Alerts and Warnings in Social Media: A Simulation Experiment
Charles File, Rannie Teodoro, Mor Naaman, Paul Kantor
Rutgers University School of Communication and Information
{chasfile, rteodoro, mor, paul.kantor}@rutgers.edu

ABSTRACT
Social media represent a powerful new tool for peer-to-peer communication and collaboration. Recent events – like the Moscow airport bombing (Anon, n.d.) – have shown that sometimes the information posted to social media like Twitter and Facebook by ordinary people at the scene of emergencies can be the best and most rapid source of information about those emergencies. Researchers of the Alerts and Warnings in Social Media (AWSM, pronounced “awesome”) project organized a competitive on-campus event at a major Eastern University. The event called “HatChase” was intended to simulate aspects of urgent emergency situations. It was designed to elicit student interest and to yield information about how students organized for the competition, and how effective they were in discovering and disseminating information. Semi-structured interviews were conducted with event participants, addressing search strategies, team coordination, and dissemination of information with communication technologies. Social media data and team communication reports were also collected and monitored. The team reports were analyzed for speed, dissemination, and accuracy. The analysis showed a great diversity of strategies. The analysis also revealed that there is relatively little analyzable content in the communications among the participants in an organized activity of discovery and dissemination.
Table of Contents

Alerts and Warnings in Social Media: A simulation experiment ................................................. 1

ABSTRACT ................................................................................................................................. 1

1 INTRODUCTION ..................................................................................................................... 4

2 OBJECTIVES OF THE AWSM PROJECT ............................................................................... 4

3 RELATED WORK AND BACKGROUND .................................................................................... 4

4 METHODS: SIMULATED EVENT OF INTEREST ...................................................................... 5

4.1 Description of HatChase .................................................................................................... 5

4.2 Participants .......................................................................................................................... 6

4.3 HatChase: Planning ............................................................................................................ 7

4.3.1 Administrative concerns ............................................................................................... 7

4.3.2 Experiment concerns ...................................................................................................... 8

4.4 HatChase: Execution .......................................................................................................... 9

4.4.1 Phase 1: Promotion ......................................................................................................... 9

4.4.2 Phase 2: HatChase Competition .................................................................................... 10

4.4.3 Phase 3: Judging ............................................................................................................ 12

4.4.4 Phase 4: Interviews with participants .......................................................................... 13

5 RESULTS ............................................................................................................................... 13

5.1 OBJECTIVE 1: DIGITAL MEDIA STRATEGIES TO COORDINATE EFFORTS .... 13

5.2 OBJECTIVE 2: EFFECTIVE STRATEGIES FOR DISSEMINATING & REPORTING 15

5.3 OBJECTIVE 3: STRATEGIES FOR LIMITING FALSE POSITIVE REPORTING ... 19

5.3.1 Sabotage! ....................................................................................................................... 19

5.3.2 Lack of data ................................................................................................................... 22

6 CONCLUSION ....................................................................................................................... 23

7 ACKNOWLEDGEMENTS ........................................................................................................ 23

8 REFERENCES .......................................................................................................................... 23

9 APPENDIX ............................................................................................................................. 26

9.1 Research Protocol for HC-1: AWSM Project ..................................................................... 26

9.1.1 Background .................................................................................................................... 26

9.1.2 Objectives ....................................................................................................................... 26

9.1.3 Subject Population and Recruitment ............................................................................. 26

9.1.4 Methodology ................................................................................................................. 27

9.1.5 Details about the challenge ............................................................................................ 27

9.1.6 Judging of Entries .......................................................................................................... 28

9.1.7 Flow-down of conditions ensuring data collection and protection of persons ............. 28

9.1.8 Provisions for Protection of Private, Identifiable Information ...................................... 31

9.1.9 Exemption Justification .................................................................................................. 31

9.1.10 Risks and Benefits ........................................................................................................ 32

9.2 Research Protocol for HC-1 Interviews: AWSM Project ....................................................... 33

9.2.1 Principal Investigator ..................................................................................................... 33

9.2.2 Summary ....................................................................................................................... 33

9.2.3 Objectives ....................................................................................................................... 33
9.2.4 Subject Population and Recruitment ................................................. 33
9.2.5 Consent Procedures ........................................................................ 33
9.2.6 Potential Benefits ........................................................................ 34
9.2.7 Potential Risks .............................................................................. 34
9.2.8 Protection of Subjects/ Private and Identifiable Information .............. 34
9.2.9 Analysis and Methodology .............................................................. 34
9.2.10 The Risk/Benefit Ratio .................................................................. 34
9.3 Consent Form to Participate in a Research Study ................................... 35
  9.3.1 INTRODUCTION ............................................................................. 35
  9.3.2 BACKGROUND/PURPOSE ................................................................. 35
  9.3.3 INFORMATION ............................................................................... 35
  9.3.4 RISKS .......................................................................................... 35
  9.3.5 BENEFITS ................................................................................... 35
  9.3.6 CONFIDENTIALITY ...................................................................... 36
9.4 Audio Addendum to Consent form ...................................................... 38
9.5 Sample Oral Consent Script .................................................................. 39
1 INTRODUCTION
Grassroots social action by everyday citizens help emergency responders like police officers, paramedics, and other crisis response officials become aware of and report crisis activity (Palen et al., 2007). While one cannot be certain of the accuracy and the truthfulness of citizen reports during tragedy and disaster, people have repeatedly banded together to spread accurate information and stifle false rumors (Tapia et al., 2011; Mendoza, 2010). Moreover, information and communication technologies (ICTs) like social networking sites and wikis afford online spaces where disaster survivors, suspicious or curious bystanders, and helpful Samaritans can interact (Palen & Liu, 2007).

As the use of social media to monitor, detect, and share unusual events rises, there is an increasing need to understand how groups form and communicate about geographically dispersed, but related events. The project described in this paper examines how individuals collaborate and coordinate in unexpected and time-constrained situations set up to simulate some aspects of an emergency/dangerous situation. Participants formed teams, were asked to input sightings into the event website, and were free to strategize and report their own communication and detection systems of the unusual campus activity. The project is designed to include a number of experiments. The present report addresses the design, execution, and lessons learned from the first HatChase (HC-1) experiment. Specifically, the report addresses:

- The objectives of the AWSM project
- Experimental procedures (planning and implementation)
- Analysis of the social media data and team-generated data

2 OBJECTIVES OF THE HAT-CHASE EXPERIMENTS

The purpose of this study was to create a controlled simulation (non-threatening, but readily observable event) of a terrorist attack and to monitor and record the ways in which individuals in the area of that attack might detect it, report it to authorities, and relay the information to others. The Defense Advanced Research Projects Agency (DARPA) Network Challenge (Hesse, 2009) influenced the design of our study. The chief goals of our research were to:

1. Study the ways in which groups use digital media to coordinate their efforts to detect emergencies
2. Discover effective strategies for disseminating and reporting information about emergencies
3. Determine strategies used for limiting false positive reporting

3 RELATED WORK AND BACKGROUND

We briefly review related work on the role of social media and mobile technology, the relevance of trust in emergency situations, and the emerging role social media plays today in rapid detection and dissemination of information.
Social media and mobile technology provide platforms through which people can communicate urgent and critical information in real time. Humans can act as “sensors” and share their observations and views via mobile devices and the Internet (Sheth, 2009; Lane et al., 2010). Numerous studies have looked at “social awareness streams” (Naaman et al., 2010) for the rapid detection of urgent and potentially life-threatening events (Hughes & Palen, 2009; Vieweg et al., 2010; Kendra & Wachtendorf, 2002).

