only returns five articles, with two of them are relevant, i.e. Haworth (2016) and Gil-Garcia, Zhang, and Puron-Cid (2016). Two other articles with respect to mobile banking adoption and rural ageing were off topic. The results only add one more article even though we expanded the field of search into life, physical and health sciences. The article highlights the role of Volunteered geographic information (VGI) to the widespread creation and sharing of geographic information by private citizens, through tools such as online mapping tools, social media, and smartphone applications for supporting emergency management. In this study, Haworth (2016) reports that the digital divide, data management, misinformation, and liability concerns are perceived as the challenges of the crowdsourcing type of data collection and sharing. Interestingly, although the stakeholders in this research strongly support empowerment of citizen and citizen-produced information; accuracy, management and liability are the main concerns, exceeding the security or privacy. In addition, no specific definition of resilience is proposed, except that community engagement and citizen supported map information contributes positively toward disaster resilience. In short, in the resilience context, community engagement is perceived as a way for sharing responsibility in emergencies.

Removing "community" and "engagement" in the SCOPUS search results in nine articles, but then the cyber security topic is becoming prominent. Only one additional work can be considered relevant (Oh, Agrawal, & Rao, 2013). The definition of resilience that includes ICT often treats it as critical infrastructure. Thus, the resilience definition covers how to enable such systems to survive, and fulfil the resilient principles such as reorganization, absorption, functional redundancy, and physical redundancy (Jackson, 2013). However, it is also not clear if it is applicable to ICT in terms of its usage for community engagement, community resilience and city resilience. The definition of resilience from the perspective of engineering, technology and ICT is often inflexible, and put a stress on the properties of physical infrastructure to cope with the hazard, and rarely put in the context of society. To put it differently, the link between technology and community is still missing.

Our work seeks to understand what properties that make community engagement through the use of information and communication technology able to contribute to the community's resilience to disaster. The vagueness of the resilience concept, the lack of consensus on the definition of resilience and the lacking technological aspects in some important documents encouraging community engagement and collaboration are noticeable. Under those circumstances, we are open to the development and change of the definition of resilience so that it encapsulates the meaning we try to capture and apprehend. As also mentioned in the DFID framework, in one hand, resilience should be placed in a "context", and allow a coherent answer to the question "resilience of what?". On the other hand, it should also cover "the disturbance", allowing one to address the question (DFID, 2011).

In some literature, city resilience stands on the partnerships and community resilience (Coles & Buckle, 2004; Norris, Stevens, Pfefferbaum, Wyche, & Pfefferbaum, 2008; Wells et al., 2013). They interpret community resilience as community capabilities that buffer it from or support effective response to disasters. Such capabilities include effective risk communications, organizational partnerships, and community engagement to improve, prepare to and respond to disaster. Communication through information sharing and knowledge exchange is one important keys for partnerships, which eventually is the very fundament of community resilience (Plough et al., 2013; Wells et al., 2013), and social media can be one mode of how to achieve that (Dufty, 2012).

For this article, we prefer the use of specified resilience "of what", and "to what" as also suggested by (Carpenter, Walker, Anderies, & Abel, 2001) to help us go further beyond the general resilience definitions that often proposed elsewhere in the literature. We suggest a working definition of resilience in this work as an adaptation of UNISDR's resilience definition to fit the city context and provide a room for the community engagement. The use of ICT technologies in the disaster, improvement for security and privacy of information sharing tools, and resilient communication should as much as possible be encapsulated in the definition.

To repeat, UNISDR (2004) defines resilience as the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. In the city context, we adapt this definition, and suggest that resilience should include explicitly all the important elements in a city (individual, community, organizations, and authorities) as well as physical infrastructure and environment to adapt by resisting or changing in order to reach and maintain acceptable level of functioning and structure. This is determined by the degree to which each element in all levels are capable of organizing themselves to increase this capacity. Embedded in this capacity is the ability of individuals and communities to absorb and prepare to make use of the different crisis management communication technologies, so that they can engage and share information better with each other and with public authorities. The definition should also include the capacity for learning practical security and privacy knowledge for better use of ICT-based engagement tools.

2.2. On Information Sharing, Security and Privacy

Indeed, sharing information is important, but recognizing factors (Yang & Maxwell, 2011) and challenges (Bharosa, Lee, & Janssen, 2010) that influence the success of information sharing is even more crucial. Different studies have mentioned that motivations, approaches and channels affect successful information sharing and indeed the technology. As often discussed in the Technology Acceptance Model (TAM), acceptance of technology is actually influenced by many factors (Aedo, Díaz, Carroll, Convertino, & Rosson, 2010; Lee, Bharosa, Yang, Janssen, & Rao, 2011; Turner, Kitchenham, Brereton, Charters, & Budgen, 2010), such as usefulness, being easy to use, trust (in giving personal information, in the technology itself), subjective norms, perceived innovativeness, and many more. Likewise, acceptance of the use of technology for communication in emergencies and sharing are affected by similar factors (Cha, 2014). Note that trust is actually one of the main factors that influence whether or not people will share information.

At this point, the importance of security and privacy will gradually come into the resilience picture via the following sequence of cause-effects: the resilience of the city is built upon community resilience which is basically the engagement of individual citizens in a disaster. Community resilience itself is built upon the willingness of individuals and organizations to cooperate and share information through existing or planned communication channels that more and more relies on ICTs. Attitude to privacy is very personal (Cottrill & "Vonu" Thakuriah, 2015), whether or not anonymity matters for them, thus security and privacy will be important. For some groups of individuals in the society, lack of security and privacy reduces enthusiasm for sharing information. The chain of weakening reverse effects will eventually divert the city's goal from achieving resilience.

Privacy and security often appear together although these two concepts are actually different. There are many different definitions of security, depending on the problem domain and the focus, and since security is a very complex concept, it is often defined with a focus on certain aspects of security rather than the complete abstract concept of security. However, in the broadest most abstract sense, security can be defined as "the state of being free from danger or threat" (Oxford dictionaries) or "the state of being protected or safe from harm" (Merriam Webster). Applied to computers, networks and information (Assel, Wesner, & Kipp, 2009), there are corresponding definitions focused on protecting computer hardware, software, networks, and in particular information (Assel, Wesner, & Kipp, 2009; Smith, Dinev, & Xu, 2011). What information protection entails is often divided into 3 (the 3 first) or 4 different concerns;

- **Confidentiality:** That only authorised personnel are able to access the information.
- **Integrity:** That only authorised personnel are able to modify the information.
- **Availability:** Authorised personnel are able to access the information when needed.
- **Authentication:** Verification of the identity of authorised personnel.

