

# Secure and Privacy-preserving Information Sharing for Enhanced Resilience

Jaziar Radianti<sup>1</sup> and Terje Gjøsæter<sup>2</sup>,

<sup>1</sup> Centre for Integrated Emergency Management UiA,  
Department of ICT, Jon Lilletunsvei 9,  
N-4879 Grimstad, Norway

<sup>2</sup> HIOA, Department of Computer Science, Box 4, St. Olavs plass  
N-0130 Oslo, Norway

jaziar.radianti@uia.no, terje.gjosater@hioa.no

**Abstract.** City resilience is a pressing issue worldwide due to the fact that the majority of the population reside in urban areas. When disaster strikes, the consequences will be higher in the cities as more people are affected. To achieve resilience, different entities as well as the public in the city should cooperate and share information during a disaster. Community engagement and information sharing using ICT are considered to be efficient means for strengthening community and city resilience. Here, we suggest an easy-to-use set of metrics for evaluating the security and privacy of information sharing platforms for resilience, and apply them to a selection of these platforms to evaluate the state of the art with regard to these aspects. [It turns out that in most of them are reasonably well-protected, however with less than private default settings.](#) We furthermore 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. [This discussion reveals that security and privacy is of particular importance for whistle-blowers that sometimes may carry urgent information, while volunteers and active helpers are less affected by the level of security and privacy offered.](#)

**Keywords:** Resilience, security, privacy, resilience tool, information sharing

## 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 [1]. 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 [2, 3], with the help of information and communication technologies (ICT) tools that are becoming acceptable for facilitating crisis communication [4]. Interpreting further the spirit of the Hyogo Framework Action [5], 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. Hence, the role of ICT tools to enable the society in general to adapt and recover from hazards and stresses is evident [6], especially to ensure that the right information flows smoothly to the intended audience.

What is resilience? UNISDR [7] 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 [8, 9], 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 [10]. 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 [6, 11].

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 [12]. Security of information is essential to some organizations and actors before they are willing to share it [13]. For private citizens, trust concerning privacy protection is crucial, covering personal sensitive information (PSI) and personally identifiable information (PII, information that can identify them) [14]. 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 prioritised 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 paper 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.

This paper is divided into 6 sections. In the next section we describe our scope, research questions and methodology. Section 3 describes the relevant literature for our case. In Section 4, we report the result and analysis from our study. Discussion and lessons learnt from our research and implications for disaster resilience is presented in Section 5. Section 6 is a summary of the main findings of this study and its limitations.

## **2 Scope and Methodology**

To clarify the limits and focus areas of our research, we delineate the scope of this article. First, we will not discuss privacy and security in terms of algorithms which are very common in computer science literature [15-17]. We also did not include the privacy issues caused by providers of engagement platforms. Instead, we suggest metrics that are possible to use for people with limited computer security

background to assess security and quality of engagement tools or platforms. In other words, we use testable, easy-to-use metrics. Finally, in the outcome of this study, we will not propose metrics to measure the influence of privacy and security on the disaster resilience. We will instead 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. 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 and platforms 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.

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-Metrics.** We investigate different methods or metrics for evaluating the *security* and *privacy* of information sharing tools, and then select methods that are non-obtrusive, allow us to observe without being an insider. There are many criterias 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 [18]. 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 metric is not included in our evaluation.

- *Aspects of Security*: Security has different aspects that can be discussed separately [12]: 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 platform.

**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" [19] 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:

**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	

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 [20]. 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.

**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
---	--	---------

**Stage 2-Tools.** In this stage, we selected samples of tools for information sharing, as there are many tools or platforms 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. 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 Wiki platforms, Smartphone apps, social media (especially Facebook, YouTube and Twitter), and other online engagement and real-time community mapping platforms.

Ushahidi [21] or Google Crisis Response [22] are examples of platforms 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 [23], Hurricane App (USA), Disaster Alerts, Emergency+, First Aid or Fire Near Me [24] (Australia). Globally, some apps have been developed to alert of earthquakes such as QuakeWatch [25], Earthquake buddy [26] or Disaster Alert [27].

For testing purposes, we have looked at different categories of information sharing models to support crisis, i.e. Wiki-based platforms, a large amount 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 Platforms.** We have selected the two platforms *Wiki for professionals* [28] and *Emergency 2.0 Wiki* [29]. *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 [30] 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. These metrics and tools will form a basis for answering **RQ 1** and **RQ2**.

**Stage 3-Use Cases.** In the third stage, we examine the use cases in more detail, i.e.:

- **Whistle-blowers:** ("The dam is going to break, and 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 platform, 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 Related Works

This section targets answering the following questions: How do 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?

Indeed, sharing information is important, but recognizing factors [2] and challenges [31] 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 [32-34], 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 [35]. Note that trust is, in fact, 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 [36], 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.