Emergency situations and unexpected events can force individuals to trust and rely on information from unknown or unfamiliar others. However, despite concerns for false reports or information, people frequently bond together in times of crisis. For example, Vieweg et al. (2008) looked at the online interactions that occurred in the aftermath of the 2007 Virginia Tech Shooting, a tragic on-campus event that resulted in the death of 32 people. They found that despite the high distribution and decentralization of the problem, people demonstrated benevolent collective intelligence (Hiltz & Turoff, 1993) and exhibited problem-solving capabilities through online forums such as Facebook.

Most recently, social media services have emerged as channels for predicting and confirming unusual activity across what initially look like unrelated incidents or personal experiences. Sakaki et al. (2010), for instance, proposed an algorithm to monitor earthquakes in Twitter and detect a target event. Notably, most emergency response and preparedness studies (Brodie et al., 2006; Sutton et al., 2008; Mendoza et al., 2010) have examined citizen coordination, communication, and outcomes “after the fact.”

The DARPA Network Challenge has some overlap with the work described in this paper, and influenced the structure of our experiment. The DARPA Network Challenge required participants to locate ten large red weather balloons placed across the nation. Our analysis extends part of their work on crowdsourcing strategies and time-urgent problems and describes unusual activity on a smaller, more localized scale. Unlike the DARPA Network Challenge, our study asks both for the quickest detection of the activity and the broadest dissemination of the activity. Other than the DARPA experiment, no studies to our knowledge have actually controlled the variable representing the “emergency situation” to provoke “realistic” and “natural” citizen-generated social media data.

4 METHODS: SIMULATED EVENT OF INTEREST

Given the objectives of the project, “HatChase” was conceptualized as an event to simulate unusual events occurring on a university campus. This section describes the rules, plans, and implementation of that event.

4.1 Description of HatChase
HC-1 was an organized competitive event held at a large northeastern university. The event involved research accomplices who wore very “unusual” hats and placed themselves at scheduled locations on each of the several campuses of the university. Public notices about the event were released roughly a week before the actual event date.

The key features of the experiment are:
1. Participants were asked to self-form teams with the goal of quickly detecting and accurately reporting the sightings of hats (using a secret team passcode) on the official HC-1 website. Teams created their own selection of systems or procedures that leveraged social media and communication technology to detect hat sightings, filtered those detections in order to maximize reliability, and alerted the team members to those events.

2. After a period of discussion on campus and team formation, the teams competed to sight the location of the hats and detailed description of the hat wearers.

3. Teams also encouraged others (friends, friends of friends, etc.) to report sightings under their team passcode to boost their scores and chances of winning a large prize (First place: $4000, Second place: $2000, Third Place: $1000).

4. After the event, all teams were required to submit de-identified logged team communication records, or the most accurate possible description thereof. These reports supported our analysis and assessment of their specific strategies for motivation and dissemination.

5. A panel of judges (including representatives of the research project and its collaborators at other institutions, persons from the New Jersey Office of Homeland Security Preparedness, and the United States Department of Homeland Security Office of Science and Technology) assessed the performance of the teams with regard to the speed, dissemination, and the accuracy of their detection of the unusual hats.

4.2 Participants

Participants included University graduate and undergraduate students and staff not directly involved in the project at the time the experiment was run. Due to IRB restrictions, emphasis was placed on the role of “team leaders” (TLs) who provided consent for participation. No consent was obtained initially from other “team members” (TMs) or from people recruited to participate by team leaders. These team leaders were considered the “human subjects of the study” with whom researchers could interact directly. Researchers did not communicate with TMs during the experiment, and TLs freely recruited TMs on an ad hoc basis. TLs were responsible for: (a) presenting the team’s plan for detection and dissemination to the researchers; (b) assembling either a team or a “team formation scheme”; (c) aggregating the team’s social media communications during the challenge event; (d) de-identifying all team communications prior to submitting the communication record to the researchers; and (e) accepting the prize award, if any, on behalf of the team.

Our analysis included detailed interviews of TLs from the top seven teams in the competition. Due to the IRB-approved protocol, researchers were limited in making direct or persistent contact with other participants. However, researchers were able to interview leaders, and in some cases, one additional member, of each of the top seven teams, to explore the most “successful” team strategies. Table 1 describes the number of members and general makeup of the top seven teams in the competition.

Team Leaders revealed a crucial distinction between “core team members” (those who were part of the team from the start to finish of the event) and “unofficial team members” (those who helped the team, but did not/would not share in the prize). Over the top seven teams, the number of “core” members ranged from 3 to 86 (see Table 1, column “Number of ‘core team members’”). The first place team had 16 core TMs, second place team had 8 core TMs, and the third place team had 86 core TMs. Three teams (Teams 64, 29, and 11) created payment structures for those
who participated in posting confirmed sightings, and to those were the first sighters of hats. The other four teams reported that they decided to divide potential winnings equally among core members. Unofficial TMs primarily made reports of hats (see Table 1, column “Number of unique users who reported sightings”) and were occasionally extra pairs of eyes, passively (opposed to actively) searching for hat sightings, at the request of teams.

<table>
<thead>
<tr>
<th>Team Ranking</th>
<th>Team ID</th>
<th>Number of “core” team members</th>
<th>Number of unique users who reported sightings</th>
<th>Membership Characteristics of “core” team members</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st place</td>
<td>64</td>
<td>16</td>
<td>48</td>
<td>Members recruited from reddit.com¹. Team leader did not know any of the team members prior to HC-1.</td>
</tr>
<tr>
<td>2nd place</td>
<td>43</td>
<td>8</td>
<td>49</td>
<td>Seven family members and one close family friend.</td>
</tr>
<tr>
<td>3rd place</td>
<td>29</td>
<td>86</td>
<td>107</td>
<td>All male and members of an on-campus fraternity.</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
<td>11</td>
<td>4</td>
<td>Members were close friends prior to HC-1.</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
<td>41</td>
<td>3</td>
<td>All males, roommates.</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
<td>46</td>
<td>15</td>
<td>Originally from a non-course related research project. Team included friends and friends of friends.</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
<td>54</td>
<td>5</td>
<td>All males and members of an on-campus fraternity.</td>
</tr>
</tbody>
</table>

Table 1: Membership characteristics of the top seven teams

Notably, there were unequal numbers of males and females. Only two out of these top seven TLs were female. Most of the interviewed participants were male. In one respect, the study’s results from interview responses leave out perspectives from a large chunk of potential citizen reporters who can become aware of suspicious activity (The 2010 U.S. census data found that women make up 50.8% of the population). However, this low number of females in our sample (2 out 7 female TLs, 28%) is comparable to the fact that sworn law enforcement is heavily male-dominated. In fact, our numbers reported here are higher than the national averages. Only 13% of sworn law enforcement personnel are women (National Center for Women & Policing, 2002) and only 14.8% of Federal officers with arrest and firearm authority are women (Reaves & Bauer, 2003).

4.3 HatChase: Planning

Several conditions and limitations shaped the study. These can be grouped into administrative concerns and experiment concerns.