Privacy is an important related concern which is equally a complex issue (Bélanger & Crossler, 2011). It includes the ability to keep personal sensitive information confidential and to control the dissemination of personal information in general, as well as "the right to be let alone" and personal autonomy. In the Internet age, there are new challenges to privacy in the form of protection of online information (Cavoukian, Taylor, & Abrams, 2010), trusting the third- party storage providers (Galiero & Giammatteo, 2009), and accountable privacy supporting services (Camenisch, Groß, & Heydt-Benjamin, 2009). The methods used for online privacy protection are often similar to or identical to the methods used in information security, such as cryptographically protected communication and information storage (Bharosa, Janssen, & Tan, 2011; Hildebrandt, 2013), and privacy and security should exist by-design (Camenisch et al., 2009; Chik, 2013; Cottrill & "Vonu" Thakuriah, 2015; Galiero & Giammatteo, 2009; Hong & Landay, 2004; Lederer, Hong, Dey, & Landay, 2004; Parrish, 2010).

Measuring security and privacy is not easy. A lot of metrics have been proposed (Stolfo, Bellovin, & Evans, 2011), but many of them are not easily used by non-security experts. Pekárek and Pötzsch (2009) and Hull, Lipford, and Latulipe (2011) addresses the privacy issues in collaborative workspaces and social networks, which also can be including the consent dilemma (Solove, 2012). Pekárek and Pötzsch (2009) compare Wikipedia and Facebook and point out that in both, it is quite simple for third parties to gain access to personal data without infringing the technical rules set out for the use of the systems. In the case of Facebook this is due to the belief on the privacy default settings are optimum, or the users have no interest in privacy settings at all. For users of Wikis, customisation is simply not foreseen by the application, and thus the general user is often allowed access to a limited set of personal information, i.e. a basic profile or the user page. In the meantime, Hull et al. (2011) discuss further Facebook privacy issues arising from features, allowing non-friend users to see the contents shared for specific friends. In brief, privacy and security issues that may arise from different information sharing tools are evident, but in fact, it will also depend upon what types of users that will use the tool.

3. SCOPE AND METHODOLOGY

3.1. Scope

To clarify the focus areas of our research, we suggest metrics to assess security and quality of engagement tools that are useful for people with limited computer security background and no access to system internals. In other words, a set of metrics that are intended to be easy to use e.g. for researchers and practitioners in Emergency Management. Finally, in the outcome of this study, we will discuss the properties of three different user groups regarding the willingness to share information in a disaster. From this point of view, we will then discuss qualitatively how these properties affect resilience with examples or scenarios.

3.2. Research Questions

The central research questions (RQs) in this paper are as follow:

RQ 1: What is a good pragmatic approach to evaluate security and privacy of tools for citizen engagement in disasters?
RQ 2: What aspects of information sharing for supporting disaster resilience are not well covered in current state of the art?
RQ3: In what way can security and privacy concerns strengthen or weaken the disaster resilience?

There are several practical examples behind our earlier questions and arguments. Implementation of encryption, for example, a common method to protect information, is resource consuming. If the security is very strong and complex, it can make implementation and execution of the system hard, and usage more complicated. The end result could be that good intentions lead to making information less available rather than more. To support our research, we will investigate several cases and examples, as well as carry out a thorough analysis on these cases to show the relevance of our research questions. We will also support this by looking at the current information sharing tools and providing scenarios where security and privacy can be highly important, but currently often overlooked.

The contributions of this article are fourfold. First, we propose evaluation criteria for security and privacy of information sharing tools that are commonly used or designed for community engagement and information sharing purpose in a disaster situation. Second, we perform an evaluation of a relevant selection of tools according to our evaluation criteria and for some selected cases. The method is non-intrusive, based on published information, documentation, and policies. Third, we suggest practical recommendations for stakeholders wanting to implement a new engagement tool. Fourth, we define groups of users as a starting point to enable us to discuss properties of groups that can contribute to strengthening the city resilience, and to discuss how to build synergy and minimize trade-offs between security, privacy and resilience.

3.3. Methodology

We use a three-stage procedure, i.e. investigating different metrics for evaluating security and privacy, reviewing a selection of information sharing tools to test our proposed evaluation metrics, and finally examining different typical user groups and their needs for security and privacy to be willing to share information. We use the results as a basis for coming up with a set of recommendations. Our methodology is as follows:

Stage 1: We investigate different methods or metrics for evaluating the security and privacy of information sharing tools, and then select methods that are non-obtrusive, allowing us to observe without being an insider.
Stage 2: In this stage, we selected samples of tools for information sharing, as there are many tools available for use in non-crisis and crisis situations. In each stage of the emergency management cycle (preparedness, response, recovery and mitigation), different information sharing tools may be used. These metrics and tools will form a basis for answering RQ 1 and RQ2.
Stage 3: In the third stage, we examine the use cases in more detail, i.e.:

- **Whistle-blowers:** ("The dam is going to break, but the manager wants to hush it down instead of evacuating the valley!"). Whistle-blowers have a strong need for protection, or even their physical security could be endangered.
- **Social Media Users:** Twitterers and other social media members writing information that is accidentally or intentionally relevant for a case but aimed at friends/family and harvested by some tool. The general social media using public expect a certain level of security and privacy in the social media, and they should be able to expect their privacy to be respected if their posts are harvested for emergency management use, e.g. by anonymization or aggregation.
- **Active Helpers** and Disaster Actors i.e. People entering information into a tool with the express purpose of mitigating the disaster and strengthening the resilience. They know what they are doing, and in most cases, we only need to provide a minimum of security and privacy.

These three groups of users will be central to discuss RQ3 – if privacy and security strengthen or weaken resilience (section 5).