Measuring security and privacy is not trivial, as a lot of metrics have been proposed [37], and many of them are not so easily used if one is not a computer security expert. [Pekárek and Pöttsch \[38\]](#) and [Hull, Lipford \[39\]](#) addresses the privacy issues in collaborative workspaces and social networks, which also can be including the consent dilemma [40]. [Pekárek and Pöttsch \[38\]](#) compare the Wikipedia and Facebook platforms and point out that on both platforms, 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, Lipford \[39\]](#) discuss further Facebook privacy issues arising from features, allowing non-friend users to see the contents shared for specific friends. The privacy design is blamed as a cause of this issue. 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.

#### 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 and platforms for citizen engagement in disasters?*

**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 platform.
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.

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 platform tools that are available in the market (as free, open-source or commercial tools). We investigate a selection of existing solutions or platforms 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 5.** The Test Results of the Security and Privacy of the Information Sharing Tools

TOOLS	Security				Privacy				Non-repudiation
	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
<i>Social Media</i>									
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)
<i>Wiki-based Platform</i>									
Wiki for professionals	No	No <sup>1)</sup>	No	Yes	No <sup>2)</sup>	No	No	No	Yes (log)
Emergency 2.0 Wiki	? <sup>3)</sup>	?	?	Yes	Yes <sup>4)</sup>	?	?	?	?
<i>Mobile App</i>									
FEMA App	? <sup>5)</sup>	No	No	No <sup>6)</sup>	Yes	No	Yes	No	No (moderated)
Emergency+	N/A <sup>7)</sup>	N/A	N/A	No <sup>8)</sup>	No	No	No	N/A	No
<i>Community Mapping</i>									
Ushahidi deployments <sup>9,10)</sup>	Optional <sup>11)</sup>	N/A	N/A	Yes <sup>12)</sup>	Yes <sup>13)</sup>	Yes <sup>14)</sup>	Yes	Optional <sup>15)</sup>	No
Google Crisis Response	Yes	Yes	Yes	No <sup>16)</sup>	Yes <sup>17)</sup>	No	No	No	Yes
Facebook safety check	Yes	Yes	Yes	No <sup>18)</sup>	Yes	Yes	No	Yes	N/A
<i>Instant Messaging</i>									
Skype	Yes <sup>19)</sup>	Yes	No	Yes	Yes	Yes	No	Yes	Yes (marked)

Note: 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.

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 the 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 [41]. The wiki-based platforms 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 and platforms. 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 platforms, Ushahidi is special in that it is not one single tool, but rather a platform to be 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 an account, as opposed to most of the other tools and platforms. 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 Implications 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 platforms. 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 match the provided information sharing platforms. *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.** 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?

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.

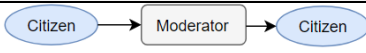
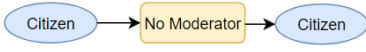

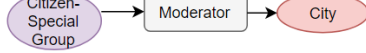
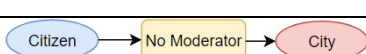
Strong privacy could also include anonymity, which will encourage *Whistle-Blowers*, since they can submit reports without risk of repercussions. If we consider our analysis in Section 4, the *Whistle Blower* will tend to use e.g. an Ushahidi-type platform where reporters can provide information without being identified or required to login. However, Ushahidi, of course, is very much dependent upon the preference and deployment configuration of the platform 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 [42] 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 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 platforms (any available tools), but preferably simple tools. Note that this preferred tools 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. Table 7 proposes five information flow models that link the user groups with predicted security requirements.

**Table 7.** Information flow model, privacy-security requirement

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

In *Model 1*, the information flows via sharing platform 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 platform 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. *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 Conclusions, Limitations and Future Work

In this paper, 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 platform 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 platforms, including representative platforms from those classes of platforms 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 platform 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 is 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.~~

## 7 References

1. UN. *World's population increasingly urban*. 2014; Available from: <http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html>.
2. Yang, T.-M. and T.A. Maxwell, *Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors*. *Government Information Quarterly*, 2011. **28**(2): p. 164-175.
3. Palen, L., et al. *A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters*. in *Proceedings of the 2010 ACM-BCS visions of computer science conference*. 2010. British Computer Society.
4. Pipek, V., S.B. Liu, and A. Kerne, *Crisis Informatics and Collaboration: A Brief Introduction*. *Comput. Supported Coop. Work*, 2014. **23**(4-6): p. 339-345.
5. UNISDR. *Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters*. in *World Conference on Disaster Reduction*. 2005. Kobe, Hyogo, Japan.
6. Trnka, J. and B. Johansson, J. E. , *Resilient Emergency Response: Supporting Flexibility and Improvisation in Collaborative Command and Control*, in *Crisis Response and Management and Emerging Information Systems: Critical Applications*, E.J. Murray, Editor. 2011, IGI Global: Hershey, PA, USA. p. 112-138.
7. UNISDR, *Living with risk: a global review of disaster reduction initiatives: 2004 version - Volume II Annexes*, in *International Strategy for Disaster Reduction (ISDR)*. 2004, United Nations: New York and Geneva.
8. Liu, S.B., *Crisis Crowdsourcing Framework: Designing Strategic Configurations of Crowdsourcing for the Emergency Management Domain*. *Comput. Supported Coop. Work*, 2014. **23**(4-6): p. 389-443.
9. Liza, P., *Sociotechnical Uses of Social Web Tools During Disasters*, in *Knowledge Development and Social Change through Technology: Emerging Studies*, C. Elayne, Editor. 2011, IGI Global: Hershey, PA, USA. p. 97-108.
10. Tapia, A.H. and K. Moore, *Good Enough is Good Enough: Overcoming Disaster Response Organizations' Slow Social Media Data Adoption*. *Comput. Supported Coop. Work*, 2014. **23**(4-6): p. 483-512.
11. Lindsay, B.R., *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations*, in *Congressional Research Service*, C.R.f. Congress, Editor. 2011.
12. Avizienis, A., et al., *Basic Concepts and Taxonomy of Dependable and Secure Computing*. *IEEE Trans. Dependable Secur. Comput.*, 2004. **1**(1): p. 11-33.
13. Liu, P. and A. Chetal, *Trust-based secure information sharing between federal government agencies*. *Journal of the American Society for Information Science and Technology*, 2005. **56**(3): p. 283-298.
14. Schwartz, P.M. and D.J. Solove, *Pii problem: Privacy and a new concept of personally identifiable information*, *the NYUL Rev.*, 2011. **86**: p. 1814.
15. Herrmann, D.S., *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*. 2007: Auerbach Publications. 848.
16. Jansen, W., *Directions in security metrics research*. 2010: Diane Publishing.

