Managing Visibility and Validity of Distress Calls with an Ad-Hoc SOS System

ALEXANDER BODEN, Fraunhofer FIT
AMRO AL-AKKAD, Fraunhofer FIT
MICHAEL LIEGL, University of Hamburg
MONIKA BUSCHER, University of Lancaster
MARTIN STEIN, Fraunhofer FIT
DAVID RANDALL, University of Siegen
VOLKER WULF, University of Siegen

The availability of ICT services can be severely disrupted in the aftermath of disasters. Ad hoc assemblages of communication technology have the potential to bridge such breakdowns. This paper investigates the use of an ad-hoc system for sending SOS signals in a large-scale exercise that simulated a terrorist attack. In this context, we found that the sensitivity that was introduced by the adversarial nature of the situation posed unexpected challenges for our approach, as giving away one's location in the immediate danger of a terrorist attack became an issue both for first responders as well as affected people in the area. We show how practices of calling for help and reacting to help calls can be affected by such a system and affect the management of the visibility and validity of SOS calls, implying a need for further negotiation in situations where communication is sensitive and technically restrained.

Categories and Subject Descriptors:

- **Human-centered computing: Empirical studies in collaborative and social computing**
- Human-centered computing: Empirical studies in HCI
- Human-centered computing: Empirical studies in ubiquitous and mobile computing

General Terms: Participatory Design

Additional Key Words and Phrases: SOS calls, Visibility, Validity, Emergency Response, Mobile computing

ACM Reference Format:

Alexander Boden, Amro Al-Akkad, Michael Liegl, Monika Buscher, Martin Stein, David Randall, and Volker Wulf, 2016. Managing Visibility and Validity of Distress Calls with an Ad-Hoc SOS System. *ACM Transactions On Human Computer Interaction* 9, 4, Article 39 (March 2016), 27 pages. DOI:http://dx.doi.org/10.1145/0000000.0000000

This research has been partially funded by the EU as part of the BRIDGE project (FP7SEC-2010-1) under grant agreement n°261817.

Author's addresses: A. Boden, A. Al-Akkad, and M. Stein, Fraunhofer Institute for Applied Information Technology FIT, Schloss Birlinghoven, Sankt Augustin, Germany; M. Liegl, Sociology Department, Hamburg University, Hamburg, Germany; M. Buscher, Centre for Mobilities Research, Lancaster University, UK; D. Randall and V. Wulf, Information Systems and New Media, University of Siegen, Siegen, Germany.

DOI:http://dx.doi.org/10.1145/0000000.0000000

1 INTRODUCTION

Research into technological support in disaster and other emergency situations has become increasingly common. One aspect of this burgeoning research agenda has been investigation into the role that mobile devices might play. However, the availability of networks is a recognized problem in such situations. It can take hours, sometimes weeks, in the aftermath of a disaster for the mobile network to be fully restored (Al-Akkad et al., 2013; Jennex, 2012; Palen and Liu, 2007; Sutton, 2012), leaving people in what has been termed an information vacuum (Sutton, 2012).

Some studies have focused specifically on the use of remnants of technology in the aftermath of disasters. For example, researchers have analyzed how people leverage information and communication technology (ICT) in war zones (Mark & Semaan 2008; Mark et al. 2009; Semaan & Mark 2011). Other studies have investigated how people re-appropriate discarded resources, such as, for instance, a power generator in response to a large-scale outage caused by a hurricane (Palen et al., 2010b).

In response to the challenge of dealing with disrupted infrastructures, novel systems for emergency communication attempt to leverage alternative communication interfaces (such as Bluetooth or Wi Fi radio functionality) to facilitate the construction of ad hoc communication links. As people "repurpose, reconfigure, or combine surviving portions of pre-existing technology, adopt discarded resources, or share access to still working ICT services" (Al-Akkad et al., 2013), new forms of network infrastructure are created, which reconnect people and allow them to send and/or receive up to date information. However, the design of technologies for emergency response needs to be particularly sensitive to the complex contexts in which they are to be used (French and Niculae, 2005). Safe use requires new attitudes, regulations and tools that help people involved in, or affected by, an emergency to assess which data sources are trustworthy and which are not (Palen et al., 2010b). Also, in the light of a continuous stream of emerging technologies, a continuous assessment is needed in order to understand which systems are appropriate for which information (Reuter et al., 2012). Constraints may arise not only in relation to the available technological infrastructures, e.g. in terms of what devices are needed to form ad hoc networks, but also with a view to the ethical implications of such technology in emergency situations. Many post-disaster reviews find that there are serious shortcomings in the ability of the diverse actors involved to collaborate and coordinate their efforts. Studies of how systems are deployed in the wild, then, can help to shed light on contingencies and consequences of novel technologies, and allow us to better understand design implications as well as in-situ aspects of technology appropriation.

In this paper, we study the use of an ad-hoc SOS system for smartphones in the context of a large-scale "terrorist attack" scenario. The aim is to further our understanding of how technology can support those who need to call for help in emergency situations, and how systems supporting SOS calls interact with the practices of professional emergency responders. The scenario in question was chosen because of the dangers of giving away one's position in adversarial situations such as an ongoing terrorist attack.[1]

Our research is part of a long term iterative participatory design process with professional practitioners, deploying an enhanced prototype of a system that we have developed (Al-Akkad et al., 2014b), which creates short-lived ad-hoc networks between neighboring devices. It allows people in disaster situations to broadcast a distress

[1] This scenario was purposely designed to echo, in some respects, the awful events of July, 2011 on the island of Utøya in Norway (cf. https://en.wikipedia.org/wiki/2011_Norway_attacks).

signal that can be picked up by rescue workers. Moreover, rescue workers may acquire further information, such as the GPS location of the sender. In a series of workshops and experimental implementations during emergency response training exercises, the system was increasingly realistically integrated into practices of responding to different emergencies including a fire in a train in a tunnel and a car accident. The details of the technical development of the system as well as a mainly technical evaluation have been published elsewhere (Al-Akkad et al., 2014b). This paper takes a step forward by exploring how the system was used by first responders and students acting as victims during a large-scale emergency exercise in Norway, and reflecting these experiences against our design rationale as well as the literature on crisis response. During the exercise, our system was used by a special unit of the police who were searching for persons at the site of the incident. After the exercise, we conducted interviews with a police officer and three students who acted as affected people during the exercise. We further evaluated the concept in a workshop with practitioners for crisis management.

Our study shows that two aspects are particularly important to make ad-hoc communication systems useful in adversarial situations where communication is restricted to peer to peer channels and especially sensitive to interception and misuse. Firstly, it must be possible to assess the validity of the distress calls in terms of their content. Can the calls for help be trusted? For a police unit, key questions are whether the information related to this call is truthful (i.e. not a hoax or, worse, a trap) and whether it is accurate, as the person's position may become obsolete. Secondly, there are issues around the (in-) visibility of the system's operation in terms of who is able to detect distress calls. For the people sending the distress signals, key questions are "has my call been heard?" and "by whom?" Based on an analysis of our findings, we explore implications for an enhanced design of mobile SOS systems, highlighting novel aspects that are relevant for researchers working in the field of designing support systems for emergency response.

2 RELATED WORK

Information and Communication Technologies (ICT) are bringing new kinds of transformation. A process of 'informationalising' (cf. Liegl et al. 2016) crisis response and management is currently underway, following in the footsteps of similar developments in other industries and services. In the following sections, we provide an overview on related work from designing mobile applications for communication in emergency situations, as well as on SOS calls.

2.1 Supporting Communication in Emergency Situations

People increasingly rely on technology in their daily routine, but having access to ICT services can also be crucial in disaster situations, when it is important to receive and send up to date information (Coyle and Meier, 2009; Palen and Liu, 2007). For instance, the Federal Emergency Management Agency (FEMA) provides an application (http://1.usa.gov/P8V5sf) that enables people in distress to receive shelter information and also to submit images with a short description to the FEMA website, which will be placed on a map for public viewing. Another system, SafeCity (http://www.safecity.nl), allows the reception of live video streams from mobile devices reporting crimes or other distress situations. Professional responders use a dedicated application to stream video along with their GPS position to the command center or to other colleagues in the field. Users can install a free application called Bambuser (http://www.bambuser.com), which enables them to view and stream live video. In order to report any video to authorities, users need to register for specific “shares”, such as “Crime stoppers” or “Public Officials”. All these existing emergency response systems represent promising tools for communication between the public and authorities or non-governmental organizations during a crisis. However, to be of use, any of these systems require the network infrastructure to be still operable. At the same time, the reality is that availability of ICT services can be severely disrupted in the aftermath of disasters; that is, in the very moment when people rely most on communication technology to report their emergency needs (Reuter, 2013). These disruptions can result from damage to, or congestion in, the preexisting network structure, or large-scale outages.

Several systems have been developed that attempt to leverage ad-hoc communication links for enabling users to exchange emergency messages in situations where the existing communication infrastructure has stopped functioning, for instance NowForce (http://www.nowforce.com), Zello (http://www.zello.com), Twimight (Hossmann et al., 2011) or OpenGarden (Iosifidis et al., 2014), to name just a few. Our approach goes into a similar direction, enabling users to broadcast messages via Wi-Fi. The particular scope of the technology developed is to address disaster situations in which people can no longer communicate via everyday services, such as phone calls, texting services, messengers or social media, because the underlying network infrastructure is disrupted. In such situations, people look for any method of connectivity in order to regain their ability to communicate and retrieve information about ongoing events during and in the aftermath of a disaster.

We have provided an extensive review of such existing systems in our previous work (Al-Akkad et al., 2014b). Summarizing, one can say that existing systems are often hard to deploy because they either require difficult pairing mechanisms (often based on Bluetooth) or special hardware / software configurations (such as rooted devices or availability of networking standards such as WiFi Direct that are not yet established) that makes it impossible to deploy them on standard hardware, strongly limiting their practicality. We therefore wanted to create a system that overcomes these limitations, allowing people to send SOS messages in situations where the network infrastructure has failed, and one that is both easy to use and runs on off-the-shelf devices as well.