3.4. Procedures

To implement the methodology described earlier, we conduct the following procedures:

Stage 1-Metrics. There are many criteria that could be used to evaluate the *security* of the systems in question, among others:

- **Security by Design/Built-In Security:** This is a common criteria for evaluation of security (Fernandez, 2004). The system should be designed and built with security as a fundamental requirement from the start, not as an afterthought. However, this criterion is hard to judge in our case because we are doing black-box evaluation. In other words, security by design is only possible to evaluate with some degree of certainty for insiders, and is not easy to judge without knowing the technical details of the tool. Therefore, this criteria is not included in our evaluation.
- **Aspects of Security:** Security has different aspects that can be discussed separately (Avižienis et al., 2004): confidentiality, integrity and non-repudiation, and availability. It is important that these aspects are covered by the selected metrics. Authentication is also essential to ensure that the user is authorized to access information.
- **Testable security criteria:** Based on the listed security aspects as shown in Table 1, we select the following set of criteria for security evaluation since they are immediately observable and testable as a user on the running tool.

Table 1. Principles of Security

Security Aspect	Tested
Confidentiality	Secured communication (https/ssl/tls)
Integrity and nonrepudiation	Secured communication (https/ssl/tls)
	Can messages be deleted or modified
Availability	System is available at time of testing
Authentication	Password strength requirements
	2-factor authentication available

Concerning privacy, the Privacy by Design concept is essential. It is based on seven "foundational principles" (Cavoukian, 2006) as seen in the Table 2. The factors that can be tested to give an objective result in our scenario are marked as such in the table:

Several of these criteria are vague and hard to give a binary score, and some require insider information. And, not all security requirements can be tested (Pfleeger, 2012). Therefore, we have made a selection of the privacy and security criteria and concretized them into the tests that can be seen in the Table 3. The definitions and applications of these metrics are provided in Section 4.

Stage 2-Tools. Which tools are preferred to use can also vary from country to country, and from hazard to hazard. A wide range of ICT tools, and technologies has been proposed and used, ranging from Wikis, Smartphone apps, social media (especially Facebook, YouTube and Twitter), and other online engagement and real-time community mapping tools.

Ushahidi or Google Crisis Response are examples of tools for community mapping. Some of these ICT-based tools support crowdsourcing. In different countries, smartphone apps for emergencies have been widely used as communication tools by the government such as FEMA App, Hurricane

Table 2. Principles of the Privacy by design

Principles	Testable
Proactive not reactive; Preventative not remedial	
Privacy as the default setting	X
Privacy embedded into design	
Full functionality – positive-sum, not zero-sum	
End-to-end security – full lifecycle protection	X
Visibility and transparency – keep it open	
Respect for user privacy – keep it user-centric	

Table 3. Testable metrics for our research purpose

Metrics	What to check	Privacy/ security aspect
Encrypted communication	Communication over https/ssl/tls	confidentiality, integrity
Password minimum requirements	e.g. requirements for minimum length, combination of characters	authentication
Optional 2-factor authentication	Extra factor in addition to password, e.g. one-time code from mobile app or SMS.	authentication
System is online at time of testing	Simply testing that it is possible to use the system at time of testing.	availability
Privacy policy statement on web page or in app	Privacy policy statement visible from home web page or app start screen	privacy
Privacy configuration available	Is it possible to modify the privacy settings for the user?	privacy
Privacy-preserving options as default setting	If privacy configuration is available, do the default settings preserve privacy?	privacy

App (USA), Disaster Alerts, Emergency+, First Aid or Fire Near Me (Australia). Globally, some apps have been developed to alert of earthquakes such as QuakeWatch, Earthquake buddy or Disaster Alert.

For testing purposes, we have looked at different categories of information sharing models to support crisis, i.e. Wiki-based tools, a large number of mobile-apps, and social media, community mapping. We have only included those that are formally adopted or recommended as crisis communication tools in a specific country, or region. We varied the geographical area of the origin of the tools and included globally popular social media. The availability of these tools for testing, and enabling citizen engagement, were additional criteria we used when searching for them, thus we omitted the commercial ones. It is worth to mention that it is not our intention to provide an exhaustive list of engagement tools. Our goal is rather to provide exemplary cases where it is possible to use and test our proposed criteria to evaluate the security and privacy matters. The list of the tools covered in our analysis is as follows:

- **Wiki-Based Tools:** We have selected the two Wikis *Wiki for professionals* and *Emergency 2.0 Wiki* . *Wiki for professionals* is a product from the EU FP7 PEP (Public Empowerment Policies in Crisis Management) project that tried to engaged public to take concrete actions and share information in crisis preparedness, planning and response. Inclusion of public communication initiatives in authority communication, accessibility and inclusiveness of authority communication and making information widely available and findable, are among the strategies that are consider by the PEP project as key enablers for public empowerment.
- **Mobile Apps:** *FEMA App*: The app can be used for sharing disaster pictures, save a custom list of the items in your family's emergency kit, as well as the places users will meet in case of an emergency, and locations of open shelters. *Emergency+* is a national app circulated by Australia's emergency services to enable people to call the right number at the right time, anywhere in Australia. The app uses a mobile phone's GPS functionality so callers can provide emergency call-takers with their location information as determined by their smart phone. Emergency+ also includes SES and Police Assistance Line numbers as options, so non-emergency calls are made to the most appropriate number.
- **Social Media:** A study in the Public Empowerment Policies (PEP, 2016) project shows that Facebook, Twitter, blogs and YouTube are most preferred social media for preparedness, response and recovery. For our testing purpose, we look at Twitter, YouTube, Facebook and Google+ that are popular channels for communication, also about disasters.
- **Community Mapping:** These tools are often used with a crowdsourcing approach to information sharing or participatory mapping. A group of digital volunteers works together in a common shared map intended for improving the knowledge about disaster information, such as location of shelters, victims, hospitals, the supply needs. Ushahidi and Google Crisis Response, will be used as examples in this article for further analysis.

We do not elaborate further Stage 3 as it is quite clearly described in the Methodology Section.

4. RESULTS AND ANALYSIS

In section 4 and 5, we answer the three questions posed in section 2. First, we consider **RQ1:** What is a good pragmatic approach to evaluate security and privacy of tools for citizen engagement in disasters?