4.3.1 Administrative concerns

Although the experiment was to “mimic” an emergency event, HC-1 organizers were limited in the ways they could actually execute the experiment. First, the experiment was as controlled as

¹ Reddit.com is a social news website where users submit content. Other users can then “vote the content up” (positive) or “vote it down” (negative) to appear in the general page or individual pages. Registered users can also subscribe to or create their own individual “subreddits” within the general pages. In the case of Team 64, the team was formed out of a “subreddit” community.
possible and held solely within the University campuses. Second, organizers worked with University police and were careful not to actually create a public disturbance. Third, in order to respect the campus and the students’ need for rest, the challenge only ran during the day. Fourth, the challenge was run at a time when there were few other major events on campus (i.e., classes just ended, but finals had not yet begun), in order to maximize student involvement. Lastly, Institutional Review Board (IRB) constraints were considered throughout the study: our study participants were limited to University students and no outside participants were permitted, any communication data submitted were required to be anonymized by team leaders, and researchers could only ever have direct contact with team leaders and not team members.

4.3.2 Experiment concerns
The experiment goals and outcomes of the study guided the design of the challenge rules. First, researchers considered the simulation of participants making formal reports of suspicious activity to local law enforcement. An official challenge website was then created for participants to report their sightings. In order to access the reporting portion of the site, participants had to login with their standard University-affiliated username and password. This is common practice among affiliates-only University websites. The event website utilized the University Central Authentication Service (CAS) a single sign-on solution that allows any web service hosted on University servers to verify the NetIDs of members of the University community. By verifying the NetIDs of participants attempting to log on, the number of sighting reports that they could make was limited. However, again due to IRB protocols, the HC-1 website only ever received, stored, and checked for duplicates using a secure one-way hash of the user credentials, which researchers received in already-encrypted form from the University CAS servers. Figure 1 shows the CAS sign-in screen, the first step towards reporting a sighting.

![University CAS login screen](image)

The day before the HC-1 competition was to begin, each team leader was mailed a passcode that they could give to their team members and others. These passcodes were relatively easy to remember but also relatively secure. Examples include “banana09”, “pingpong28”, and “ancient25”. Once in the system, participants who reported a sighting would use this code to count their sighting in the team totals for the team assigned that particular passcode. In this way, researchers were able to correlate individual sightings with a team, without having to know anything about the identity of the participant making the sighting, which was a stipulation of the IRB protocol. This functionality also eliminated the possibility of participants making false reports in the name of other teams in an attempt to submarine their precision performance.
To be sure that some of the hats were found, and yet to ensure sufficient differentiation among teams’ results to allow for comparison, some hats were relatively stationary and easy to locate while others were difficult to find or relocated once during the sighting period.

Third, in order to satisfy the goal related to dissemination, teams were required to find unusual hats (locate “suspicious activity”) and to spread the information to as many people as possible (disseminate awareness of “suspicious activity”). Verification of the dissemination was also a concern for us.

Fourth, teams needed to understand that reporting false positives counted against them in the performance assessment. This addressed Goal 3 regarding strategies for limited false reports.

Lastly, any digital communication by teams amongst themselves throughout the event gave us insight into detection, communication, coordination, and dissemination strategies. Therefore, teams were required to submit reports with breadth (reflective of as many communication technologies as they used) and depth (detailed content of any team communication) or transcripts of team communication during the event, for consideration in judging. Figure 2 below is an example of submitted team data. Under the IRB-approved design the team was responsible for anonymizing the message, by hash-coding the users’ identifications before submitting the data to the researchers.

![Sample of anonymized data (text message conversation)](image)

Figure 2: Sample of anonymized data (text message conversation) submitted by one of the teams.

### 4.4 HatChase: Execution

Due to delays in the IRB approval process, the HC-1 was run on an extremely tight timeline. The study occurred at the end of the semester, when participants were preparing for finals or about to leave campus. This presented a difficult deadline and a very tight window for executing the study. HC-1 was scheduled to run over 24 hours, stretching from Monday, May 2, 2011 to Tuesday, May 3, 2011. These days occurred just after classes ended but before final exams began on May 5, 2011. It was hoped that this would allow for maximal levels of participation for a large number of possible participants.

#### 4.4.1 Phase 1: Promotion
During the time between IRB approval on April 18 and May 1, 2011, promotional efforts were conducted to encourage participants to sign up as team leaders and to recruit teams. Promotional efforts included solicitations on a number of University mailing lists, announcements made in classes around campus, flyers, handbills, a news release, advertisements in the campus newspaper, and others. The promotions period – despite its somewhat truncated timeline – was considered a success: In all, there were 62 teams registered by the time the team sign-up period ended. Promotions directed team leaders to sign up at a website created by the investigators. A screen shot of the website appears in Figure 3.

![Figure 3: HatChase website prior to the competition](image)

4.4.2 Phase 2: HatChase Competition
As already noted, team leaders organized individual groups as part of the HC-1 competition. Over the course of 24 hours, the groups were to find a number of hats spread out over the University campuses. Team leaders were asked to organize a team to find as many of the hats as possible, and then have their team (or anyone else they could recruit) report those sightings on the official website. As noted above, they agreed to submit anonymized versions of transcripts of any communications their team made through digital media. (This is the only way the investigators could collect this data and still adhere to IRB protocols). Essentially, then, there were four judging criteria:

1. Number of hats found
2. Number of correct sightings made
3. Number of incorrect sightings (false positives) made
4. Quality and quantity of transcript data

The judging criteria are useful to understand the execution of the challenge because researchers needed to consider balanced “difficulty levels” of hat placements. If hidden too well, teams may simply give up and no data would be collected. If hidden too poorly, every team would find every hat, and researchers would have no differences in values for judging criterion 1 (above), which would also hurt our data collection. We decided that a balance should be struck, so that some hats were located in heavily trafficked areas (near a major dining hall, for instance) while some were located far more out of the way places (behind a staircase in the lobby of the marine
A second consideration raised in the Planning section was the need to encourage participation over the course of the event, while balancing this with the ability to verify hat sightings. If the hats stayed still for the entire 24 hours that the challenge ran, it would be quite easy to verify correct and incorrect locations in the sightings submitted to the website. However, teams might quickly grow bored, or same maximum-score bunching issues discussed above may arise. On the other hand, if the hats were constantly on the move, it would be all but impossible to reliably verify if sightings made at a given time indeed correctly reported the location of the hat at that time. The compromise reached was that the hats would remain stationary for 3-hour shifts, and then move to new locations. There would be three such shifts throughout the challenge. This, too proved an effective compromise, as it kept teams involved throughout the entire 24-hour run of the challenge – which in turn increased the data collected – while at the same time making verification easy: when reporting a sighting, participants were simply asked if the sighting occurred during shift 1, 2, or 3. A full version of this schedule appears in Table 2.

<table>
<thead>
<tr>
<th>Hat</th>
<th>Day 1: 12pm - 3pm</th>
<th>Day 1: 3pm - 6pm</th>
<th>Day 2: 9am-12pm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Student Center 1</td>
<td>Library 1</td>
<td>Library 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Student Center 2</td>
<td>Class Building 1</td>
<td>Dining Hall 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Student Center 3</td>
<td>Dining Hall 1</td>
<td>Student Center 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dining Hall 1</td>
<td>Library 2</td>
<td>Student Center 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Library 1</td>
<td>Student Center 2</td>
<td>Student Center 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quad 1</td>
<td>Student Center 1</td>
<td>Class Building 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Student Center 4</td>
<td>Class Building 3</td>
<td>Class Building 1</td>
</tr>
</tbody>
</table>

Table 2: Hat location schedule
The constraints of “team leader only” communication had the added advantage of allowing teams to recruit new members on an ad hoc basis. Had we required all members of a team to register with the site before (or even during) the challenge, it would have made it difficult for teams to recruit new members on the fly. Several teams, in fact, utilized this tactic by asking nearby strangers to log onto the site and make secondary reports for their team. By permitting this type of activity, we were able to gain additional data about recruitment, coordination, and dissemination tactics. As mentioned within Experiment Concerns, this functionality did not, however, eliminate the potential problem of spamming the site with correct positive sightings.