The concept of our SOS system was inspired by how people make use of the names of Wi-Fi home networks (SSIDs) to broadcast short messages conveying simple, anonymous information. For instance, some SSIDs may express neighbourly requests, such as “Turn the noise down” or political ideas as “ILoVeObAma!!”(Al-Akkad et al., 2014b). A Wi-Fi network is visible within a certain range and the advertised SSID is usually the first thing people become aware of in terms of wireless networks. Essentially, people can easily find and understand SSID names. They represent an interesting point of contact between people. The creation of an emergency beacon defines a sort of “Help me” signal, which may help professional first responders to find persons (see Figure 1). As default settings in smartphones notify users of the presence of detected networks, any person in vicinity searching for connectivity with a smartphone may discover the emergency signal.

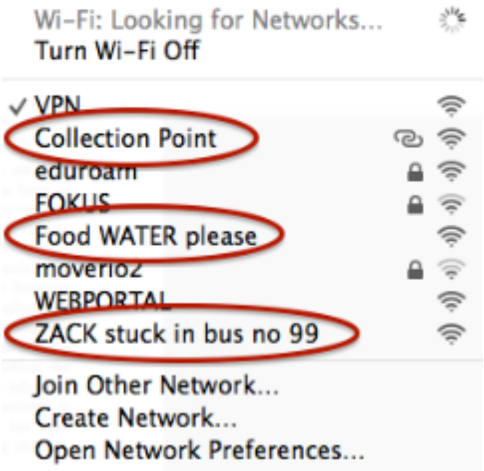

Figure 1: Example of how Wi-Fi SSIDs can be exploited to convey short messages (screenshot, not part of our prototype)

Our system enables people in distress to use their phones to communicate their situation in the form of an ad-hoc emergency signal that can be received by professional first responders, helping them to find both persons in difficulty and respective danger zones in disaster situations. To do so, the system leverages established wireless network protocols and standards to create ad-hoc communication links between wireless devices in proximity. One device, called the "Beacon", advertises an emergency message inside the SSID, i.e. the human readable name of a Wi-Fi network. In turn, another device, called the "Seeker", scans the environment for devices that advertise themselves as Beacons and instantiates brief connections to those in order to confirm to each Beacon that it has been discovered. In cases where connectivity is strong enough, both Beacon and Seeker exchange further information that exceeds the 32 ASCII characters constraint of the SSID, such as the person's location or the unique ID of a phone (shortly IMEI). The functionality of the system will be presented in more detail in section 4.2.

2.2 Conceptual Approaches Towards SOS Calls

Previous work in HCI (e.g. Starbird et al., 2010, Starbird and Palen, 2011; Ludwig et al., 2013; Reuter et al., 2012) as well as from practitioner-driven organizations such as EENA (http://www.eena.org) has investigated socio-technical issues around the enhancement of SOS calls by means of ICT (e.g. Bornheim and Fletcher, 2016) as well as the organizational and collaborative aspects of emergency response work. Within HCI, the literature on SOS calls has been based, to a substantial degree, on conversation analysis, a mode of sociological inquiry that proceeds through detailed study of talk and interaction. Most studies are concerned with the dialogic nature of calling for help and the challenge of the co-construction of meaning between caller and responder. Issues that have been discussed include problems responders face in retrieving information about the location (where?) and the nature (what?) of the incident (Baker et al., 2005), managing information overload and misunderstandings, partly due to the anxious state of the caller (Cromdal et al., 2008; Whalen and Zimmerman, 1998), the identification of hoax calls, and whether or not to initiate dispatch (Bergmann, 1993; Garcia and Parmer, 1999; Whalen and Zimmerman, 1990), difficulty in defining a proper form of response based on the information provided by the caller, i.e. negotiating the problem of initiating dispatch too early (not enough information), waiting too long, or sending the wrong kinds of resource (Larsen, 2013; Paoletti, 2009; Whalen and Zimmerman, 1990).

Further aspects discussed in this literature are the implications of the technical communication infrastructure used for the organization and the sense making processes inherent in these calls. The affordances of landline telephones and general emergency call numbers such as 911 (US) or 112 (Germany), for example, have an impact on the structure of the call in terms of what information has to be provided or what can be assumed. Callers calling from landlines, for example, may be unable to see the scene, while mobile phone calls can potentially come directly from the incident scene. Mobile phone callers often do not know the exact address of where they are, hence cannot always provide accurate instructions on the destination of the dispatch. At the same time mobile phones enable emergency services to enlist the caller into giving more detailed and live observations of the incident, helping them for instance to establish the number and condition of affected people in the vicinity, to give a clearer impression of the scale of the incident and the amount and kind of resources to dispatch (Krishnamoorthy and Agrawala, 2012). While this may allow to better calibrate the response it does take additional time, and it can recruit the caller who previously often was merely a messenger, into the situation as an "auxiliary member" of the emergency services. Moreover, it might make civilians of one kind or another early responders as denoted by Palen, Anderson et al. (2010), as such people are often acting on the basis of knowledge which is for the time being not available to emergency response authorities (Stallings & Quarantelli, 1985; Aguirre et al., 1995; Kendra & Wachtendorf, 2006).

In comparison with classic SOS calls (landline to landline), but also mobile emergency calls (mobile caller), our approach has some striking differences:

1. Messages are likely to reach professional responders only after they have been dispatched and are thus subsequent to distress calls with emergency call center operators. They may reach informal first responders, such as other people affected by the events or people in the vicinity, sooner.
2. The system affords new immediacy—a direct, local form of communication which is not characterized as a "conversation", but as a broadcast of a distress signal phrased as a statement that the sender makes about the situation at hand, i.e. it misses (or there is no need for) the co-construction of information about the incident found in distress calls to the call center.
3. We shift the focus from the classic "dispatch center" to mobile responders who are already in the field and able to pick up SOS calls similar to hearing someone calling for help vocally, implying a more direct mode of interaction between professional first responders and people in the area of a disaster (although by relaying identified Beacons to the dispatch center, the incident command can direct first responders to areas with overlooked persons).
4. We augment the distress call with additional information such as location data, shifting the mode of delivery from description to a form of auto-address through geo-coordinates, which could free time for further contextual information to be exchanged.

The immediacy of the communication resonates with emerging practices around the increasing use of social media for the assessment of emergency situations (Abel et al., 2012; Ludwig et al., 2015), which seek to enable real-time analysis of, for instance, Tweets from disaster areas. Here, issues of determining the accuracy or quality and accessibility of information have been found to be critical (Linna Li, 2010; Palen et al., 2010b). To some degree, our system has similar features to social media, but with a much more local focus and a smaller scope in comparison.

Social media are also known to play an important part in the second theme we mention, that is, cooperation between first responders and the public in order to deal with the contingent needs created by a disaster, which is commonly understood as informal response (Hagar and Haythornthwaite, 2005; Palen et al., 2010a). On the one hand, a bidirectional flow of information between formal and informal responders can be an important resource for first responders in organizing relief efforts (O'Keefe, 2009); on the other hand, it empowers people that are affected by a disaster to help themselves, challenging the notion of "victims" to some extent (Perng et al., 2013).

In respect of the way in which SOS calls provide additional information automatically, the system delegates the broadcast of information to location aware sensing systems. Metadata have been found to play an important role for the assessment of information retrieved by social media (Chorley et al., 2015). In emergencies, this renders affected people more visible and facilitates visualization on a map via location sharing (Gordon and Silva, 2011; Wu et al., 2013). Location sharing technologies have become popular, but also contested in social networks such as Facebook or Foursquare over recent years, because they allow people to stay in touch and monitor the location of friends, to engage in location sensitive mobile gaming (Gordon and Silva, 2011; Licoppe, 2004) and more recently location sensitive dating, where people willing to date or hook up make themselves discoverable and addressable by (nearby) location (Liegl and Stempfhuber, 2014, Beale, 2005; Birnholtz et al., 2014; Blackwell et al., 2014). While this kind of technology was already recognized and welcomed in the early 2000s (Rheingold, 2007), others exploited the concept of co-presence, understood as two or more people being in proximity (nearby) at a given time for meeting applications (Müller et al., 2013) that provide new and improved opportunities for urban, social interaction (Paulos and Goodman, 2004; Sutko and Silva, 2011). Other approaches make use of proximity-based affordances to enable exploration (Hornecker et al., 2011) or gaming (Falk et al., 2001) (e.g. Ingress by Google where local teams cooperatively solve tasks, or the more recent location-based game Pokémon GO). Most of these approaches have in common that they try to create awareness about opportunities nearby and, due to that opportunistic nature, are mostly concerned with providing more comfortable or localized services.

The changes that we have outlined above have the potential to enhance, but also to challenge and disrupt, the practices of professional first responders and people in disaster situations. In order to better understand the possible contingencies and consequences of deploying technology in practice we have set up an empirical study that will be presented and discussed in the following sections. Our point in so doing is twofold: Firstly, situated evaluations of this kind get much closer to real-world conditions, which are important yet extremely hard to study (cf. Turoff, 2002). Secondly, although disasters and emergencies may have some generic features, we also need to understand what is specific to a given situation, if new technology is to become widely adopted in such circumstances. In our scenario, where the threat comes from other people, there is a need to understand how to constrain the availability of communications.

3 APPROACH AND PROTOTYPE

Our study has been part of a large European research project that strives to support professional responders and members of the public by providing means for ad-hoc communication for situations in which existing network infrastructure is disrupted. In situations of disrupted infrastructure, finding trapped or hiding persons is one important need for first responders. This study builds on prior fieldwork (Al-Akkad et al., 2014b, 2013) in which we have evaluated our system during an emergency response exercise that took place in an underground tunnel fire scenario. In this previous work, we have focused on performing a mainly technical evaluation of how our prototype performed in a burning tunnel, a challenging physical environment for our technology. The field test was supplemented with interviews where we investigated how the practitioners, in this case the fire fighters that were dispatched, dealt with the emergency. We will summarize the findings of this scenario in the discussion section, comparing it with this study in order to draw out some of the specificities we mention above.

3.1 Methodology

In the context we design for, it is crucial to explore the feasibility and applicability of technology in close-to-real emergency or disaster conditions. Therefore, we tried to explore the viability of core features of our system in an early stage of development (Edwards et al., 2003). For instance, in our previous study (Al-Akkad et al., 2014b), we first conducted a feasibility study of an initial version of our prototype (TRL 4/5) in an underground tunnel in which communication was rather difficult or intermittent due to the high amount of steel and curves. We identified constraints in terms of implementation and revised our prototype, and then were able to evaluate it in the context of an emergency exercise that was organized in the same underground tunnel. As our system is in a more mature stage by now (TRL 6), we are engaging in ongoing evaluations with the technology in increasingly realistic emergency exercises in order to get a better understanding of how our solution is used in practice (Wulf et al., 2011).