To answer this question, we have proposed a set of metrics that are testable from the user perspective. It means that an organisation of institution can quickly evaluate sharing tools that are available in the market (as free, open-source or commercial tools). We investigate a selection of existing solutions that are already in place so they can be tested according to the selected criteria. The definition of each metric used for evaluation is shown in Table 4.

Table 4. Security-Privacy Metrics and Definition

Metrics	Definition
Secure communication	If the tool is accessed through a secure connection (https) or not.
Password requirements	If there are requirements to the password strength used to log in and used the tools or services, e.g. minimum 6 characters, mix of letters and numbers, or have to include special characters.
2-factor authentication	If the users need to provide additional authentication in addition to the password, e.g. a code sent to the mobile phone.
Availability	If the service is available at the time of testing.
Privacy policy	If there is a clear privacy policy statement available.
Configurable privacy	If users have a freedom to decide which personal information they are willing to share into the tool.
Privacy as default	If the default setting of the privacy is public or private. For example, the default setting of the Facebook profile picture is open to the world. Users who are not aware of this default setting, may accidentally share his/her picture although it was not the initial intention.
Asking unneeded personal info	If the tool asks unnecessary personal info when registering for the service, such as birth date.
Modify or delete after reporting	If the tool allows modification or deletion of a message after it is submitted.

The evaluation results of the security and privacy of different tools using our selected metrics is presented in Table 5. The row lists the tested tools, while the columns captures the metrics used for testing. We notice that one aspect that is not well covered is how the usability is affected by the security and privacy. Is the tool more complicated to use because of the increased security and privacy? One of the metrics touches on this, regarding the good defaults for privacy. If one has to modify several complex settings to get the system into an acceptable state regarding privacy, as is the case in particular for social network sites, the usability obviously suffers. However, to capture a more complete picture of this issue would require a much more resource-consuming user testing and is outside the scope of this study which is focused on simple-to-test metrics. The results in Table 5 are used to answer ***RQ 2****: What aspects are not well supported concerning the information sharing for supporting disaster resilience in current state of the art?*

We see that the tests to all three social media options give almost the same results. In general, they are reasonably well-protected from a security point of view and allow the users to control their privacy – however with less than private defaults. In addition, the users may retract their messages without trace, and in the case of Facebook, edit a message after posting – with an indication that the message has been edited. Note that Twitter also has guidelines for use in crisis situations (Twitter, 2016). The wiki-based tools are much weaker on security, having unencrypted communication and little or no requirements for passwords. There also seems to be little focus on privacy, and indeed the wiki concept is all about openness and information sharing.

On the other hand, all changes are logged, so information cannot be retracted undetected once posted. Note that the Emergency 2.0 Wiki requires manual steps to add a new user, so we have not been able to test this as thoroughly as the other tools. The mobile apps are both limited to their respective national audiences, and our results therefore depend on what can be glanced from public documentation and descriptions. Among the community mapping tools, Ushahidi is special in that it is not one single tool, but rather a system to be configured and deployed in time of need (e.g. in Nepal after the earthquakes in spring 2015), and therefore we have sampled a selection of different Ushahidi installations to capture a representative impression on which we base the results. What is particularly interesting about Ushahidi is that it allows anonymous messages, without the creation of

Table 5. Test Results of the Security and Privacy of the Information Sharing Tools

	Security				Privacy				Non-repudiation
TOOLS	Secure communication	Password requirements	2-factor authentication	Available at time of testing	Privacy policy statement	Configurable privacy	Privacy as default	Asking unneeded personal info	Modify/delete after reporting
Social Media									
Twitter	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes (delete)
Facebook	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes (marked)
Google+	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
YouTube	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes (delete)
Wiki-based Tools									
Wiki for professionals	No	No[1)]	No	Yes	No[2)]	No	No	No	Yes (log)
Emergency 2.0 Wiki	?[3)]	?	?	Yes	Yes[4)]	?	?	?	?
Mobile App									
FEMA App	?[5)]	No	No	No[6)]	Yes	No	Yes	No	No (moderated)
Emergency+	N/A[7)]	N/A	N/A	No[8)]	No	No	No	N/A	No
Community Mapping									
Ushahidi deployments[9,10)]	Optional[11)]	N/A	N/A	Yes[12)]	Yes[13)]	Yes[14)]	Yes	Optional[15)]	No
Google Crisis Response	Yes	Yes	Yes	No[16)]	Yes[17)]	No	No	No	Yes
Facebook safety check	Yes	Yes	Yes	No[18)]	Yes	Yes	No	Yes	N/A
Instant Messaging									
Skype	Yes[19)]	Yes	No	Yes	Yes	Yes	No	Yes	Yes (marked)

Table notes: 1) Allows e.g. "123" which is a very weak password.; 2) Link present, but no text.; 3) Test user activation pending; 4) Activated LinkedIn group membership; 4) Via Terms of Use; 5) No information if photo upload is secure; 6) No personal identifiable information (PII) sent; 6) Only available in USA.; 7) Only for making phone calls; 8) Only available in Australia; 9) https://beinglgbtinasia.crowdmap.com;10)Deployment in Sweden http://www.diskrimineringskartan.se; 11) Depends on deployment. No PII sent by default.; 12) Deployed when needed; 13) Depends on deployment; 14) For deployment managers, not for end-users; 15) Anonymous allowed; 16) Deployed as needed; 17) Basic warning info only. 18) Activated when/where needed; 19) Call from skype to phone is not encrypted across the phone network.

an account, as opposed to most of the other tools. Google crisis response consists of several tools, we have chosen to evaluate the person finder. As no fully operational person finder was available at time of testing, we base our results on a test setup. In the same way, Facebook safety check is only made available in particular large-scale emergencies, and only for people in the affected regions, so it is not possible to test. Therefore, these results are based on information gathered from documentation and other relevant sources

5. DISCUSSION, SOLUTIONS, AND IMPLICATION FOR RESILIENCE

In this section, we will answer RQ3: In what way can security and privacy concerns strengthen or weaken the disaster resilience? We analyse the willingness of different groups (whistle-blowers, social media users and active helpers) to share information during a crisis based on each group's preference on required security and privacy strength. A city is used as exemplary case in our analysis. Our discussion will focus on three points: 1) Situations that will strengthen or weaken the resilience, based on user group perspectives; 2) The predicted preferable tools of each group; and 3) The information flow model based on the tested tools linked to the predicted need for security and privacy, and user group categories that are suited for each information flow model.