The next step was to complete the sighting form on the HatChase website. In order to discourage guessing, a number of false positive, or “dummy” hats were displayed in addition to the seven correct hats actually in play. The page also asks for descriptive information about the hat wearer, similar to what a first responder investigating an emergency might ask about a suspect: specifically, age, gender, and clothing. This was added to further decrease the likelihood of someone randomly making a correct guess, to add another layer of difficulty for reporting, which would presumably add greater variance in reporting scores. This would make the data more useful, and also add some real-world-inspired external validity. The final element the sighting form requests is whether the sighting being reported was actually seen by the reporter, or was relayed to the reporter. This was added as a way to explore the ways in which sightings are disseminated, and also study the organization and nature of the teams. Figure 4 shows the full sighting report form.

4.4.3 Phase 3: Judging
A panel of judges was convened to review the results and to determine a winner, using the four judging criteria discussed earlier (number of hats found, correct and incorrect sightings made, quality and quantity of transcript data). The panel of judges included several researchers as well as expert participants from the University police department, the New Jersey Office of homeland Security Protection, and the U.S. Department of Homeland Security.
In preparation for the judging, a weighting formula was developed to include several aspects of the dissemination objective. The concern is to increase the credit for accurate reports. The resulting formula assigned: +7 points for a correct hat sighting (type and place), and +1 point each for correct age, gender, and shirt color of the hat-wearer. This provides a maximum possible score of 10 for each report. Figure 5 in the next section plots each of the top seven teams based upon their performance in terms of number of correct sightings found (horizontal axis) and calculated reporting score (vertical axis).

4.4.4 Phase 4: Interviews with participants
The researchers conducted a total of ten semi-structured interviews with HC-1 participants; seven team leaders (TLs) and three team members (TMs). Again, with the restrictions of the IRB protocol, researchers were prevented from making ongoing and persistent contact with TLs and TMs. In fact, TMs could only be indirectly contacted through the TLs. Two members of the research team conducted the interviews. All interviews were conducted over the phone and were audio recorded. Based on the team responses and submitted team data, team summary reports were created.

5 RESULTS
There were 25 teams in the entire competition that reported at least one sighting. In all, there were 4,330 reports made. On average, each team made 8 of the possible 21 sightings locations (7 hats times 3 locations, one in each shift). On average, each team made 150 reports, or 18.75 per hat. The top 8 teams, on which the judges focused, of course performed better. On average, they found 13.5 hats and made 378 reports, or an average of 28 reports per hat.

5.1 OBJECTIVE 1: DIGITAL MEDIA STRATEGIES TO COORDINATE EFFORTS
Findings from the semi-structured interviews and submitted team reports confirmed which communication technologies the teams used for coordination and monitoring. See Table 3 for the communication tools used by each team.

<table>
<thead>
<tr>
<th>Team ID</th>
<th>64*</th>
<th>43**</th>
<th>29***</th>
<th>11</th>
<th>41</th>
<th>46</th>
<th>54</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone calls</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Text messages</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Picture messages</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Emails</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Online chat messages</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>GroupMe</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Facebook</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Twitter</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>YouTube/video sharing</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Google Voice</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Shared Google Document</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Flyers</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

* 1st prize winner, ** 2nd prize winner, *** 3rd prize winner

Table 3: Communication used during search/monitoring for hats
5.1.1.1 **Mobile phones**
All teams used mobile phone technology to communicate. During the search for hats, text messages and picture messages were the most common strategies used for updating each other with information, direction, and questions. However, if something was urgent (e.g., time was running out), some teams made telephone calls.

5.1.1.2 **Social Media**
The top seven teams used Facebook and/or Twitter in some capacity to request help from others (i.e., teams requested friends be aware of sightings and/or petitioned them to report sightings). However, teams never “recruited” (in the traditional meaning of the word) additional members to join their teams. Rather, teams asked friends for help reporting and/or information but did not ask them to officially join the team and share in the monetary prize. Not much social media data was generated during the experiment outside of the messages created and facilitated by the organizers themselves. The teams submitted very sparse social media data in their communication reports. The interviews revealed that these reports were incomplete, and that team leaders often used social media to monitor announcements from HC-1 organizers and to monitor activity on the part of other teams.

Given that sightings were crucial in winning the competition, it is not surprising that teams were careful and selective about sharing and speaking of sightings. Team leader TL-29 explicitly told members not to share information with roommates or outside friends. TL-29 said, “If you hear about them joining an outside team, then don't ask them to enter in information.” TL-29 looked at the Facebook (hereafter, FB) page of the HC-1 organizers but was careful not to post. Similarly, TL-11 was concerned some friends were on other/own teams, “We can’t just tell all of our friends. If your social network is divided that kind of hinders your chance … you have to be more selective and careful.”

Additionally, the experiment’s rules seemed too complex to be efficiently shared over social media. Analysis of the reports showed that five of the seven top teams (Teams 11, 29, 43, 46, 64) created their own shortened descriptions of the already summarized FAQ section from the HC website. Teams’ descriptions went beyond the 140-character limit for a Twitter post and were never reported as posted through a FB “wall” message. Rather, these descriptions were sent via FB group message boards, FB inboxes, and emails.

TL-43 said that the use of social media to share details of the event was difficult. Face-to-face meetings with friends and even strangers had better outcomes, since the team could explain the project and convince people to login and actually input the information. TL-43 said, “Getting people to report through Facebook or Twitter was way too complex, and they (external reporters) didn’t really know why [they should report].”

From an emergency simulation perspective, the experiment design did in fact induce fast and accurate detection of strange activity. However, core team members seemed to feel the urgency more significantly and “realistically” than did the secondary reporters. Such reporters often reported sightings as “favors” to teams and/or motivated by personal financial gain.

5.1.1.3 **Google Voice**
Uniquely, Team 11 was the only team that used email and Google Voice during the search period. Team 11 set up a Google Voice phone number and Google email address (which they promoted through flyers and Facebook) for anyone to contact in the event they found a hat. The setup functioned similarly to an “emergency hot line.” According to Team 11’s communication report, they found that “outsiders” (people not on the immediate team) reported the most tips during the first session and the lowest amount during the last session. The team speculated that this was based on “convenience” to external searchers, who reported sightings because they “naturally” came across the sighting, than actively searching.

5.1.1.4 GroupMe
Other than traditional text messaging, two groups (54, 64) used GroupMe, a group text messaging service that allows all users to send and receive text messages via a single phone number. However, TL-64 (with 16 members) reported that group texting created some confusion because hundreds of texts occurred at once. This group texting strategy is comparable to receiving emergency updates and questions every second. TL-64 said, “There were definitely people checking into places [to search for hats] that other people had already checked.” Analysis of Team 64’s submitted communication transcripts confirmed that consecutive text messages about multiple topics caused confusion among members:

- TM-A: This is a bit confusing, should everyone be submitting these hats on the website?
- TL-64: I am compiling a list, we can submit later.
- TM-A: Oh ok
- TM-B: Yes, submit them all on the website
- TM-C: do we have anything from library for this time slot?
- TL-64: Yes.
- TM-D: nothing in bottom floors of x y or z
- TM-E: I also checked x and y. Where are you headed next?