From an organizational perspective the goal of introducing a system such as ours should be to enhance and support established practices of emergency response. Emergency response is a domain with rigid structures (Denef et al., 2011) and a need for a combination of agility and discipline (Harrald, 2006). This creates a dynamic ecology for the design and implementation of new technologies. Hence, we continuously evaluate our design through various qualitative research methods: participant observation, one-to-one interviews, workshops, and real world exercises. The participants of our evaluations are practitioners of emergency response ranging from fire fighters, police officers, paramedics, reconstruction engineers, to experts and consultants for crisis management (cf. Liegl et al., 2016).

Besides practitioners in emergency response teams, our methodology also involves people in distress as the other group of end-users, which in the following we will refer to as affected people (as opposed to responders or practitioners). This avoids the problematic and misleading implications of the term “victim”. Not all people affected by disasters are victims, and even if they are, they may not be passively awaiting rescue by the professional responders. The image of passive victims runs counter to the intention of our SOS system and also to the empirical fact that people affected by disasters are in general more resilient, capable, active, altruistic and calm than assumed in popular imaginaries, circulating in the media but also amongst first responders (Mitchell et al., 2000; Dynes, 1995; Jul, 2007; Quarantelli and Dynes, 1972). For this reason, and despite the fact that the term “victim” is an established term in the emergency response domain and was frequently used by our practitioner research collaborators to describe the users of the SOS technology amongst people affected by an emergency in our empirical work, we decided against using it here.

It is important to note that collecting input from people affected by disasters is complex for both practical and ethical reasons. In order to explore the use of our technology from this perspective, we organized interviews and observations with students who volunteered to act as affected people in simulated scenarios and exercises, thus gathering feedback and identifying limitations of the current state of the technology. This is part of an iterative development process, helping us to continuously adapt our design and to address more properly the needs of both affected people as well as practitioners who participated in the exercise, in our case members of a special unit of the police.

After the exercise we conducted semi structured interviews with both groups of users, encouraging them to share any ideas or concerns that came up in their experience with using the technology. We interviewed the students on the day directly after the exercise; representatives from the police unit were interviewed on phone two weeks later. The interviews were conducted by two members of our research group who had also attended the exercise. We followed a loose guideline where the participants were asked to talk about their experiences during the exercise in general and especially their impressions of using our technology. The interviews were recorded with permission of the interviewees and transcribed with a focus on the contents of the conversation. We then performed a topic based qualitative content analysis of the transcripts as well as our field notes from the exercise with a focus on limitations of our prototype and lessons learned and especially on anything unexpected.

3.2 Prototype

Our system comprises two applications (see Figure 2). The first is an SOS application which enables its users to create an emergency beacon by placing short messages inside the SSID of a Wi-Fi network. The other application is the corresponding “Seeker” that supports professional first responders in discovery of the requesting Beacons. Both applications can be deployed on devices running Android (supported APIs range from 2.3.3 to 4.x). Android is the most widespread operating system for mobile devices and by supporting lower API versions the system can be installed on a wide range of devices. As soon as the SOS application is launched, it starts to broadcast a help message that users can pick from a pre-defined list or enter themselves (see left image in Figure 2).

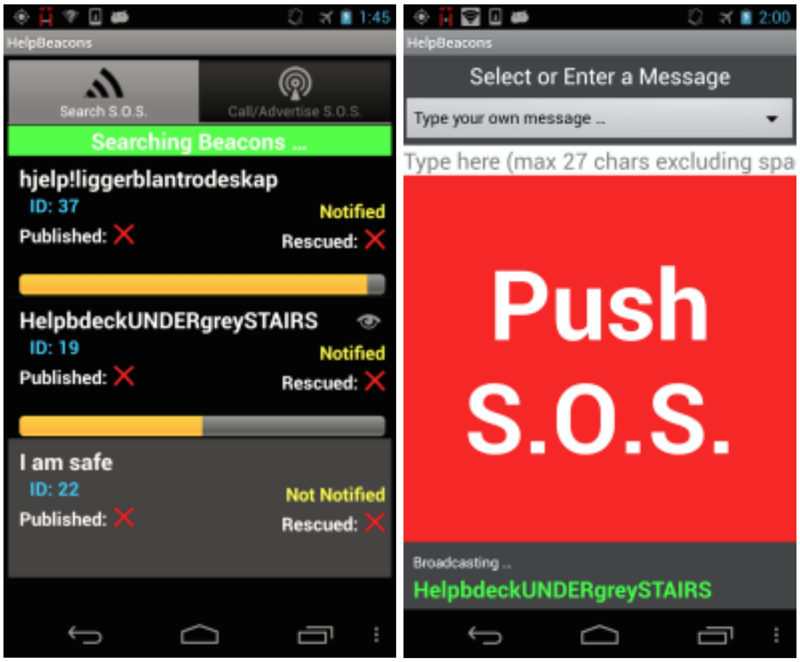

Figure 2: Application for responders (left) and application for affected people (right)

The Seeker (see right image in Figure 2) continuously searches the environment for Beacons and filters the scanned Wi-Fi networks based on an uncommon sequence of characters (*#%), which is put as a prefix inside the SSID of a Beacon device. When a Seeker connects to a Beacon the phone behind the Beacon plays a "beacon-like" sound and vibrates briefly. The audio-vibration feedback can help responders to locate affected people, depending on the kind of gear they are wearing and how the device is carried (e.g. in a pocket, with a strap around the neck, or in hand, Al-Akkad et al., 2014b).

When the SOS application is launched, but no locations services are activated yet, the application asks the user if s/he would like to enable location services. If the Beacon is not able to retrieve a GPS fix, the position of the Seeker is used instead, giving at least some rough indication. As indoor GPS is not available and moreover GPS modules embedded in smartphones only provide an accuracy of up to 10m, further means for positioning people are needed. Currently, the reception of a Wi-Fi signal implies that the mobile hotspot is within 60-200m range of the receiving device, depending on the environment as well as the strength and configuration of both phones' antennas.

Users can update their status messages at any time. In the case when a person wants to stop broadcasting an SOS signal (e.g. because they feel safe), users can select a specific entry (i.e. "I'm safe") from the list. Then, the application will place a specific suffix in the SSID of the signal that informs the Seeker that this Beacon should no longer be considered and marks them accordingly.

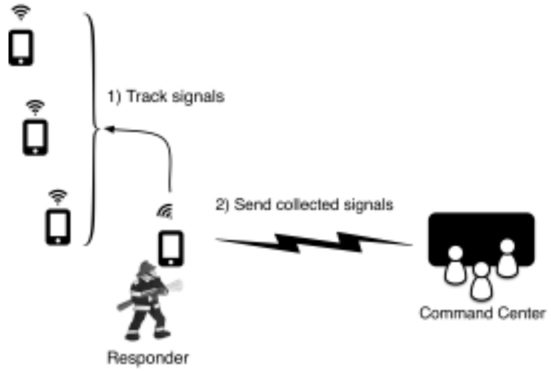

Figure 3: Integration with established emergency systems

The usefulness of the SOS system can be greatly extended when it is linked to other emergency response systems. Figure 3 depicts the big picture in which the presented system is operated in the frame of the research project, which develops infrastructural support for interoperability and the assembly of systems of systems. Within the broader system, the responder application that runs on the Seeker device sends the data acquired from Beacons to a command center using a mesh network, which routes the data to a publish-subscribe system that pushes the data to a command center. There, the personnel can view the Beacons on a map and use the data to coordinate response efforts. For instance, incident commanders may be able to roughly gauge progress in search and rescue efforts visually, as persons sending a Beacon are being found and deactivate their beacons.

4 FINDINGS

In this section we describe results from our ongoing evaluation of the prototype and the socio-technical innovations arising around it in the project. In particular, we will present findings from a field evaluation of our prototype in a real world exercise (sections 5.1 and 5.2). In the second part (Sections 5.3 and 5.4), we describe the feedback on our prototype received from students and a member of a special police unit. Finally, in section 5.5, we illustrate aspects raised in a workshop with a group of experts.

4.1 Real World Exercise Simulating a Terrorist Attack

We had the opportunity to participate in a large-scale exercise that took place at the port of a Norwegian city with a high concentration of industries for petrol and gas. The overall goal of the exercise was to train inter-agency collaboration between the three main response units (police, fire brigade, and ambulance). Planned in the aftermath of the 2011 Norway attacks (Perng et al., 2013) and in relation to local risks and the potential for man-made disasters in the industrial area at the port, the exercise simulated a scenario in which a group of armed criminals entered the area through the ferry port with the aim of attacking a chemical factory located next to it. The exercise scenario was labeled a terrorist attack. As the attackers proceeded through the ferry-boat and the ferry terminal, they shot, injured and killed a large number of people.

Figure 4 shows a layout of the incident site. After discussing with the exercise committee of the exercise, we chose the ferry as our main site for the evaluation of the SOS system. As users of our system, we chose a special police unit that would have to search for affected people and attackers on the area, and that would also enter the ferry at some point. The officers were introduced to our system a day before the exercise, but did not have any details about the planned exercise—neither the kind of incident, nor the area. Furthermore, the exercise committee allowed us to equip three students (V1, V2, and V3) on board of the ferry with smartphones. Before the exercise, the training exercise supervisors gave instructions to the students to act as affected passengers during the exercise, and to play their role as realistically as possible in the sense of doing what felt natural to them in such a situation.