Table 6 depicts the proposed framework to analyse the willingness to share information given different privacy and security strength in the engagement tools. The rows represent the user groups. The columns capture the strength categories of security and privacy embedded in the sharing tools i.e. "No privacy/ security", "Average privacy/ security" and "Strong privacy/ security/ anonymity". *The light grey* area on the right side represents the optimal smooth information flow to the city stakeholders, when the preferable privacy of users matches the provided information sharing tools. The dark grey colour area in the middle, shows the information flow to the city when the security and privacy level of the tools is average. While the black area in the left side is a situation where only people who do not bother so much about privacy, motivated by altruistic spirit and would just help facilitating the communications. In this situation, we may lose the potential information from two other groups, i.e. Whistle-blowers and social media users.

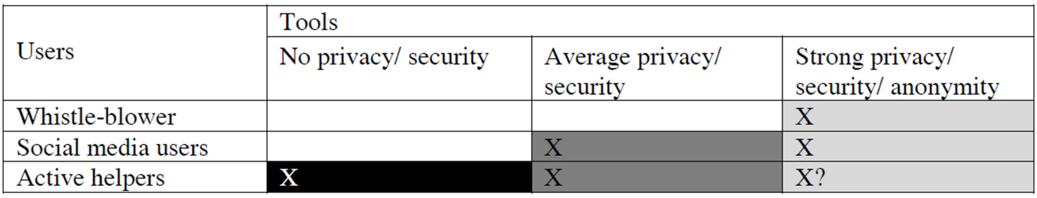
Table 6 implies that active citizen engagement for sharing disaster related information only occur if the stakeholders can provide tools that incorporate different groups' requirement for security and privacy. The grey area in Table 6 represents the information flow from different user groups that may be weakened or blocked.

Strong privacy could also include anonymity, which will encourage Whistle-Blowers, since they can submit reports without risk of repercussions. If we consider our analysis in Section 4, the Whistle Blower will tend to use e.g. Ushahidi-type tools where reporters can provide information without being identified or required to login. However, Ushahidi, of course, is very much dependent upon the preference and deployment configuration of the system owners if they would like to encourage submission of information from Whistle-Blowers or only from Active Helpers.

Why do we care about Whistle-Blowers in this information sharing context? Because Whistle-Blowers who want their privacy to be particularly protected, could be the group that possess unique and important information that may require rapid handling and mitigation. Therefore, they have a clear reason and need to be protected as informants. Wikileaks is an extreme example of framework that fits the Whistle-Blowers, where people feel secure to share information anonymously without fear of being identified as a reporter, apart from the controversy surrounding this case. In the disaster case, the example could be any extreme hazards such as industrial disaster hazards e.g. chemical leaks, radiation leaks to the water system or other critical infrastructure services that is vital for the city life and the citizens. In such case, the most knowledgeable person knowing the detail of the case may be reluctant to openly share the information because of many different reasons such as loss of reputation, job or even being taken to court for leaking confidential information.

The Active Helpers may not care about strong or weak security because the motivation is to help, share information and contribute as much as possible to mitigate the disaster impact. Thus, too much

Table 6. Willingness to share information



Users	Tools		
	No privacy/ security	Average privacy/ security	Strong privacy/ security/ anonymity
Whistle-blower			X
Social media users		X	X
Active helpers	X	X	X?

security may just hinder or slow them down to actively share information, which eventually may weaken the resilience. Thus, the X sign with a question mark in the right bottom corner in the Table 5 represents the double-edged sword issue that may arise, when the extra effort to ensure security becomes too much, while this group could in fact be the most active one.

By having a good framework for understanding the willingness to share in the different groups of users as shown in Table 6, we can then predict the preferred tools for each type of user group. The whistle blower prefers tools allowing anonymous submission or sharing. Social media users prefer Facebook, Twitter, YouTube or other channels. While active helpers will use social media, mobile apps, sharing tools (any available tools), but preferably simple tools. Note that this preferred tool example does not necessarily indicate that it should be exactly this one in reality. The security and privacy features are what matters in the indicated choices of our example. Figure 1 proposes five information flow models that link the user groups with predicted security requirements.

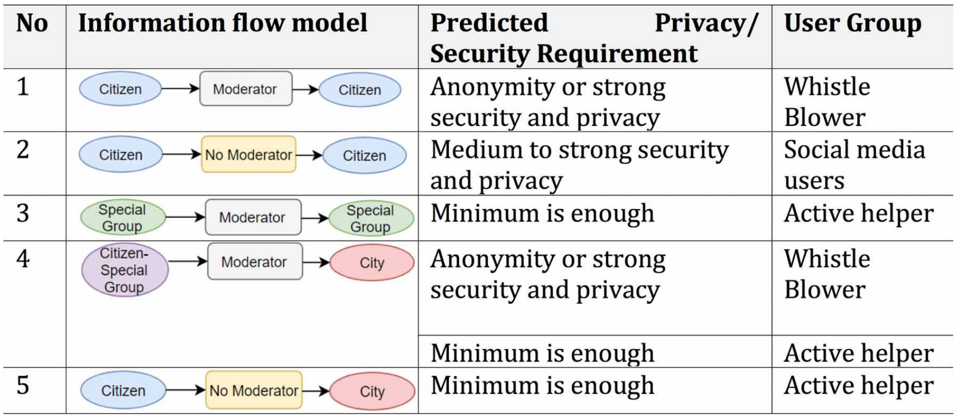
In Model 1, the information flows via sharing tool from citizen to citizen (C to C) is moderated. The intended communication of this type of users is to provide an alert about threats or dangers that if not reported, would have been unknown to other citizens. This type of information needs moderation for quality and truth validation. The tool needs to be supported by strong security and privacy. This model is likely to fit whistle-blowers.