The TL-64 sifted through all the text messages at the end of the search day and consolidated a list of sightings to be emailed among the team. As a winning TL, he said beyond setting up the GroupMe and money distribution, “I didn’t really have to do much.” However, he admitted the group texting could have used more active moderation and leadership.

5.1.1.5 Vimeo Video
One team (Team 11) created an online instruction video with steps to report a sighting. According to Team 11’s report, their goal was “to make the login process as quick and easy as possible for those logging in, especially because they are doing a ‘favor’ for us.” Team 11 believed that face-to-face recruitment to help in the activity was the most “productive.”

5.2 OBJECTIVE 2: EFFECTIVE STRATEGIES FOR DISSEMINATING & REPORTING
Three of the top teams (Teams 41, 43, 46) asked friends and appealed to their social networks to report sightings. However, these teams found that the time and effort necessary for making reports was cumbersome and annoying to their friends. Therefore, they reported entering sightings on their behalf. Team 43 consolidated TMs login information and had a “kiosk” person log-in sightings on behalf of all members as sightings were found. Then, the team recruited individuals independently to input information. Team 11 created instructional videos and Google

2 Names of locations were removed.
Document intended to share instructions and sightings. According to TL-11, about 500 people (some of which were part of Teams 43 and 64) viewed the Google doc. However, they were uncertain whether people actually logged in on their behalf. Team 29 petitioned fraternity brothers to enter in sightings, and asked its members to sit down with friends and login information with them. Team 54 also petitioned the help of friends through phone calls and mass text messages. Similarly, Team 64 members reported sightings for themselves and requested help from their personal networks.

<table>
<thead>
<tr>
<th>Team ID</th>
<th>64*</th>
<th>43**</th>
<th>29***</th>
<th>11</th>
<th>41</th>
<th>46</th>
<th>54</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face-to-Face</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Phone calls</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Text messages</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Picture messages</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Emails</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Online chat messages</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>GroupMe</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Facebook</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Twitter</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>YouTube/video sharing</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Google Voice</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Shared Google Document</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Flyers</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 4: Communication used during dissemination of hat sightings

5.2.1 Dissemination Workarounds
While all teams petitioned friends and social networks to report sightings into the HC-1 website, some (Teams 41, 43, 46) openly reported during interviews it was much “easier” and less “annoying” to request login information, so teams could input sightings using the identities of those who shared passwords with them. While this strategy generated more reports towards the teams’ scores, this subverted the real-world goal of disseminating and increasing person-to-person awareness of emergency information. Sharing personal information was beyond our control and can be compared to reports made to authorities under false or misleading identities. Table 4 shows the different strategies teams used to disseminate information about hat sightings to other people so that they could log-in and report a sighting on the team’s behalf.
There is a remarkable difference in terms of the performance here, with some teams (43 and 64, for instance) finding almost all the hats, while other teams (like 29) finding far fewer hats but making many more reports. These differences can be more clearly seen in Figure 5, which presents this data in Table 5 for the top seven teams in terms of hats found.

<table>
<thead>
<tr>
<th>Team ID</th>
<th>Correct hats found</th>
<th>Correct reports made</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>64*</td>
<td>17</td>
<td>529</td>
<td>5021</td>
</tr>
<tr>
<td>43**</td>
<td>16</td>
<td>540</td>
<td>5258</td>
</tr>
<tr>
<td>29***</td>
<td>9</td>
<td>762</td>
<td>7337</td>
</tr>
<tr>
<td>41</td>
<td>15</td>
<td>348</td>
<td>3360</td>
</tr>
<tr>
<td>46</td>
<td>14</td>
<td>122</td>
<td>1148</td>
</tr>
<tr>
<td>11</td>
<td>15</td>
<td>133</td>
<td>1251</td>
</tr>
<tr>
<td>54</td>
<td>12</td>
<td>357</td>
<td>3465</td>
</tr>
</tbody>
</table>

* 1st prize winner, ** 2nd prize winner, *** 3rd prize winner

Table 5: Hats found, reports made, and reporting score for top seven teams

The judges also calculated a difficulty score for each hat based upon the number of teams that found it. Each report could then be weighted in terms of its difficulty. Table 6 contains this data. Again, team 29 does well in this metric, suggesting that in addition to making many reports, they also tended to make reports about the more difficult to find hats, which is interesting.


<table>
<thead>
<tr>
<th>Team ID</th>
<th>Aggregate report difficulty score</th>
</tr>
</thead>
<tbody>
<tr>
<td>64*</td>
<td>493.9</td>
</tr>
<tr>
<td>43**</td>
<td>491.7</td>
</tr>
<tr>
<td>29***</td>
<td>696.3</td>
</tr>
<tr>
<td>11</td>
<td>313.3</td>
</tr>
<tr>
<td>41</td>
<td>114.6</td>
</tr>
<tr>
<td>46</td>
<td>122.3</td>
</tr>
<tr>
<td>54</td>
<td>329.5</td>
</tr>
</tbody>
</table>

* 1st prize winner, ** 2nd prize winner, *** 3rd prize winner

Table 6: Aggregate reports made difficulty score for top 7 teams

The judges also took into account false reports, which was a major point of emphasis for expert members of the panel from law enforcement. To examine this, the researchers calculated an average report precision score for each team (the number of correct reports divided by the number of total reports). This precision score was also taken into account when judging each team’s performance. Figures 6 and 7 plot the top teams in terms of hats found and report score, respectively, on the horizontal axes and precision score on the vertical. It is interesting to note how some of the top teams in terms of hat sightings – such as teams 64 and 11 – did relatively poorly in precision of hat reports. On the other hand team 29, which clearly focused on reporting over sighting hats, had remarkably good precision in their reports.

Figure 6: Reporting precision of top teams in terms of reports made
5.3 OBJECTIVE 3: STRATEGIES FOR LIMITING FALSE POSITIVE REPORTING

All of the top seven teams, with the exception of 64 and 29, recruited close friends and family members. Some teams (Teams 43, 41, 54, 11, 46) stated that they intentionally kept the number of team members low to increase the amount of prize money per person and have trustworthy others.

5.3.1 Sabotage!

Two teams (Teams 11, 43) consolidated sightings with Google Docs, however, only Team 11 made those sightings viewable to the public. Again, although Team 11’s Google document was reportedly viewed by almost 500 people, they were uncertain of “who” those individuals were. Analysis of the reports and interview responses showed that two teams (Teams 43 and 64) had actually intercepted this information, suggesting the viral nature of social media and power behind online surveillance.

The TL-43 said the team was concerned this was a “decoy document,” but noticed this team had three more hat sightings than they did. Therefore, they first compared and verified the similar sightings both teams had. Since 15 out of Team 11’s 18 sightings matched Team 43’s sightings, Team 43 assumed the three additional sightings as correct, and began to enter in these additional sightings under their own team password. Additionally, Team 43 obtained the other team’s password and entered in false information and bogus sightings on their behalf. Interviews with Team 11 showed they were not aware of any infiltration. TL-11 said that they discussed the possibility of sabotage, but that there was no certain way to prevent it. Instead, they released information via a Facebook group message towards the very end to prevent other teams from sabotaging their sightings or abusing access to their password.