17. Jaquith, A., *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. 2007: Addison-Wesley Professional.
18. Fernandez, E.B. *A Methodology for Secure Software Design*. in *Conference on Software Engineering Research and Practice (SERP'04)*. 2004.
19. Cavoukian, A., *Privacy by design: The 7 foundational principles. implementation and mapping of fair information practices*. en ligne: <https://www.privacyassociation.org/media/presentations/11Summit/RealitiesHO1.pdf>, 2006.
20. Pflieger, S.L., *Security measurement steps, missteps, and next steps*. IEEE Security and Privacy, 2012. **10**(4): p. 5-9.
21. Ushahidi. Available from: <https://www.ushahidi.com/>
22. Google. Available from: <https://www.google.org/crisisresponse/>
23. FEMA. Available from: <https://play.google.com/store/apps/details?id=gov.fema.mobile.android> .
24. NSW. Available from: <http://www.rfs.nsw.gov.au/about-us/our-districts/mia/fire-information/fires-near-me>
25. Quakewatch. Available from: <https://itunes.apple.com/app/disaster-alert-pacific-disaster/id381289235?mt=8> .
26. EarthquakeBuddh. Available from: <https://www.techinasia.com/earthquake-buddy-alert-location>
27. DisasterAlert. Available from: <http://www.pdc.org/solutions/tools/disaster-alert-app/>
28. WikiForProfessionals. Available from: [http://www.crisiscommunication.fi/wiki/Main\\_Page](http://www.crisiscommunication.fi/wiki/Main_Page).
29. Emergency2.0. Available from: [http://emergency20wiki.org/wiki/index.php/Main\\_Page](http://emergency20wiki.org/wiki/index.php/Main_Page)
30. PEP. *Public Empowerment Policies for Crisis Management*. 2016; Available from: <https://agoracenter.jyu.fi/projects/pep>.
31. Bharosa, N., J. Lee, and M. Janssen, *Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises*. Information Systems Frontiers, 2010. **12**(1): p. 49-65.
32. Turner, M., et al., *Does the technology acceptance model predict actual use? A systematic literature review*. Information and Software Technology, 2010. **52**(5): p. 463-479.
33. Lee, J., et al., *Group value and intention to use — A study of multi-agency disaster management information systems for public safety*. Decision Support Systems, 2011. **50**(2): p. 404-414.
34. Aedo, I., et al., *End-user oriented strategies to facilitate multi-organizational adoption of emergency management information systems*. Information Processing & Management, 2010. **46**(1): p. 11-21.
35. Cha, J., *Usage of video sharing websites: Drivers and barriers*. Telematics and Informatics, 2014. **31**(1): p. 16-26.
36. Cottrill, C.D. and P. “Vonu” Thakuriah, *Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making*. Transportation Research Part C: Emerging Technologies, 2015. **56**: p. 132-148.
37. Stolfo, S., S.M. Bellovin, and D. Evans, *Measuring security*. IEEE Security & Privacy, 2011(3): p. 60-65.
38. Pekárek, M. and S. Pötzsch, *A comparison of privacy issues in collaborative workspaces and social networks*. Identity in the Information Society, 2009. **2**(1): p. 81-93.
39. Hull, G., H.R. Lipford, and C. Latulipe, *Contextual gaps: privacy issues on Facebook*. Ethics and Inf. Technol., 2011. **13**(4): p. 289-302.
40. Solove, D.J., *Introduction: Privacy self-management and the consent dilemma*. Harv. L. Rev., 2012. **126**: p. 1880.

41. Twitter. *Best practices for using Twitter in times of crisis*. 2016 [cited 2016 March, 15]; Available from: <https://about.twitter.com/products/alerts/helpful-assets>.
42. Wikileaks. Available from: <http://www.wikileaks.com/>