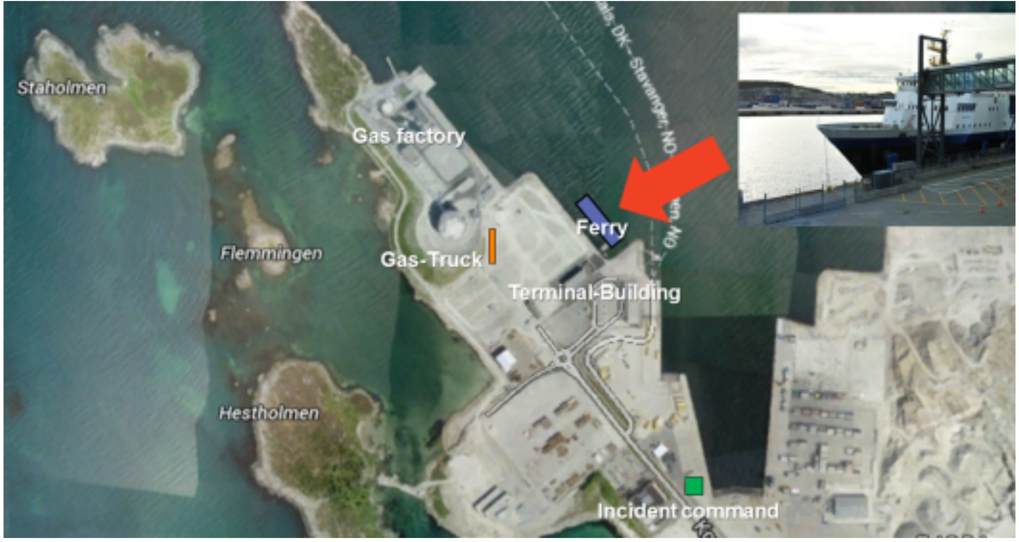

Figure 4: Disaster zone of the large-scale exercise

To explore how the amount of steel inside the ferry might weaken the signals and impact the functionality of our technology, we conducted several test runs on the ferry a few days before the large-scale exercise took place. Figure 5 shows one researcher searching for signals and V1 hiding behind the door of one cabin. In the beginning, the students kept the sound feature of the SOS application turned on, making it quite easy to locate them. Then, the students switched the sound off, reasoning that it could also make the attackers in the exercise aware of their location and put them in danger. As the ferry was a quite familiar place for the students, they found hiding places quite easily and we had great difficulties to locate them when receiving no additional information. GPS would not work inside the ferry. Thus, acting from necessity one researcher looked into the Android Wi-Fi settings, which indicate the signal strength for each detected Wi-Fi network, and in this way could help to locate the hiding students.

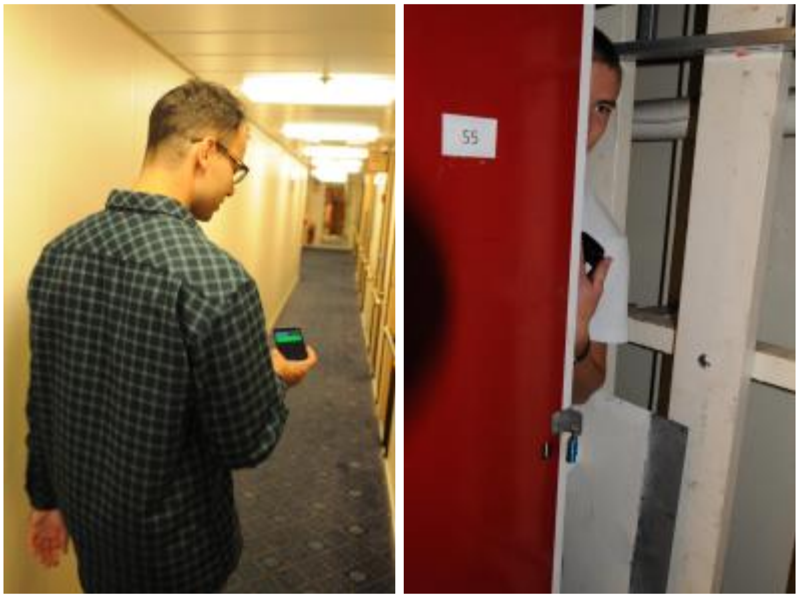

Figure 5: Search for signals and V1 hiding in a cabin

The responder application was enhanced to display the signal strength (see above Figure 2 yellow bar of first two entries in the responder application). The orange scale depicted in the responder application depicts the signal strength of the tracked Beacons. This signal strength bar shows the received signal more precisely than the Android Wi-Fi settings, which only highlights or shades the four semicircles of the Wi-Fi logo. The responder application maps the received signal to a scale from 1 to 20, whereby 20 is the highest value. It provides a finer granularity. When no signal is received for a Beacon, the signal strength bar disappears from the user interface.

Having enhanced the system with some means for indoor localization, our system was ready to be deployed in the large-scale exercise. We left five smartphones with the three students—two additional ones as backup—to be used during the exercise, and we met with them one day after the exercise to discuss their experience of the system and conduct semi-structured interviews.

4.2 Overall Response Operation

The SOS systems played a small but significant role in the overall response operation. The responder application in Figure 2 depicts distress signals that were configured by the three affected people during the exercise and the Seeker phone that discovered those signals.

Figure 6: Special police unit entering the ferry

At an early point during the exercise a special police unit was formed ‘on the hoof’(see Figure 6), which entered the ferry, following a report that at least one terrorist had been seen on the ferry. This special police unit discovered V1, who was hiding on the deck in the back of the cabins, without the help of our technology.

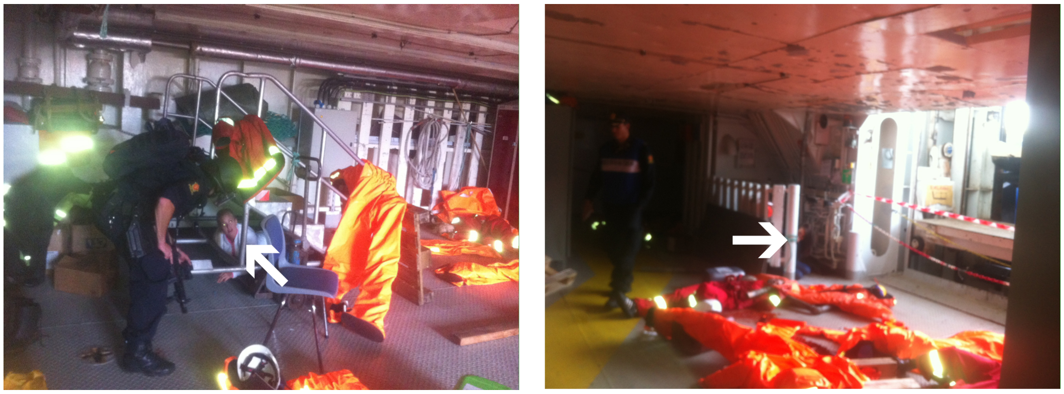

Figure 7: V2 hiding under stairs (top) and V3 behind a barrier (bottom).

The remaining two affected persons hiding from the attackers (V2 and V3 in Figure 7) were later discovered using our system with the responder application “sniffing” for the presence of Beacons. One user device was able to retrieve a GPS fix. The two other Beacons were mapped to the GPS position of the responder device at the time it discovered these two Beacons. The data from Beacons were forwarded to an operational control room where their locations were visualized on map by means of their (precise or approximated) GPS positions.

4.3 Feedback from the Students

Overall, the students reported that they experienced the exercise itself as highly realistic. Even though they knew everything was just a simulation, they had to wait for a long time in their hideouts until the police units found them. In this regard, the general possibility of having access to an SOS system was very positive for them, as it made them feel less alone in the situation. At the same time, they had a mixed experience of the system, as it became clear to us in the following interviews. For instance, V2 pointed out that the SOS application could be misused to play a joke on the emergency personnel. Aligned to this, V3 explained that initially—after playing "hide and seek"—she liked the idea of leveraging the ubiquity of Wi-Fi SSIDs to convey emergency needs. However, she then realized that that very ubiquity could spell danger and became concerned that the attackers would detect her messages, too:

> V3: If I had run wild in the woods the app would be great, but it is not good in case of a terroristic attack.

This was also a more general concern mentioned by all three students. The dissemination of data to untrusted people was seen as a flaw. Their desire would be that only the police or trusted response units would be able to pick up their messages in such kinds of emergency scenarios. Also, V3 pointed out that she would like the Seeker device to connect to her phone, when she set up her status to "safe" in order to know that the personnel in the field and in the control room had become aware of her new state. At the same time, the students would have liked to have some kind of feedback about the status of the rescue operations.

With regard to the distribution of the application, both V1 and V2 could imagine obtaining the application in a decentralized way (Al-Akkad et al., 2014a), in case Internet connection was disrupted. Even so, they would prefer to have the application preinstalled.

> V1: I propose to have it shipped in every phone, already when you buy it.

Not least, V2 expressed the difficulty of designing interactions for each context.

> V2: The area was dark; when I was using the app it would light up the area. So if the terrorists were near they would see the light.

Other aspects that were mentioned by the interviewees related to the limited size of the messages that would require some creativity and may be too limited in more complex situations. Another proposal made by V2 was to take pictures and add keywords and then send this data out when exchanging details between the Beacon and the Seeker device.

4.4 Feedback from Members of Special Police Unit

During the exercise, a special unit of the police was deployed to look for terrorists and affected people. At some point this team entered the ferry accompanied by one of the authors who was able to observe the rescue mission and assist in the handling of the Seeker device. Two weeks after the exercise, we organized a semi-structured interview with one police officers of the special unit who interacted with our system while being assisted from one of the authors.

The police officer (PO) explained that their main mission was to chase the terrorists, and at the same time take care of the health personnel entering safe areas in order to do their job. PO explained that during the operation his team and he experienced a lot of problems with the radio, i.e. the walkie-talkie system used by the police. This hampered the communication between response personnel in the field and the incident commander. Initially, the special police unit did not go on the ferry as some smoke was coming out. Though, after several unsuccessful attempts to contact the fire brigade the special police unit decided to go onto the ferry despite the absence of any "green light" confirmed by the fire brigade.

> PO: After a while we tried to get hold to somebody of the fire department, because we wanted to be told what kind of smoke is coming from the boat before we went in. So, we have the correct

> equipment immediately to go in. We waited like 5-10 minutes, which felt in this situation like years. Finally we couldn't wait anymore, and as we understood there are problems with the radio, we went in to the boat. It was our own decision, as we saw the smoke decreasing, we saw our chance to get inside the ferry.

As the radio was not working, the leader standing outside near to the ferry could not instruct them, as he would have liked to. In response to this, for example, the special police unit tried to go for sounds and also talking to affected people or other witnesses who had seen any of the terrorists.

At the same time the PO made clear that locating people was not the highest priority in the beginning of their mission, but later in the progress of the operation it became more important.

> PO: First of all we had to locate the terrorist to avoid any further harm. That was a big challenge, as while we were searching for the terrorists, we encountered a lot of injured and shocked people.

Further, the PO made clear that during the beginning of a mission he and his colleagues normally have their hands full and cannot use additional devices such as our Seeker device.

> PO: I had my private phone with me but I didn't use it. Our mission does not allow us to use phones [...] but if things calm down we might have one hand free.