In order to further investigate the ability of each team to limit incorrect reports, the reliability of the reports of each team was considered by the judges. For each team, a calculation was made of the number of correct reports made for each hat found. In addition, a similar calculation was
made of the number of incorrect reports made for each hat found. The ratio of these values was calculated as a “sureness score.” It is a measure of reliability that rewards true positive reports and punishes false positives. Table 7 shows the results of these calculations. Again, Team 29 – the team that focused on reporting over finding hats – did far better in terms of the reliability of its reporting than any of the other teams. In other words, the data from Team 29 demonstrate a far stronger likelihood that the reports team 29 made were correct. However, it must be taken into account that the utility of this information is limited by its scope: Team 29 found far fewer hats than did Teams 43 and 64.

<table>
<thead>
<tr>
<th>Team ID</th>
<th>Correct reports per hat</th>
<th>Incorrect reports per hat</th>
<th>Sureness score</th>
</tr>
</thead>
<tbody>
<tr>
<td>64*</td>
<td>15.6</td>
<td>1.0</td>
<td>15.6</td>
</tr>
<tr>
<td>43**</td>
<td>20.0</td>
<td>0.8</td>
<td>25.7</td>
</tr>
<tr>
<td>29***</td>
<td>36.3</td>
<td>1.1</td>
<td>33.1</td>
</tr>
<tr>
<td>11</td>
<td>10.5</td>
<td>1.7</td>
<td>6.3</td>
</tr>
<tr>
<td>41</td>
<td>7.6</td>
<td>0.1</td>
<td>61.0</td>
</tr>
<tr>
<td>46</td>
<td>4.7</td>
<td>1.9</td>
<td>2.5</td>
</tr>
<tr>
<td>54</td>
<td>14.3</td>
<td>2.5</td>
<td>5.8</td>
</tr>
</tbody>
</table>

* 1st prize winner, ** 2nd prize winner, *** 3rd prize winner

Table 7: Top five teams in terms of sureness score

In the end, the judges selected the following teams as winners:

1. First place: Team 64
2. Second place: Team 43
3. Third place: Team 29

Figure 8 below compares the numbers of hats found and the number of reports made for each of the teams. This graph again demonstrates the differing strategies taken by teams. Teams 43 and 64 clearly sought to maximize the number of hats found, and very nearly found them all. Team 29, on the other hand, sought to maximize reporting, and made around 200 more reports than either Team 43 or Team 64. Teams 54 and 11 did worse in the number of hats found than Teams 43 and 64 and also worse on reporting than Team 43.
Figure 8: Number of sightings and reports made by each team

Figure 9 below compares the number of hats found and sightings reported for each of the teams in a different way. On the horizontal axis is the number of hats found by the team, while on the vertical axis is the number of reports made per team member class. The two classes analyzed here are the actual team members identified by the team leaders (in blue) and the total number of people who submitted reports for that team (in red). Many teams recruited people to make reports for them, though some recruited more than others. Figure 9 illustrates the difference.

Figure 9: Number of reports made per actual team member and per individual associated with a team by number of hats found.

Team 29, for instance had very similar values for sightings per team member and sightings per team associates, implying that nearly everyone who reported sightings for them was a member of
the team. Given the large number of sightings they made, this may have been an effective way to leverage a large team. As such, if the commitment required to join the team was low (i.e. merely filling out the sightings on the website) then it might be easier for team leaders to convince people to join their teams. On the other hand, if the requested commitment involved hunting on foot and in-person for people in hats, it might be more difficult to convince prospective team members to join.

Teams 11, 43, and 54 have a wide disparity between reports per team member and reports per team associate. This implies that the actual team is either very small, or the team recruited a large number of people to make sightings, or both. These teams fell in the middle of the pack, and none of them scored either the most sightings or the reports. However, this large divide between sightings per member and associate is fairly common, implying that it was a typical strategy to employ a small number of team members to do most of the coordination and actual hat sightings, while they would recruit a large outside group to do the reporting. Given the mediocre performance of these teams, this would appear to be a weaker strategy. This strategy puts a heavy burden on the primary team members, and does not leverage the power of crowdsourcing in a meaningful way. That is, these teams did not outsource search tasks to a large network of people and distribute the weight or responsibility of the work. Rather, they placed responsibilities of searching and reporting upon themselves. Although this meant greater monetary payoffs per team member, this also meant more labor-intensive efforts per team member. In fact, Team 43 won second place with $2000, but distributed the work among only eight members ($250 per person). Meanwhile, Team 64 won first prize of $4000 but distributed the prize among 16 members (roughly $208-$240 per person with a $15 “bonus” for spotting a hat first). In terms of outcomes, members in Teams 43 and 64 won roughly the same amount of money but put in substantially different amounts of effort. However, had Team 43 won first place, they would have yielded an even larger sum of money ($500 per person).

Team 64 had roughly three times as many reports per team member as per team associate, implying that the number of associates they had was a bit less than 3 times the number of team members that they had (since in this data “team associates” includes team members). Given that Team 64 had the most sightings while also having one of the best total numbers of reports, judges concluded that they should rank first in the competition. While recruiting a team that focused on reporting rather than searching allowed Team 29 to assemble a very large team, it sacrificed searching for more hats in order to accomplish this. On the other hand, Teams 11, 43, and 54 focused more on recruiting a large number of outside helpers, their core team remained small. In the end, this compromised their ability to compete long-term, as only the small core team was fully committed to the team. Team 64, on the other hand, struck a balance between having a fairly large team and also a large group of outside associates to help, but not one that dramatically out-numbered them. These compromises led to a team that could perform strongly in both the sighting and reporting tasks.

5.3.2 Lack of data
Findings from the interviews suggested that the research interests competed with the interests of the participants, which ultimately affected the desired outcomes of the study. There was a challenge of balancing participants’ motivation to spread the word versus their motivation for money. While teams wanted to spread the reports of their sightings with trusted others, they did not want to share the prize money. In fact, six out of the seven Tls interviewed said they
intentionally kept their teams relatively small, suggesting teams were hesitant to recruit more members because that meant sharing more of the prize money. Indeed, in a true emergency situation, individuals might be motivated differently to share critical information; for instance, if the wellbeing of family and friends was at stake compared to the need for extra cash.

Although social media data were not as heavily generated as we expected in this experiment, the findings from the interviews and communication reports collected from the participants helped inform the rules and implementation for a second HatChase experiment.

6 CONCLUSION

In this competition, students developed plans, formed teams and created systems and procedures that leveraged social media to detect real-world events. Participants verified through the event website that sightings were accurate and true, shared sightings via publicly available social media communications, and petitioned personal networks for dissemination and searching assistance. The conditions of the competition also encouraged participants to filter true and false detections in order to maximize reliability and alert others to those events.

Analysis of the results informs research about the potential utility of social media as means for quick and accurate discovery, aggregation and dissemination about an “unusual event” occurring on a university campus. The experiment also studied, in an *ex post facto* manner, the ways in which social media has been used to deal with informal communication that might arise during emergencies on a college campus. This study carried this work a step further by creating a controlled simulation of an emergency situation, in order to improve both the quality and the breadth of data collected. However, social media data was barely generated as a result of this experiment, which suggests the complexity and difficulty in simulating genuine motivations for sharing urgent, emergency information publicly and unreservedly in social media. Therefore, we planned a second experiment, Hat Chase 2 with modified rules and restrictions. These were intended to require more use of social media and to provide more incentive to share information publicly, and quickly. The results of that experiment will be reported elsewhere.

Overall, the experiment demonstrated that students can self-organize in many ways, with effective results for a pre-announced event. The diversity of structures was so great that none of them emerges as a clearly preferred model strategy that should be disseminated to other campuses and groups of first responders.