Model 2 is unmoderated C to C information flow which typically intended for informing the circle of friends and family. The social media users belong to this second model, who are likely to be satisfied with medium security/privacy requirements. In this case, moderation is unnecessary.

Model 3 is moderated information flow from Special group to special group (SG to SG). The aim of the communication in this model is to voluntarily gather necessary disaster-related information as quickly as possible and share it to other voluntary groups. The ultimate goal is to help people affected by crisis with extra useful information. To a certain degree, it may help disaster responders. Moderation in this communication model is necessary. Predicted users are "active helper" groups, who can work with minimum security or privacy.

Model 4 is the moderated information flow from citizen to city (CSG to City). The intended communication of this type of users is twofold. For SG is to inform about the resources available, critical situations that need to be tackled, or other issues that are thought necessary for the stakeholders in crisis. For **C**, the communication goal is the same as Model 1, i.e. to give an alert. The information flow in this Model 4 does not need to be known by all people. The expectation is quick actions taken based on shared information. The active helpers and whistle-blowers belong to this fourth model. Thus, flexible security and privacy are highly important. In this case, moderation is necessary.

Figure 1. Information flow model, privacy-security requirement



No	Information flow model	Predicted Privacy/ Security Requirement	User Group
1	Citizen → Moderator → Citizen	Anonymity or strong security and privacy	Whistle Blower
2	Citizen → No Moderator → Citizen	Medium to strong security and privacy	Social media users
3	Special Group → Moderator → Special Group	Minimum is enough	Active helper
4	Citizen-Special Group → Moderator → City	Anonymity or strong security and privacy	Whistle Blower
		Minimum is enough	Active helper
5	Citizen → No Moderator → City	Minimum is enough	Active helper

Model 5 is unmoderated Citizen to City information flow. The intended communication is to notify stakeholders their availability or their volunteer efforts in responding to disasters. This type of communication does not need moderation.

6. CONCLUSION

In this article, we have proposed security and privacy metrics, and intuitive-based user group classifications with respect to the information and communication engagement tools. We conclude that the requirement for privacy and/or anonymity depends on the intended communication target, and this varies between the different user groups, and on the potential risk associated with a breach of privacy. The insights from the discussion in this paper is that we should mitigate reluctances of the whistle-blower to use any types of community engagement and information sharing. For a whistle-blower that sometimes carry urgent information, the risk is very high that he will be in major trouble if his privacy is violated. We also should not slow down the active helpers by making the tool too complex - e.g. through excessive security, although for an active helper, that risk is more like a minor annoyance. Both these groups usually want to spread the information as wide as needed to reach the proper authorities. On the other hand, social media users tend to target friends and family and may for example either want to tell that they are safe, or inform about local risks. This information may still be of use to the crisis handlers if it is available to the public, but reasonable privacy settings may also prevent this to happen.

Thus, the policy makers or local authority in the city should be willing to consider all relevant types of user groups in the society based on their preferred privacy and security requirements, and allow different user groups to participate through different tools, including representative tools from those classes of tools mentioned in Table 6. Leaving out whistle-blowers or slowing down and annoying active helpers would impair citizen engagement and ultimately resilience. To be able to get a complete picture from information shared by citizens, we suggest that both a specialised tool with simple verified-user messages as well as opening for moderated anonymous messages - and relevant social networks, should be utilized.

Finally, we also need to cover some limitations of our work: 1) We assume that evaluators of the security and privacy level of the engagement tools have a limited expertise on security but should know the minimum requirements to determine whether or not such criteria are fulfilled or covered. 2) The methods for evaluating security and privacy of the engagement tools are not from the insider perspective but from what information has been made available for public or is externally observable. 3) The suggested metrics are only an initial proposal. The security and privacy metrics that are relevant for city stakeholders can be elaborated further in different stages of the resilience cycle: preparedness, response, recovery and mitigation. Likewise, the matrix for the user groups can be elaborated further to include e.g. engagement tools for helping individuals that are affected by the disasters, where the security and privacy will be extremely important. For example, the engagement tools will include counselling for trauma, shocks or other psychological or psychosocial problems, or other issues that are not identified here. 4) To be aware that the strong privacy or anonymity that allows whistle-blowers to feel comfortable enough to submit their information, can also be used for actors with bad intentions, for misleading of even attempting to trap rescue personnel, or for submitting bomb threats and other criminal messages. 5) Our experiment, especially the evaluation of the availability metric is based on limited observation time, and not e.g. through monitoring over longer period, where then we could claim e.g. "uptime of 99%".

There are many directions that could be investigated further based on this study, but it should still be able to stand on its own as a set of guidelines for the security and privacy aspects of selecting tools for engaging citizens in creating a resilient society.

REFERENCES

Aedo, I., Díaz, P., Carroll, J. M., Convertino, G., & Rosson, M. B. (2010). End-user oriented strategies to facilitate multi-organizational adoption of emergency management information systems. *Information Processing & Management*, *46*(1), 11–21. doi:10.1016/j.ipm.2009.07.002

Aldunce, P., Beilin, R., Handmer, J., & Howden, M. (2014). Framing disaster resilience: The implications of the diverse conceptualisations of "bouncing back". *Disaster Prevention and Management: An International Journal, 23*(3), 252-270. doi:10.1108/DPM-07-2013-0130

Assel, M., Wesner, S., & Kipp, A. (2009). A security framework for dynamic collaborative working environments. *Identity in the Information Society*, *2*(2), 171–187. doi:10.1007/s12394-009-0027-1

Avižienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, *1*(1), 11–33. doi:10.1109/TDSC.2004.2

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information system. *Management Information Systems Quarterly*, *35*(4), 1017–A1036. doi:10.2307/41409971

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, *49*(18), 5375–5393. doi:10.1080/00207543.2011.563826

Bharosa, N., Janssen, M., & Tan, Y.-H. (2011). A research agenda for information quality assurance in public safety networks: Information orchestration as the middle ground between hierarchical and netcentric approaches. *Cognition Technology and Work*, *13*(3), 203–216. doi:10.1007/s10111-011-0172-9

Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers*, *12*(1), 49–65. doi:10.1007/s10796-009-9174-z