However, the practitioners acknowledged that the leader of the operation could maybe handle the device.

> PO: The leader should not use both hands for weapons. So he has one hand free, which he could work with more than one device and provide information to us and to the other members outside.

At the same time, the PO said that our technology could also be useful for supporting the communication between the police officers in case the radio is not working, as it happened during the exercise.

> PO: Good backup plan if the radio is not working, so we could listen whatever is going on from our commanders [...] that could go through our personal phone.

Reflecting on the question if it would be dangerous for affected people to advertise their help messages via a Wi-Fi SSID names, the PO had some concerns that the messages could be picked up by terrorists.

> PO: I mostly agree that terrorists would get this information as well [...] people send information to police that they need help and where they are [...] it might be possible to check out who is sending the message [...] depending on how many people are there.

When we discussed with the PO the possibility of reverting the setup, i.e. a responder would broadcast a signal that affected people could track by their phones, the PO agreed that it might be a preferable option in comparison to the current setup:

> PO: Maybe it is better that we, as the police, send out the signal in order to help the people around us and tell them where they can meet us. If in worst case the terrorists can see us, we are somehow ready to cope with them as well. Maybe we have a description of them. Instead of the terrorist can sort of see where victims are hiding [...] I think it

> would be very interesting to try out the other way around, I guess this could be helpful.

4.5 Workshop with Domain Experts

In addition to evaluating our system as part of the exercise, we organized a workshop with five practitioners for crisis management who were invited to attend the exercise as observers:

- A head of the ambulance service (AS),
- An officer of a European federal police (FP),
- An inspector at a police college (PC),
- A head of division for civil protection (CP), and
- An industrial manufacturer (IM).

The workshop was organized on the day before the exercise and took place on the same site during the preparations. First, the practitioners were briefed on the plans for the exercise. Then, we had the opportunity to present our technology against this background, and discuss with them how it would be used during the day of the exercise. The workshop mainly consisted of presentations and group discussions, which were audio recorded for later analysis, but the participants also had the opportunity to attend the preparations of the exercise and see demonstrations of our prototypes. The overall goal of the workshop was to receive multiple high-level perspectives from different crisis stakeholders on the applicability and possible implications of using our system in the emergency response domain, also sensitizing us for the field work on the following day.

At first the practitioners confirmed the trend towards equipping field personnel with wireless devices as smartphones or tablet computers. Then, the head of civil protection (CP) made the request to investigate into possibilities to use voice channels in order to confirm to people that their signal has been picked up. He critically pointed out the practice of receiving a text-based confirmation without talking to personnel.

> CP: This would frustrate people. It's like receiving a number when you are waiting in the queue of a hotline, where you know it will take time to talk to somebody [...] I suggest to enhance your system for the possibility of sending short voice messages.

We also confronted the practitioners regarding an inverted setup. In this context, the police college inspector (PC) voiced concerns about the possibility of a terrorist obtaining a responder device and stressed that this would present a risk.

> PC: "Let's say you secure the device the responder is supposed to carry [...] I am afraid that people would still be able to hack it and gain access. Then, your system would become even counter productive."

The federal police officer (FP) supported this by giving an example of a sniper in Norway who called the police pretending to be asking for help, thus setting up a trap in which two police officers were fatally injured. In response, the head of civil protection (CP) made a suggestion to use an inverted setup of our system.

> CP: Responders who carry devices that broadcast a sort of "we are in here and we are trying to get through to you". I guess that makes more sense. It is similar to current practices of fire fighters […] when responders enter a house they talk to the persons inside the house in order to get relevant information from the people.

There were also other ideas for possible improvements made during the workshop. For instance, the head of ambulance (AS) brought up the aspect of civilian-to-civilian communication. Although this idea conflicts with the risk that a person broadcasting a Beacon may actually be a terrorist, he justified his opinion by explaining that, for other scenarios, a civilian-to-civilian communication would be helpful. For instance, in the aftermath of a flooding or an earthquake, volunteers or local residents could use our technology supporting them while trying to help affected people.

The industrial manufacturer (IM) further proposed to link the responder application via the GPS feature with a map-based application that also works in an off-line modus by caching GPS positions. Having this in place, the IM explained the use case of a responder independently looking for affected people in the vicinity without having received instructions from the incident commander.

Finally, the federal police officer (FP) underlined the limitation of relying on location changes being only visible through the Wi Fi SSID.

> FP: What happens if a victim moves elsewhere? I mean assume his position would change significantly its position. Then the location that you have obtained earlier when connecting to a victim's phone would become obsolete.

5 DISCUSSION

The evaluation allowed us to gain insights into the usefulness our system in the practice of emergency response in the specific context of a simulated terrorist attack. As we have seen, the visibility and validity of help messages were the most important concern for the participants of our study. In this section, we further discuss our findings with regard to these aspects and suggest design responses to address them within the scope of our solution. We also explore some more general implications for the design of ethically-aware SOS systems in general.

In our previous study, we received positive feedback regarding our prototype, it being deemed to be useful during emergency response operations in such constrained environments as the tunnel fire that we investigated, especially for later phases of the emergency operations where the immediate danger of the fire would be under control and other tasks such as finding affected persons more important (Al-Akkad et al., 2014b). Even in the tunnel fire scenario, however, it became clear that responders were dealing with a multitude of sometimes conflicting aims and shifting priorities, and that designing our solution for such practices did not only require providing a usable, technically working solution, but also to better understand the needs and constraints of emergency response practice in which context our solution was meant to be used.

5.1 Managing (In-)visibility of Distress Calls

The strategy of exposing the presence of an affected person through a Beacon is useful for disaster scenarios such as natural or industrial disasters, where it is hard to conceive of situations where exposing their presence would put a person at risk (Al-Akkad et al., 2014b). In the large-scale terrorist attack scenario, however, it turned out to be problematic, as users expressed the concern that their freely broadcast distress signals could alert the terrorists to locate and harm them. In the post-exercise interviews both affected people and responders voiced concerns about potentially disclosing their location to the terrorists. In a shooting or a terrorist attack, any perpetrator using a phone with Wi-Fi capability could retrieve the Beacon information on the presence, and potentially even descriptions of the locations of affected people, as the default settings of their phone would notify them of any discovered Wi-Fi network in range.

Within the context of terror attacks, privacy issues in nearby networks gains much greater importance than in other use cases. Privacy based on proximity such as described by Toch & Levi (2013) fail because they fall short of granting access only to a subset of users within a given radius. Yet, in situations with strongly limited infrastructures, it is challenging to provide a technological solution that still scales as easily as the HelpBeacons prototype on the one hand and on the other is powerful and flexible enough to allow management of visibility and security.

Thus, from our perspective, the need to manage the visibility of the beacons in a better way involves making it clearer to users that, depending on the situation, using the app in this particular way could potentially put them in danger. On the positive side, users were quite aware of this aspect in our study, so it could be enough to offer the possibility of entering a "silent" mode of the distress application which would either remain completely silent, only scanning for other beacons, or convey less information about the location of the user. Moreover, as the police seemed to be less concerned about broadcasting their location, we are now working on an inverted setup of our system, i.e. a responder would carry a device that broadcasts a "I'm a responder that is here to help you" message of sorts, which in turn people carrying devices in Wi-Fi scan mode would be able to discover and connect to in order to notify the responder device of their presence (as a side effect, this would also save battery power on phones carried by affected people). Such a setup would be more suitable in situations in which the user behind a Beacon could get in danger by broadcasting his/her position, and decides to hide instead of calling for help, and it would offer additional possibilities for improving the security of the handshake between the devices (for instance by using fixed SSIDs for the seeker or certificates for authentication).

In situations where the police might also be concerned about giving away their position, the broadcasting device and/or the Seeker could also be attached to an unmanned aerial vehicle (UAV), if the area of operation allows it. This approach would be useful, in particular for adversarial situations in which it is dangerous for responders to approach an impact zone, or where they need to cover a wide area. Tracking Wi-Fi phones via UAVs has already been investigated by some research (Wang et al., 2013; Yanmaz, 2012), and seems to be a promising approach to explore. We think this approach could help significantly to increase the scalability of our system, besides the implementation of an inverted setup. Also, such an approach might support the discovery and rescue of affected people who are not able to set up a distress signal, but are nevertheless near to tracked signals.

Regarding the requests for getting an answer to the SOS signal, our system so far only supports a very preliminary function of sending an automated response to users when their signal has been picked up by the Seeker. This gives users at least a very basic feedback when their message has been received. However, our findings show a need for support for richer engagement, because people in distress would want to have human contact rather than getting an automated "answering machine" style message (for example, people in distress want to know when help will be coming, or what to do until then). It would, therefore, be interesting to extend the capabilities of our system towards a more dialogic way of communication, allowing for example the field operators or incident commanders to record situation-specific answers to help calls which are conveyed as soon as the system gets a connection again. However, due to the resource limitations of our approach as well as the contingencies of emergency situation it remains a question for further research. Additional technical design concepts may be needed as well as changes in social and organizational practices and structures in order to bring such tools into practice. The informal response capabilities of our system could be enhanced by such functionality, allowing – where visibility is not a problem – other users in the vicinity of a person in distress to pick up a signal and communicate, supporting affected people in helping each other, potentially prior to or alongside the involvement of professional responders.

5.2 Assessing Validity of Data

The validity of distress calls was another identified limitation of our system, one previously unconsidered in our earlier study, where such possibilities would be hardly conceivable. Practitioners pointed out situations where attackers might pretend to be responders by using a stolen Seeker device. While the benefit of our system unfolds through the ubiquity of Wi-Fi SSIDs, at the same time our technology can be misused to set up malign messages. Given the terrorist attack scenario, a terrorist could have set up a deceptive message and harmed responders lured into trusting the distress signal. Of course, such misuse of the system mirrors known threats such as hoax calls or misusing the police radio channel (Bergmann, 1993; Garcia and Parmer, 1999; Whalen and Zimmerman, 1990). As a police officer, entering a situation with violent criminals is always dangerous, and the police would never simply trust the messages they receive during such an incident. However, having to take the decision whether or not to enter a certain area, the validity of the received messages both in terms of content and additional data (such as location information) was definitely a concern for the police officers in our study. Given the events that can arise in the course of a disaster—the location of a person might change or their state of health might deteriorate—it is not always possible to assess whether the received information, even when truthfully entered, is still up to date.