7 ACKNOWLEDGEMENTS

This study builds on other work done by other AWSM project researchers at Johns Hopkins, USC, RPI, and other institutions. Also, special thanks to researchers at the Rutgers University Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA), a Department of Homeland Security Center of Excellence (2009-ST006-1-CCI002-0-3).

8 REFERENCES


9 APPENDIX

9.1 Research Protocol for HC-1: AWSM Project
This is an unusual study design in that it calls for a competition among self-forming teams of persons. The researchers will judge the performance of those teams on a challenge task, based on task performance and on examination of de-identified communications records. Those records will further be used in research on the underlying scientific questions. We propose that the researchers obtain from team leaders signed agreements regarding the conditions of the challenge, and the protection of personally identifiable information about team members. We believe that this design is either “not study of human subjects”, or eligible for exemption in Category 2.

9.1.1 Background
Social media represent a powerful new tool for peer-to-peer communication and collaboration. Recent events – like the Moscow airport bombing – have shown that oftentimes the information posted to social media like Twitter and Facebook by ordinary people at the scene of emergencies can be the best and most rapid source of information about those emergencies. Researchers at The NameOfUniversity Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA) are interested in learning how these tools can be harnessed in order to help first responders, such as police and fire fighters, respond quickly and effectively.

9.1.2 Objectives
This study is funded by a grant from the Department of Homeland Security in order to study ways of using social media to improve emergency response.

The steps of the proposed research are:
6. Create a competition that will elicit student interest, and generate new ideas, for the discovery, aggregation and dissemination about an “unusual event” occurring on a university campus. In this competition, students will form teams and create systems or procedures that leverage social media to detect real-world events, filter those detections in order to maximize reliability, and alert the team members to those events.

7. After a period of discussion on campus, and team formation, we will announce and then create a non-threatening, but readily observable event, on the NameOfUniversity Campuses, so that the teams can compete to discover the nature and location of the event (see below) and inform the team members of the event.

8. After the event, the performance of the several teams will be assessed with regard to the speed and the accuracy of their detection of the planned event. All teams will be required to submit their de-identified logged team communication records, or the most accurate possible description thereof. In the judging, preference will be given to models that include data logging as described below.

9.1.3 Subject Population and Recruitment
This experimental study involves persons who will interact directly with the researchers, in their role as team leaders. It will be their responsibility to: (a) present the team’s plan for detection and dissemination to the researchers; (b) assemble either a team or a “team formation scheme”; (c) aggregate the team’s social media communications during the challenge event; (d) de-identify all team communications prior to submitting the communication record to the researchers; (e) accept the prize award, if any, on behalf of the team. We regard these persons as the “human subjects of our study”, since we will interact with them directly. A detailed consent form, including the terms of the challenge competition, is attached.

9.1.4 Methodology
This project will be conducted on the NameOfUniversity campus. It will begin as soon as possible after receipt of IRB approval. It is anticipated that the recruitment and challenge activities will take place during the remainder (April and early May) of the Spring Semester. All data relating to this study will be destroyed on December 1, 2014.

The first phase of this study first invites students to participate in a competition that can leverage social media to accomplish some task related to the detection of emergency situations. Students might take as inspiration a related contest designed by the Defense Advanced Research Projects Agency (DARPA), the Red Balloon Challenge. In DARPA’s challenge, teams were asked to identify the position of 10 large, red balloons hidden throughout the United States. The winning submission to this contest will display a similar level of creativity, inspiration, and technical sophistication.

9.1.5 Details about the challenge.
Certain specifics of the challenge activity will not be revealed until the time of the competition, to ensure that no team has an unfair advantage, including the specific date on which the activity will occur.

On the announced day, beginning no earlier than 12 noon, some number greater than 5, but less than 9, of persons who are retained for this purpose by the research team, will augment their clothing with some easily recognizable but non-threatening and non-offensive articles of clothing. By way of example, and without limitation, such augmentation might include an extraordinary hat; a very colorful sash or poncho; etc. The challenge announcement will indicate what kind of unusual garb is to be identified. These persons will follow pre-assigned routes across the NameOfUniversity Campus, to provide a complex challenge to their detection and geo-location. They may also “disappear” for periods of time, by removing the special garments. At 6pm they will stop wearing the special garments, and they will resume at 9am the following morning. At 1pm on the second day, the challenge exercise will end. The paths to be followed by the persons to be detected will be known to, and reviewed by, the NameOfUniversity Public Safety Authority, to ensure that no false alarms are created by the research activity.

The persons to be detected will be of varying habitus and will include males and females. Accurate identification will require that the team detecting the person correctly match the garb, habitus and gender of the persons to be detected. Additional credit will be given for correctly geo-locating them with respect to the landmarks of the NameOfUniversity Campus, which may be specified informally in the team’s reports.
The research team will establish collector web sites, one for each team, to which members of the team are to report when they have been informed of the agreed upon final team answer. This will assess the speed of discovery and dissemination achieved by each team.

In addition, each team will be required to submit de-identified communications logs. The completeness and usefulness of these logs will be considered in the awarding of the first and second prizes for the competition. Instructions for de-identification follow.

9.1.6 Judging of Entries
A first prize of $4,000 will be awarded to the first place team, and a prize of $2,000 will be awarded to the second place team. The decision will be made by a panel of judges including representatives of the research project and its collaborators at other institutions (University of Southern California; Rensselaer Polytechnic Institute) and possibly persons from the New Jersey Office of Homeland Security Preparedness, and the United States Department of Homeland Security Office of Science and Technology. Prizes will be award to teams that are among the top three in speed and accuracy of discovery of the persons to be detected. The ordering of those three will be determined by examination of the completeness and usefulness of the recorded data. This consideration flows from the fact that this research is part of a larger project aimed at providing useful information about Alerts and Warnings in Social Media to the community of first responders. For this purpose, richer data sets are to be preferred to leaner ones, since in a realistic application neither the community nor the first responders will know precisely what type of unusual event is to be detected. While it is an unpleasant possibility to contemplate, experts in homeland security anticipate that the United States may well be subjected to a Mumbai-type attack by a dispersed group of armed terrorists. The present design mimics some aspects of that detection problem.

9.1.7 Flow-down of conditions ensuring data collection and protection of persons
We present here the agreement that will be signed by leaders of participating teams, in order to ensure that the proposed de-identification procedures will meet NameOfUniversity’s standards for the protection of human subjects.

Team Leaders’ Agreement to be Eligible to compete in the AWSM Challenge.

This is an agreement by and between the Manager of the AWSM Challenge research project, Paul Kantor and ______________________________ [list persons], leaders of the _____________ [Team Name] Team with regard to the competition to be held on the NameOfUniversity Campus, in Spring of 2011.

Study Description and Goals.
This study will involve the competition among self-formed teams of students, to detect a benign but unusual event on the NameOfUniversity Campus. The goal of this study is to learn more about ways of using social media to improve emergency response.

Description of Participant Activities.
You are agreeing to participate as a team leader in a study that involves: (1) forming a “detecting team”; (2) using social media to detect a benign but unusual event on the NameOfUniversity
Campus; (3) de-identifying the social communications; (4) delivering them to the research team and; (5) destroying any personally identifiable records, one week after the results of the competition are announced. You may elect to invest funds as well as time in this activity. Those funds will not be reimbursed by the research team. The winning teams will receive a cash prize as described below.

**Duration of Participation.**
The involvement of the challenge team is anticipated to include a period of approximately 4 weeks of preparation communication and software tools, and recruitment of team members. As team leaders you will choose your own level of involvement during this period. There will be one “target period” of 25 hours, that will be announced one week in advance, during which the events to be detected will occur.