Birkland, T. A. (2009). Disasters, catastrophes, and policy failure in the homeland security era1. *The Review of Policy Research*, *26*(4), 423–438. doi:10.1111/j.1541-1338.2009.00393.x

Camenisch, J., Groß, T., & Heydt-Benjamin, T. S. (2009). Accountable privacy supporting services. *Identity in the Information Society*, *2*(3), 241–267. doi:10.1007/s12394-009-0023-5

Carpenter, S., Walker, B., Anderies, J. M., & Abel, N. (2001). From metaphor to measurement: Resilience of what to what? *Ecosystems*, *4*(8), 765–781. doi:10.1007/s10021-001-0045-9

Cavoukian, A. (2006). Privacy by design: The 7 foundational principles. Implementation and mapping of fair information practices. *Privacy Association*. Retrieved from https://www.privacyassociation.org/media/presentations/11Summit/RealitiesHO1.pdf

Cavoukian, A., Taylor, S., & Abrams, M. (2010). Privacy by design: Essential for organizational accountability and strong business practices. *Identity in the Information Society, 3*(2), 405-413. doi:10.1007/s12394-010-0053-z

Cha, J. (2014). Usage of video sharing websites: Drivers and barriers. *Telematics and Informatics*, *31*(1), 16–26. doi:10.1016/j.tele.2012.01.003

Chik, W. B. (2013). The Singapore personal data protection act and an assessment of future trends in data privacy reform. *Computer Law & Security Review*, *29*(5), 554–575. doi:10.1016/j.clsr.2013.07.010

Coles, E., & Buckle, P. (2004). Developing community resilience as a foundation for effective disaster recovery. *Australian Journal of Emergency Management*, *19*(4), 6.

Cottrill, C. D., & "Vonu" Thakuriah, P. (2015). Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. *Transportation Research Part C, Emerging Technologies*, *56*, 132–148. doi:10.1016/j.trc.2015.04.005

CrisisCommunication.fi. (2014). Crisis communication wiki for professionals. Retrieved from http://www.crisiscommunication.fi/wiki/Main_Page

DFID. (2011). *Defining disaster resilience: A dfid approach paper. Department of international development*. Retrieved from http://www.fsnnetwork.org/sites/default/files/dfid_defining_disaster_resilience.pdf

Dufty, N. (2012). Using social media to build community disaster resilience. *Australian Journal of Emergency Management*, *27*(1), 40.

Emergency2.0 Wiki Editors. (2011). Emergency 2.0 wiki. Retrieved from http://emergency20wiki.org/wiki/index.php/Main_Page

FEMA. (2017). Fema mobile app. Retrieved from https://www.fema.gov/mobile-app

Fernandez, E. B. (2004). A methodology for secure software design. *Paper presented at the Conference on Software Engineering Research and Practice (SERP'04)*, Las Vegas, NV.

Galiero, G., & Giammatteo, G. (2009). Trusting third-party storage providers for holding personal information. A context-based approach to protect identity-related data in untrusted domains. *Identity in the Information Society*, *2*(2), 99–114. doi:10.1007/s12394-009-0033-3

Gil-Garcia, J. R., Zhang, J., & Puron-Cid, G. (2016). Conceptualizing smartness in government: An integrative and multi-dimensional view. *Government Information Quarterly*, *33*(3), 524–534. doi:10.1016/j.giq.2016.03.002

Google. (2018). Google person finder. Retrieved from https://google.org/personfinder

Haworth, B. (2016). Emergency management perspectives on volunteered geographic information: Opportunities, challenges and change. *Computers, Environment and Urban Systems*, *57*, 189–198. doi:10.1016/j.compenvurbsys.2016.02.009

Hildebrandt, M. (2013). Balance or trade-off? Online security technologies and fundamental rights. *Philosophy & Technology*, *26*(4), 357–379. doi:10.1007/s13347-013-0104-0

Hong, J. I., & Landay, J. A. (2004). An architecture for privacy-sensitive ubiquitous computing. *Paper presented at the 2nd international conference on Mobile systems, applications, and services.*

Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology*, *13*(4), 289–302. doi:10.1007/s10676-010-9224-8

Jackson, S. (2013). Resilience principles for the ICT sector. *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, 36.

Lederer, S., Hong, J. I., Dey, A. K., & Landay, J. A. (2004). Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing*, *8*(6), 440–454. doi:10.1007/s00779-004-0304-9

Lee, J., Bharosa, N., Yang, J., Janssen, M., & Rao, H. R. (2011). Group value and intention to use — a study of multi-agency disaster management information systems for public safety. *Decision Support Systems*, *50*(2), 404–414. doi:10.1016/j.dss.2010.10.002

Lindsay, B. R. (2011). *Social media and disasters: Current uses, future options, and policy considerations*. Retrieved from https://www.nisconsortium.org/portal/resources/bin/Social_Media_and_Dis_1423591240.pdf

Liu, P., & Chetal, A. (2005). Trust-based secure information sharing between federal government agencies. *Journal of the American Society for Information Science and Technology, 56*(3), 283-298. doi:10.1002/asi.20117

Liu, S. B. (2014). Crisis crowdsourcing framework: Designing strategic configurations of crowdsourcing for the emergency management domain. *Comput. Supported Coop. Work, 23*(4-6), 389-443. doi:10.1007/s10606-014-9204-3

Liza, P. (2011). Sociotechnical uses of social web tools during disasters. In C. Elayne (Ed.), *Knowledge development and social change through technology: Emerging studies* (pp. 97–108). Hershey, PA: IGI Global.

Manyena, S. B. (2006). The concept of resilience revisited. *Disasters, 30*(4), 434-450. doi:10.1111/j.0361-3666.2006.00331.x

Martin, R. (2012). Earthquake buddy app sends your location to friends when an earthquake hits. *Techinasia*. Retrieved from https://www.techinasia.com/earthquake-buddy-alert-location

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American Journal of Community Psychology, 41*(1-2), 127-150. doi:10.1007/s10464-007-9156-6

NSW. (2018). Nsw rural fire service. Retrieved from http://www.rfs.nsw.gov.au/about-us/our-districts/mia/fire-information/fires-near-me

Oh, O., Agrawal, M., & Rao, H. R. (2013). Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. *MIS Quarterly: Management Information Systems*, *37*(2), 407–426. doi:10.25300/MISQ/2013/37.2.05

Palen, L., Anderson, K. M., Mark, G., Martin, J., Sicker, D., Palmer, M., & Grunwald, D. (2010). A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters. *Paper presented at the 2010 ACM-BCS visions of computer science conference*.