Preventing fake or untruthful messages in a system that is deliberately as open and simple as ours poses great challenges and brings new disadvantages. From our perspective, automatic identification of fake messages is hardly possible, as we cannot control which users install the application and what they do with them. It is thus up to the responders in the field or in the command center to interpret the information they receive via the system. Similar to the problem described for the visibility of the messages, we believe that adding a feedback channel could have some positive effects here, as it would allow police officers to initiate at least a simple dialog with the users behind a Beacon. However, the high stress level and the multitude of tasks that characterize emergency response operations (Al-Akkad et al., 2014b) would make it difficult for practitioners to employ substantial resources to checking yet another interactive response channel to detect hoaxes or malign messages.

From a response point of view, the validity of the distress signals in terms of being "up-to-date" is much more important. As pointed out by the practitioners, distress calls might change over the course of the response operation and require changes in the logistics of response efforts. To complicate the process of setting up a message would decrease the simplicity of our system making its usage less attractive. However, it would be possible to follow a layered approach here, where users can select additional functionalities if they so desire, while keeping the very simple "just push a button to send SOS" approach intact. In addition, it would be possible to prompt the user for a status update every once in a while, either based on a predefined interval (every 30 minutes) or based on changes the app would be able to detect automatically (such as when the GPS position changes, or the signal gets lost).

In the future, we could enhance our system to automatically indicate to a Seeker that the state of a Beacon, for e.g. the GPS position, has changed. For doing so, the Beacon app could monitor its state and indicate changes with a special byte in the broadcasted SSID. The Seeker could then re-connect to such marked beacons and update the information accordingly. Of course, this approach would reduce the space reserved for the help message by a further ASCII-character. To recognize that the state of a Beacon has changed could also be dealt with at the site of the Seeker by two strategies: When tracking more than once the same Beacon, the Seeker could compare the location of the Beacon with the location the Seeker had when it tracked the Beacon for the first time, or after a certain time interval the cached list of Beacons could be refreshed, then the Seeker would track and connect to the Beacons as if the Seeker had not previously encountered the Beacons.

5.3 General Ethical Deliberations

Introducing new technology into the organization of response can have disruptive effects. Ellebrecht and Kaufmann (2014), for instance, document how in a trial of e-triage technology, intended to speed up the triage process in German ambulance service, the primary effect was the introduction of a formal triage algorithm. They find that, in terms of time savings, the system responds to – and drives and further legitimizes – currently contested changes in the organization of triage in German emergency response organizations. There are two elements. Firstly, in Germany, mass casualty incident triage was traditionally carried out by physicians and documented by paramedics. This is a costly, labor intensive and relatively slow practice with high quality standards. The e-triage system they discuss supports paramedic triage, that is, a shift of responsibility from emergency physicians to (cheaper and more numerous) paramedics, who can be prompted or strictly guided by a "simple triage and rapid treatment" protocol (START) captured in the algorithm that takes the paramedic through a series of diagnostic steps. By highlighting a series of ambiguities arising in the co-constitution of technology and society, Ellebrecht and Kaufmann's study sensitizes the reader to the entanglement of social practice, societal values and technological potential.

In the case of our technology which provides information on victims and their locations, this tool might be used to organize and direct the allocation of help and the dispatch of teams, which could disrupt established ways of organizing response, similarly leading to potential ethical implications. For example, today, it is common practice for first responders to organize the search for affected people based on a grid pattern, where one sector after another is cleared by the responders operating in the field. Sticking to the pattern, the first responders might even ignore calls for help from other sectors on purpose. This procedure has several ethical implications: on the one hand, ensures that there is no preference in the order in which affected persons are rescued, implying a certain kind of fairness in the response, and it tries to avoid that anybody is overlooked. On the other hand, there is the chance that precious time is wasted while searching the "wrong" sectors first; especially in time critical missions where there might be many wounded people, an argument could be made for changing the prioritization of the response efforts to sectors with the most (or most severely) wounded.

Our system certainly has the possibility to affect such practices, as it allows identifying distress calls in an automatic way, and visualizing them on a map in the incident command center. However, this does have strong ethical implications, as it could discriminate against people who have no means to send a help signal (because they simply don't have a smartphone, the battery is drained, or when they are unable to use the application because of a wound or because they are unconscious). In addition, the availability of such a system might put pressure on the response agencies, making it hard for them to justify why a certain person wasn't rescued, despite the fact that they and their situation were known (Büscher et al., 2014). Hence, while the additional information that can be gathered with such an SOS system is of course of potential interest for first responders, there is a need for caution towards the potential ethical implications of the introduction of such a system, and a need for a careful negotiation of priorities in the organization of response. Potentially there will also be the need to find new (ethical) justifications.

This finding is related to a more conceptual layer of emergency response work, namely the question how logistical decisions of the rescue operations affect ethical issues such as fairness and humanity (in terms of who has better chances to be rescued first). We would argue that such ethical implications can likely not be fully covered and/or prevented by the technical design of systems; due to the complex and often contradictory nature of socio-technical innovations, especially in domains with such high stakes as emergency response, we would argue that it is rather necessary to make such implications explicit and cover them in the co-design process right from the start—similar to the improvisational and situated models of change management that researchers have recommended for technology design in general (Orlikowski and Hofman, 2009). It would hence be important to find ways to react to such deeper consequences of new technologies for the practice of emergency responders, and enable different stakeholders (such as practitioners, but also civil representatives, lawyers, and politicians) to participate in a way that allows for the discussion of possible implications on a higher level than on the specifics of particular details of design decisions and technical solutions. This requires novel approaches to co-design which demonstrate an ethical awareness in the sense that they go beyond the focus on changing practices from a merely "operative" perspective towards a greater societal and ethical background (Liegl et al., 2015; Liegl et al., 2016; Pereira and Baranauskas, 2015).

6 CONCLUSION

In this paper, we have presented a study on the use of a lightweight SOS system for smartphones in the evaluation context of a large-scale terrorist attack exercise. Studying the deployment of our system in a different scenario and with a different conceptual basis and focusing on the dialogic and local nature of distress calls allowed us to identify unforeseen contingencies and subtleties in the practices we are aiming to support. This added a new context dimension to our work, and allowed us to refine our design and add to the discussion on the practicality of ad-hoc communication systems in crisis informatics (e.g. Hagar and Haythornthwaite, 2005b; Palen and Liu, 2007). It further, and of equal importance, demonstrated the importance of understanding the specificities of emergency and/or disaster response as well as their more general features.

Arguably, based on our empirical work the forms network infrastructure may take in emergencies can be projected by two contingent dimensions (see Figure 8): the grade of the availability of network infrastructure (i.e. whether mobile services are available or not), and the degree of sensitivity of the communication (i.e. between people in distress and the police).

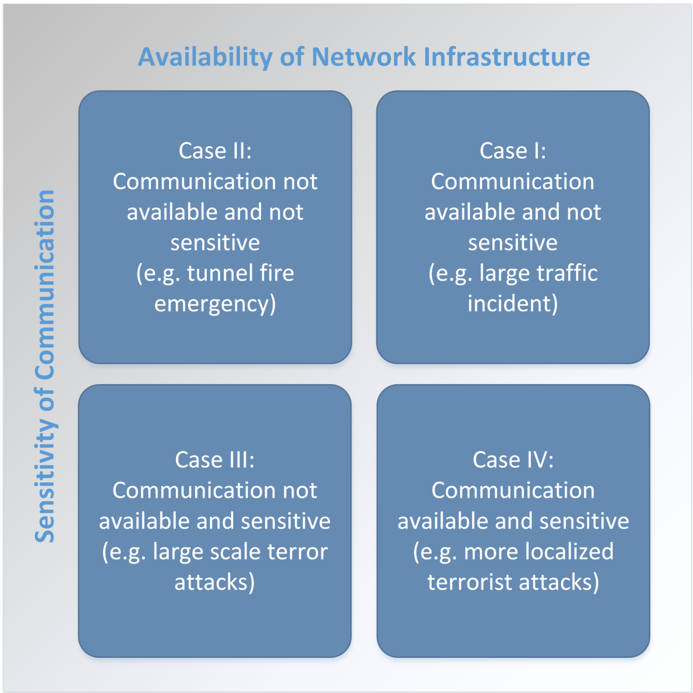
Availability of Network Infrastructure
Sensitivity of Communication
Case II: Communication not available and not sensitive (e.g. tunnel fire emergency)
Case I: Communication available and not sensitive (e.g. large traffic incident)
Case III: Communication not available and sensitive (e.g. large scale terror attacks)
Case IV: Communication available and sensitive (e.g. more localized terrorist attacks)

Figure 8: Different emergency scenarios based on the availability of networking and the sensitivity of communication.

Much work within the field of crisis informatics (Ludwig et al.,2015; Reuter et al., 2013; Palen et al., 2007) has dealt with the means of emergency response by using existing infrastructures and crowdsourced information (Case I). The tendency of infrastructures to break down in emergency situations motivated us to develop our prototype on a backdrop of potential lack of infrastructure and infrastructural breakdown (Case II). In our prior work, we intended to provide a means to enable untargeted, ad hoc solutions to request help and ease the rescue process (Al-Akkad et al., 2014a,b). Yet deploying and testing our prototype in the context of terror attacks revealed new design challenges, which dealt with the sensitivity of information, the ability to control overall visibility and the management of the target audience (Case III). For this case, existing solutions appear not to work too well, as the sensitivity of communication challenges existing peer to peer approaches. Likewise, approaches that have been investigated in the context of social media analysis which, to some extent, can lead to similar deliberations regarding the "accuracy" of the received information (Linna Li, 2010; Palen et al., 2010b) are hard to leverage for our SOS system because of the much smaller and more localized scope.

To address these issues, we were able to conceptualize new solutions based on our empirical findings for managing the validity (in terms of "is the received information truthful and up-to-date") as well as the visibility (in terms of "who can see my SOS signal, if at all") of SOS messages. Further possible augmentations entailed the idea of inverting the roles of sender and receiver (to avoid having people broadcasting their location) and/or placing the seeker device on a UAV. Such features could be even further augmented in Case IV scenarios where the communication network is at least partially restored (e.g. by the emergency responders rolling out their own networks), allowing to exchange more data or open additional communication channels to control the visibility of information and assess the authenticity of the recipient. Combining centralized approaches and our concept would allow us to address remaining limitations that are inherent to peer to peer protocols by augmenting our tool with location-based services (cf. Gordon and Silva, 2011; Wu et al., 2013). Here, the challenge would be to extend and adapt existing approaches where co-location is used mainly to enhance interaction and information exchange (Stein et al., n.d.; Toch and Levi 2013), without taking care of the potentially life-threatening implications of giving away ones location in adversarial situations as the one we studied.

Apart of opening a new area for design, our study also has general implications for the design of ad hoc SOS systems. While most emergencies will not be identical in character to the one we describe, it is our contention that the understanding of a variety of scenarios is important in determining the degree to which generic approaches to 'help' in disaster conditions might be valid. Our findings underline that the attempt to simplify distress calls by exchanging the "classic" dialogic nature of calling a help line with the broadcasting of simple statements might, whilst useful, also come with certain problems. Depending on the nature of the incident, people may alternatively hide or shout for help, and situations might be easily too complex to be described in a single, brief statement (this implies further challenges for the design of interfaces that are usable in life-threatening situations). Furthermore, discussions with the experts during the workshop as well as the general deliberations of the students and responders in our study revealed some interesting aspects: that despite the rather "local" nature of the technology—which could be interpreted as being very close to vocal calls for help—and the additional contextual information that is exchanged by the tool in terms of GPS location and "safe/unsafe", status information is not always sufficient. Also, even in non-threatening situations, the users wanted to have more information about whether their SOS signal would have been picked up, and by whom. Hence, our findings also have implications for disaster situations in general (i.e. even when sensitivity and connectivity don't pose issues). Especially, with regard to the informal response capabilities that allow people in the vicinity of a disaster to cooperate (see Palen et al., 2010a), and with regard to more general ethical deliberations of emergency response (cf. Liegl et al. 2015; Liegl et al. 2016).

Our previous study (Al-Akkad et al. 2014b) and the one we present here underline the importance of exploring emergency support systems in situations that are as realistic as possible and ensuring that the situations in question encompass different conditions. In this case, the importance of 'sensitivity' that is introduced by the adversarial nature of the situation is paramount. Approaches such as the one we detailed help us identify subtle and sometimes unintended side effects and contingencies that can affect the appropriation of such tools in practice. Having said that, we want to initiate the discourse on what issues should be taken into account when designing technology relevant for security. Our study highlights in particular two needs, i.e. a) being able to configure or (semi-) automate the visibility of distress calls and b) seeking for ways that validate or at least strengthen the credibility of distress calls. In order to confirm that tools as the presented one are applicable for the broad range of emergency situations, further studies need to inform the community of which aspects/issues need to be taken into account in order to ensure a wide practicality/utility of such tools.

ACKNOWLEDGMENTS

Special thanks to the practitioners who provided valuable feedback and insights for the domain of emergency response. We are grateful to our colleagues in the BRIDGE project (FP7SEC-2010-1) for their support in this research.

REFERENCES

Abel, F., Hauff, C., Houben, G.-J., Stronkman, R., Tao, K., 2012. Twitcident: Fighting Fire with Information from Social Web Streams, in: Proceedings of the 21st International Conference Companion on World Wide Web, WWW '12 Companion. ACM, New York, NY, USA, pp. 305–308. doi:10.1145/2187980.2188035

Aguirre, B., Wenger, D., Glass, T., Diaz-Murillo, M. & Vigo, G. (1995). The Social Organization of Search and Rescue: Evidence from the Guadalajara Gasoline Explosion. International Journal of Mass Emergencies and Disasters, 13:93–106.

Al-Akkad, A., Raffelsberger, C., Boden, A., Ramirez, L., Zimmermann, A., 2014a. Tweeting "when online is off"? opportunistically creating mobile ad-hoc networks in response to disrupted infrastructure, in: Proceedings of the 11th International Conference on Information Systems for Crisis Response and Management. University Park, Pennsylvania.

Al-Akkad, A., Ramirez, L., Boden, A., Randall, D., Zimmermann, A., 2014b. Help Beacons: Design and Evaluation of an Ad-hoc Lightweight S.O.S. System for Smartphones, in: Proceedings of the 32nd SIGCHI Conference on Human Factors in Computing Systems, CHI '14. ACM, New York, NY, USA, pp. 1485–1494. doi:10.1145/2556288.2557002

Al-Akkad, A., Ramirez, L., Denef, S., Boden, A., Wood, L., Büscher, M., Zimmermann, A., 2013. "Reconstructing Normality": The Use of Infrastructure Leftovers in Crisis Situations As Inspiration for the Design of Resilient Technology, in: Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration, OzCHI '13. ACM, New York, NY, USA, pp. 457–466. doi:10.1145/2541016.2541051

Baker, C., Emmison, M., Firth, A., 2005. Calling for Help: Language and social interaction in telephone helplines. John Benjamins Publishing.

Bergmann, J., 1993. Alarmiertes Verstehen: Kommunikation in Feuerwehrnotrufen, in: Wirklichkeit Im Deutungsprozesss. Suhrkamp, Frankfurt a. M., pp. 283–328.

Birnholtz, J., Fitzpatrick, C., Handel, M. and Brubaker, J. R. 2014. Identity, Identification and Identifiability: The Language of Self-presentation on a Location-based Mobile Dating App. Proceedings of the 16th International Conference on Human-computer Interaction with Mobile Devices & Services, ACM, 3–12. http://doi.org/10.1145/2628363.2628406

Blackwell, C., Birnholtz, J., and Abbott, C. 2014. Seeing and being seen: Co-situation and impression formation using Grindr, a location-aware gay dating app. New Media & Society: 1461444814521595. http://doi.org/10.1177/1461444814521595

Bornheim, M., Fletcher, M., 2016. Public Safety Digital Transformation. The Internet of Things (IoT) and Emergency Services. EENA Technical Committee Document Brussels, available online at: http://www.eena.org/download.asp?item_id=170.

Büscher, M., Liegl, M., Thomas, V., 2014. Collective Intelligence in Crises, in: Miorandi, D., Maltese, V., Rovatsos, M., Nijholt, A., Stewart, J. (Eds.), Social Collective Intelligence, Computational Social Sciences. Springer International Publishing, pp. 243–265.

Chorley, M.J., Colombo, G.B., Allen, S.M., Whitaker, R.M., 2015. Human content filtering in Twitter: The influence of metadata. Int. J. Hum.-Comput. Stud. 74, 32–40. doi:10.1016/j.ijhcs.2014.10.001

Coyle, D., Meier, P., 2009. New Technologies in Emergencies and Conflicts: The Role of Information and Social Networks. United Nations Foundation & Vodafone Foundation.

Cromdal, J., Osvaldsson, K., Persson-Thunqvist, D., 2008. Context that matters: Producing "thick-enough descriptions" in initial emergency reports. J. Pragmat., Special Issue: Questions of Context in Studies of Talk and Interaction—Ethnomethodology and Conversation Analysis 40, 927–959. doi:10.1016/j.pragma.2007.09.006

Denef, S., Keyson, D., Oppermann, R., 2011. Rigid Structures, Independent Units, Monitoring: Organizing Patterns in Frontline Firefighting, in: Proceedings of the 29th SIGCHI Conference on Human Factors in Computing Systems, CHI '11. ACM, New York, NY, USA, pp. 1949–1958. doi:10.1145/1978942.1979225

Dynes, R.R., 1995. Response to Disaster: Fact Versus Fiction and Its Perpetuation, The Sociology of Disaster. By Henry W. Fischer, III. University of America, 1994. 160 pp. Cloth, $46.50; paper, $18.50. Soc. Forces 74, 370. doi:10.1093/sf/74.1.370

Edwards, W.K., Bellotti, V., Dey, A.K., Newman, M.W., 2003. The Challenges of User-centered Design and Evaluation for Infrastructure, in: Proceedings of the 21st SIGCHI Conference on Human Factors in Computing Systems, CHI '03. ACM, New York, NY, USA, pp. 297–304. doi:10.1145/642611.642664

Ellebrecht, N., Kaufmann, S., 2014. Boosting Efficiency Through the Use Of IT?: Reconfiguring the Management of Mass Casualty Incidents in Germany. Int. J. Inf. Syst. Crisis Response Manag. IJISCRAM 6, 1–18.

Falk, J., Ljungstrand, P., Björk, S. and Hansson, R. 2001. Pirates: Proximity-triggered Interaction in a Multi-player Game. CHI '01 Extended Abstracts on Human Factors in Computing Systems, ACM, 119–120. http://doi.org/10.1145/634067.634140

French, S., Niculae, C., 2005. Believe in the Model: Mishandle the Emergency : Journal of Homeland

Security and Emergency Management. JHSEM 2.

Garcia, A.C., Parmer, P.A., 1999. Misplaced Mistrust: The Collaborative Construction of Doubt In 911 Emergency Calls. Symb. Interact. 22, 297–324. doi:10.1016/S0195-6086(00)87399-3

Gordon, E., Silva, A. de S. e, 2011. Net Locality: Why Location Matters in a Networked World. John Wiley & Sons.

Hagar, C., Haythornthwaite, C., 2005. Crisis, Farming & Community. J. Community Inform. 1.

Harrald, J.R., 2006. Agility and Discipline: Critical Success Factors for Disaster Response. Ann. Am. Acad. Pol. Soc. Sci. 604, 256–272. doi:10.1177/0002716205285404

Hornecker, E., Swindells, S., and Dunlop, M. 2011. A Mobile Guide for Serendipitous Exploration of Cities. Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, ACM, 557–562. http://doi.org/10.1145/2037373.2037460

Hossmann, T., Legendre, F., Carta, P., Gunningberg, P., Rohner, C., 2011. Twitter in Disaster Mode: Opportunistic Communication and Distribution of Sensor Data in Emergencies, in: Proceedings of the 3rd Extreme Conference on Communication: The Amazon Expedition, ExtremeCom '11. ACM, New York, NY, USA, pp. 1:1–1:6. doi:10.1145/2414393.2414394

Iosifidis, G., Gao, L., Huang, J., Tassiulas, L., 2014. Enabling crowd-sourced mobile Internet access, in: Proceedings of the 33rd Annual International Conference on Computer Communications, INFOCOM '14. IEEE, pp. 451–459. doi:10.1109/INFOCOM.2014.6847968

Jennex, M.E., 2012. Social Media – Truly Viable For Crisis Response?, in: Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management, ISCRAM'12. ISCRAM, Vancouver, BC, Canada.