Parrish, J. L. (2010). Papa knows best: Principles for the ethical sharing of information on social networking sites. *Ethics and Information Technology*, *12*(2), 187–193. doi:10.1007/s10676-010-9219-5

PDC. (2018). Disaster alert. Retrieved from http://www.pdc.org/solutions/tools/disaster-alert-app/

Pekárek, M., & Pötzsch, S. (2009). A comparison of privacy issues in collaborative workspaces and social networks. *Identity in the Information Society*, *2*(1), 81–93. doi:10.1007/s12394-009-0016-4

PEP. (2016). Public empowerment policies for crisis management. Retrieved from https://agoracenter.jyu.fi/projects/pep

Pfleeger, S. L. (2012). Security measurement steps, missteps, and next steps. *IEEE Security and Privacy, 10*(4), 5-9. doi:10.1109/MSP.2012.106

Pipek, V., Liu, S. B., & Kerne, A. (2014). Crisis informatics and collaboration: A brief introduction. *Comput. Supported Coop. Work, 23*(4-6), 339-345. doi:10.1007/s10606-014-9211-4

Plough, A., Fielding, J. E., Chandra, A., Williams, M., Eisenman, D., Wells, K. B., . . . Magaña, A. (2013). Building community disaster resilience: Perspectives from a large urban county department of public health. *American Journal of Public Health, 103*(7), 1190-1197. doi:10.2105/AJPH.2013.301268

Quakewatch. (2018). Earthquake prediction center. Retrieved from http://quakewatch.net

Rogers, P. (2013). Rethinking resilience: Articulating community and the UK riots. *Politics, 33*(4), 322-333. doi:10.1111/1467-9256.12033

Schwartz, P. M., & Solove, D. J. (2011). Pii problem: Privacy and a new concept of personally identifiable information, the. *NYUL Rev.*, *86*, 1814.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1880.

Stolfo, S., Bellovin, S. M., & Evans, D. (2011). Measuring security. *IEEE Security and Privacy*, *9*(3), 60–65. doi:10.1109/MSP.2011.56

Tapia, A. H., & Moore, K. (2014). Good enough is good enough: Overcoming disaster response organizations' slow social media data adoption. *Comput. Supported Coop. Work, 23*(4-6), 483-512. doi:10.1007/s10606-014-9206-1

Trnka, J., & Johansson, B. J. E. (2011). Resilient emergency response: Supporting flexibility and improvisation in collaborative command and control. In E. J. Murray (Ed.), *Crisis response and management and emerging information systems: Critical applications* (pp. 112–138). Hershey, PA: IGI Global. doi:10.4018/978-1-60960-609-1.ch009

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. *Information and Software Technology*, *52*(5), 463–479. doi:10.1016/j.infsof.2009.11.005

Twitter. (2016). Best practices for using twitter in times of crisis. Retrieved from https://about.twitter.com/products/alerts/helpful-assets

UN. (2014). World's population increasingly urban. Retrieved from http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html

UNISDR. (2004). *Living with risk: A global review of disaster reduction initiatives: 2004 version - volume ii annexes*. Retrieved from http://www.unisdr.org/files/657_lwr21.pdf

UNISDR. (2005, January 18-22). Hyogo framework for action 2005-2015: Building the resilience of nations and communities to disasters. *Paper presented at the World Conference on Disaster Reduction*, Kobe, Hyogo, Japan.

Ushahidi Editors. (2018). Ushahidi. Retrieved from https://www.ushahidi.com/

Wells, K. B., Tang, J., Lizaola, E., Jones, F., Brown, A., Stayton, A., . . . Plough, A. (2013). Applying community engagement to disaster planning: Developing the vision and design for the Los Angeles County community disaster resilience initiative. *American Journal of Public Health, 103*(7), 1172-1180. doi:10.2105/AJPH.2013.301407

WikiLeaks. (2015). Wikileaks. Retrieved from http://www.wikileaks.com

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, *28*(2), 164–175. doi:10.1016/j.giq.2010.06.008

Jaziar Radianti received her PhD in System Dynamics applied for an information security area from University of Bergen, Norway. Dr. Radianti is a researcher for CIEM (Centre for Integrated Emergency Management) at Department of ICT, University of Agder, Norway. She has served as a reviewer for numerous international conferences and has published more than 60 scientific papers. Her research interests include the application of simulation approaches, especially system dynamics, fire dynamics, and Bayesian network modeling for disaster and crisis management. She has extensive research experience after completing her PhD education, as she has been working on the following research areas: cyber-security, fire emergencies, smartphone sensing, disaster resilience and serious game. Currently, Dr. Radianti is a head of CIEMlab and experimental operation centre, a situation room research infrastructure for crisis management, at the University of Agder (Since 2015 to date). She is also leading the KriseSIM project, a research on virtual training tool for a control room (2017-2019), and a senior researcher I H2020 project Smart-Mature Resilience on disaster resilience (2015-2018).

Terje Gjøsæter is an associate professor in universal design of ICT at Oslo Metropolitan University, Norway. He completed his PhD at the Department of ICT at University of Agder in 2015, in computer language theory with a focus on design principles and usability of meta-modelling tools. His research interests include such diverse topics as universal design, accessibility, security of critical infrastructure, usable security, privacy, emergency management, computer language theory and metamodelling, usability of domain-specific languages, and eHealth. He has published more than 30 peer-reviewed articles and conference papers and has experience from several EU projects. He participated in the FP6 EIAO IST project from 2004 to 2007, performing research and development related to large-scale automatic assessment of web accessibility. From 2012 to 2014, he joined the FP7 PRECYSE project, doing research related to establishing a methodology for assessing and enforcing security of critical infrastructures. From 2014 to 2016, he took part in the FP7 SEMIAH project on design and development a scalable, secure and privacy-preserving energy management infrastructure for aggregation of households in the smart grid.