Jul, S., 2007. Who's really on first? A domain-level user, task and context analysis for response technology, in: Proceedings of the 4th International Conference on Information Systems for Crisis Response and Management ISCRAM 2007. pp. 139–148.

Kendra, J. & Wachtendorf, T. (2006). Community Innovation and Disasters. In Rodríguez, H., Quarantelli, E. & Dynes, R. (Eds.), Handbook of Disaster Research: 316–334. Springer.

Krishnamoorthy, S., Agrawala, A., 2012. Context-aware, Technology Enabled Social Contribution for Public Safety Using M-Urgency, in: Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services, MobileHCI '12. ACM, New York, NY, USA, pp. 123–132. doi:10.1145/2371574.2371594

Larsen, T., 2013. Dispatching Emergency Assistance: Callers' Claims of Entitlement and Call Takers' Decisions. Res. Lang. Soc. Interact. 46, 205–230. doi:10.1080/08351813.2013.810401

Licoppe, C., 2004. "Connected" presence: the emergence of a new repertoire for managing social relationships in a changing communication technoscape. Environ. Plan. Soc. Space 22, 135 – 156. doi:10.1068/d323t

Liegl, M., Boden, A., Büscher, M., Oliphant, R. Kerasidou, X. 2016. Designing for Ethical Innovation: A Case Study on ELSI Co-Design in Emergency. International Journal of Human-Computer Studies, 2016, -. doi:http://dx.doi.org/10.1016/j.ijhcs.2016.04.003.

Liegl, M., Oliphant, R., Buscher, M., 2015. Ethically Aware IT Design for Emergency Response: From Co-Design to ELSI Co-Design.

Liegl, M., Stempfhuber, M., 2014. „Raum am Draht": Empirische Beobachtung zur Soziologie der mediatisierten Anmache am Fallbeispiel von Grindr, in: Hahn, K. (Ed.), E<3Motion, Medienkulturen im digitalen Zeitalter. Springer Fachmedien Wiesbaden, pp. 19–38.

Linna Li, M.F.G., 2010. The Role of Social Networks in Emergency Management: A Research Agenda. IJISCRAM 2, 48–58. doi:10.4018/jiscrm.2010100104

Ludwig, T., Reuter, C. Pipek, V.. 2013. What You See Is What I Need: Mobile Reporting Practices in Emergencies. In ECSCW 2013: Proceedings of the 13th European Conference on Computer Supported Cooperative Work, 21-25 September 2013, Paphos, Cyprus, 181–206. Springer London.

Ludwig, T., Reuter, C., Siebigteroth, T., Pipek, V., 2015. Crowdmonitor: mobile crowd sensing for assessing physical and digital activities of citizens during emergencies, in: Proceedings of the Conference on Human Factors in Computing Systems (CHI). ACM Press, Seoul.

Mark, G. & Semaan, B., 2008. Resilience in Collaboration: Technology As a Resource for New Patterns of Action. In Proceedings of the 12th Conference on Computer Supported Cooperative Work. CSCW '08. New York, NY, USA: ACM, pp. 137–146. doi:10.1145/1460563.1460585.

Mark, G.J., Al-Ani, B. & Semaan, B., 2009. Resilience Through Technology Adoption: Merging the Old and the New in Iraq. In Proceedings of the 27th SIGCHI Conference on Human Factors in Computing Systems. CHI '09. New York, NY, USA: ACM, pp. 689–698. doi:10.1145/1518701.1518808.

Mitchell, J, Thomas, D., Hill, A. and Cutter, S. 2000. Catastrophe in reel life versus real life: perpetuating disaster myth through Hollywood films. International Journal of Mass Emergencies and Disasters 18, 3, 383–402.

Müller, H., Fortmann, J., Timmermann, J., Heuten, W. and Boll, S. 2013. Proximity Sensor: Privacy-aware Location Sharing. Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services, ACM, 564–569. http://doi.org/10.1145/2493190.2494443

O'Keefe, E., 2009. FEMA Chief Fugate Wants Public Involved in Preparation Efforts. Wash. Post.

Orlikowski, W.J., Hofman, D.J., 2009. An Improvisational Model for Change Management: The Case of Groupware Technologies.

Palen, L., Anderson, K.M., Mark, G., Martin, J., Sicker, D., Palmer, M., Grunwald, D., 2010a. 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, ACM-BCS '10. British Computer Society, Swinton, UK, UK, pp. 8:1–8:12.

Palen, L., Liu, S.B., 2007. Citizen Communications in Crisis: Anticipating a Future of ICT-supported Public Participation, in: Proceedings of the 25th SIGCHI Conference on Human Factors in Computing Systems, CHI '07. ACM, New York, NY, USA, pp. 727–736. doi:10.1145/1240624.1240736

Palen, L., Vieweg, S., Anderson, K.M., 2010b. Supporting "Everyday Analysts" in Safety- and Time-Critical Situations. Inf. Soc. 27, 52–62. doi:10.1080/01972243.2011.534370

Paoletti, I., 2009. Communication and Diagnostic Work in Medical Emergency Calls in Italy. Comput. Support. Coop. Work CSCW 18, 229–250. doi:10.1007/s10606-009-9091-1

Paulos, E. and Goodman, E.. 2004. The Familiar Stranger: Anxiety, Comfort, and Play in Public Places. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 223–230. http://doi.org/10.1145/985692.985721

Pereira, R., Baranauskas, M.C.C., 2015. A value-oriented and culturally informed approach to the design of interactive systems. Int. J. Hum.-Comput. Stud. 80, 66–82. doi:10.1016/j.ijhcs.2015.04.001

Perng, S.-Y., Büscher, M., Wood, L., Halvorsrud, R., Stiso, M., Ramirez, L., Al-Akkad, A., 2013. Peripheral response: microblogging during the 22/7/2011 Norway attacks. Int. J. Inf. Syst. Crisis Response Manag. 5, 41–57.

Quarantelli, E.L., Dynes, R.R., 1972. When disaster strikes (it isnt much like what youve heard and read about). Psychol. Today 5, 66.

R. Beale. 2005. Supporting social interaction with smart phones. IEEE Pervasive Computing 4, 2: 35–41. http://doi.org/10.1109/MPRV.2005.38

Reuter, C., 2013. Power Outage Communications: Survey of Needs, Infrastructures and Concepts. Proc ISCRAM.

Reuter, C., Marx, A., Pipek, V., 2012. Crisis Management 2.0: Towards a Systematization of Social Software Use in Crisis Situations. Int. J. Inf. Syst. Crisis Response Manag. IJISCRAM 4, 1–16. doi:10.4018/jiscrm.2012010101

Rheingold, H., 2007. Smart Mobs: The Next Social Revolution. Basic Books.

Semaan, B. & Mark, G., 2011. Technology-mediated Social Arrangements to Resolve Breakdowns in Infrastructure During Ongoing Disruption. ACM Transactions on Computer-Human Interactions, 18(4), p.21:1–21:21. doi:10.1145/2063231.2063235.

Stallings, R. A. & Quarantelli, E. L. (1985). Emergent Citizen Groups and Emergency Management. Public administration Review 45: 93–100.

Starbird, K. and Palen, L. "Voluntweeters": self-organizing by digital volunteers in times of crisis. Proc. CHI 2011, ACM Press (2011), 1071-1080.

Starbird, K. and Stamberger, J. Tweak the Tweet: Leveraging Microblogging Proliferation with a Prescriptive Syntax to Support Citizen Reporting. Proc. ISCRAM 2010, ISCRAM Press.

Stein, M., Meurer, J., Boden, A., Liegl, M., Wulf, V. (n.D.). Supporting Ridesharing Practices of Elderly – A Study of Awareness and Addressability in Situations of Physical Proximity. International Journal on Human Computer Studies, in review.

Sutko,D.M., and de Souza e Silva, A. 2011. Location-aware mobile media and urban sociability. New Media & Society: 1461444810385202. http://doi.org/10.1177/1461444810385202

Sutton, J., 2012. When Online is Off: Public Communications Following the February 2011 Christchurch, NZ Earthqauke, in: Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management, ISCRAM'12. ISCRAM, Vancouver, BC, Canada.

Toch, E. and Levi, I. 2013. Locality and Privacy in People-nearby Applications. Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing, ACM, 539–548. http://doi.org/10.1145/2493432.2493485

Turoff, M. 2002. Past and future emergency response information systems. *Communications of the ACM 45*, 4, 29-32.

Wang, W., Joshi, R., Kulkarni, A., Leong, W.K., Leong, B., 2013. Feasibility Study of Mobile Phone WiFi Detection in Aerial Search and Rescue Operations, in: Proceedings of the 4th Asia-Pacific Workshop on Systems, APSys '13. ACM, New York, NY, USA, pp. 7:1–7:6. doi:10.1145/2500727.2500729

Weidemann, C., 2013. Social Media Location Intelligence: The Next Privacy Battle - An ArcGIS add-in and Analysis of Geospatial Data Collected from Twitter.com. Int. J. Geoinformatics 9.

Whalen, J., Zimmerman, D.H., 1998. Observations on the Display and Management of Emotion in Naturally Occurring Activities: The Case of "Hysteria" in Calls to 9-1-1. Soc. Psychol. Q. 61, 141–159. doi:10.2307/2787066

Whalen, M.R., Zimmerman, D.H., 1990. Describing trouble: Practical epistemology in citizen calls to the police. Lang. Soc. 19, 465–492. doi:10.1017/S0047404500014779

Wu, A., Convertino, G., Ganoe, C., Carroll, J.M., Zhang, X. (Luke), 2013. Supporting collaborative sense-making in emergency management through geo-visualization. Int. J. Hum.-Comput. Stud., Special Issue on supporting shared representations in collaborative activities 71, 4–23. doi:10.1016/j.ijhcs.2012.07.007

Wulf, V., Rohde, M., Pipek, V., Stevens, G., 2011. Engaging with practices: design case studies as a research framework in CSCW, in: Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work, CSCW '11. ACM, New York, NY, USA, pp. 505–512. doi:10.1145/1958824.1958902

Yanmaz, E., 2012. Connectivity versus area coverage in unmanned aerial vehicle networks, in: 2012 IEEE International Conference on Communications (ICC). Presented at the 2012 IEEE International Conference on Communications (ICC), pp. 719–723. doi:10.1109/ICC.2012.6364585

Received June 2016; revised TBD; accepted TBD