**Risks and Benefits: Judging of Entries.**
Participation in this study does not entail any foreseeable risks.

Benefits are conditional on the success of the team in the challenge competition. Specifically, a first prize of $4,000 will be awarded to the first place team, and a prize of $2,000 will be awarded to the second place team. The decision will be made by a panel of judges including representatives of the research project and its collaborators at other institutions (University of Southern California; Rensselaer Polytechnic Institute) and possibly persons from the New Jersey Office of Homeland Security Preparedness, and the United States Department of Homeland Security Office of Science and Technology.

Prizes will be awarded to teams based on the speed and accuracy of detection, effectiveness of dissemination, and the completeness and usefulness of data.

**Freedom to withdraw from the study at any time without any penalty.**
Your team at any time, elect to withdraw from the study. However, if you withdraw prior to the judging, your team is not eligible to win a prize.

**Number of Participating Teams.**
The number of participating teams cannot be predicted in advance of the study but it is anticipated to be more than 2 and less than 10.

**Eligibility to Win**
To be eligible to win any of the prizes in the AWSM Challenge, you must submit a complete and de-identified log of all of the electronic communication among your team members in the course of the challenge. Of course, if people communicate by shouting to each other across the campus, there will be no record. In addition, you are not to record voice communication by telephone or VOIP, as such communications are strictly protected by state and Federal regulations. Therefore, you will only be required to submit logs of your electronic communications, capturing your use of social media such as Facebook, Twitter, and others. **You must prominently warn all persons participating in your team, that their communications regarding the AWSM Challenge will be captured, de-identified, and submitted to the researchers. Please use exactly the**

Initials: ____________

*This informed consent was approved by the Name of University Institutional Review Board for the Protection of Human Subjects on 3/16/2011; approval of this form expires on 3/15/2012.*
Notice to Participants
The following warning has been judged satisfactory by the NameOfUniversity Institutional Review Board for the Protection of Human Subjects. We strongly suggest that you use it exactly as stated here, in all recruitment materials, and, if possible, displayed on any web sites or other social media tools that you may choose to use.

All communications that you generate as part of the [Team Name] Team activity for the AWSM Challenge will be logged by the team leaders. Thus the team leaders will, in principle, be able to know any messages that you send as part of the [Team Name] Team activity for the AWSM Challenge. The leaders will de-identify all of those messages so that they cannot in any way be linked to you, before releasing the data to the AWSM Challenge researchers and judges. If you have any questions about what this means in more detail, you may contact the team leaders at:

Name       Contact Information [each team must provide its own list].
Name       Contact Information [each team must provide its own list].
Name       Contact Information [each team must provide its own list].

Method of De-identification may be chosen by the team
For each distinct person who participates in your team, you must generate a hash-coded version of that person’s name, using a process that cannot be decoded. For example, you might use the MD5 algorithms that are built into the Python language. It is extremely important that if the same person communicates using several login names, the same hash-coded version must be assigned to all of that person’s communications. You do not need to report which algorithm you used to hash-code the names, and should not provide any information that would enable the researchers to accidentally discover which real person a given hash-coded name corresponds to.

Data may not be used for any other purposes, and must be destroyed.

As a team leader you promise not to use the data for any kind of research (that is, any effort to find generalizable knowledge). You must further promise not to use it to embarrass or otherwise discomfort any members of your team. And, finally, you must promise to destroy the information within one week of the announcement of the outcome of the competition, by the judges.

Confidentiality And/Or Option To Be Named
Unless you specifically elect to be named as a team leader in this study, your name will be kept confidential by the researchers. If you wish your name to be released, in the case that your team wins one of the prizes, you will have an opportunity to authorize that release.

Signatures:
For the ________________________ Team
Leader: ______________________ [Printed name] Signature: ______________________
9.1.8 Provisions for Protection of Private, Identifiable Information
We have devised a two-stage procedure as described above, to ensure that the RESEARCHERS do not have any contact with private identifiable information about any of the persons on a given team except for designated team leader(s) who report the team name, receive information about the aggregator site to collect information about dissemination, and who will receive and further distribute, according to their teams rules, and prize moneys.

Data collected in this study will be analyzed by teams of researchers cooperating with the NameOfUniversity research team, but they will only have contact with the completely de-identified data, as described above.

Due to the nature of Social Network Analysis, reports on this work may identify individuals with a specific network role in the network (e.g. aggregation point; discovery node; etc.) but there will be no possible way to associate those roles with natural persons.

9.1.9 Exemption Justification
We have worked hard to define a process which aggregates an adequate amount of information to support the research goals of the project, but does so in a way that makes it impossible for the researchers to associate specific actions or messages with specific individuals. We recognize that in the course of the research that is proposed, some students will have access to communications
generated by other students, in such a way that their identities can be known. This is, in fact, an essential component of team organization, if the prizes are to be divided among team participants in a way that effectively incentivizes effective participation. We believe that this sharing of information will be entered into in an entirely voluntary fashion by the participating members of any team, and represents the type of information sharing that modern Americans find acceptable in many settings.

To ensure that OHSP guidelines are followed, we will require of team leaders a commitment to (a) not use the data for research and (b) destroy it within one week of the completion of the competition. We believe that this represents a reasonable level of diligence to protect team members from any negative consequences of their participation.

In sum, we believe that members of teams are not “research subjects” in the customary understanding of that term. We consider it possible that it could be deemed to be “research not with human subjects” but we understand that such decisions are made at the discretion of the IRB.

We believe that if it is deemed to be research with human subjects, that exemption 2 is applicable, since the activities of observing and communicating are, arguably, “public behavior” and we are, in fact, not observing persons engaging in those activities, but only examining de-identified communications generated by those persons.

Therefore we request either a decision that this is not research involving human subjects, or exemption from IRB review under category two.

9.1.10 Risks and Benefits
Risks: There are no foreseeable risks to participation in this study.

Benefits: A cash prize of $4,000 will be awarded to the team that is judged to have won the competition. A cash prize of $2,000 will be awarded to the team that is judged to have ranked second. Whether and how the leaders of the team will distribute that money to the participants on their team— or to some subset of those participants – is part of their design criteria and is not something under the control of the researchers.
9.2 Research Protocol for HC-1 Interviews: AWSM Project

9.2.1 Principal Investigator
Dr. Mor Naaman
School of Communication & Information, Room 305
4 Huntington Street
New Brunswick, NJ 08901
732-932-7500x8284
mor@NameOfUniversity.edu

9.2.2 Summary
The research involves interviewing the team leaders and team members who participated in a competition among self-formed teams of students to detect a benign but unusual event on the NameOfUniversity Campus (“The Hat Chase”).

9.2.3 Objectives
The goal of this research is to learn more about the ways social media can improve emergency response.

9.2.4 Subject Population and Recruitment
The researcher will ask the competition organizers to email the team leaders and ask them to contact the research team for an interview. The researcher will then ask those team leaders to reach out to their teammates ("snowball" recruitment) for an interview. Participants must be 18 years old or older to be included in the study. It is likely that team leaders and their team members will come from diverse backgrounds and from various roles at the University (undergraduate students, graduate students, etc.). However, specific interviewing procedures will be implemented and explicitly state that all participants may opt out of the interview at any time without any penalty to them.

The recruitment and analysis phase will occur over a year’s span. All data (notes, drafts, lists of subjects, tapes, computer disks, etc.) will be retained up to three years and then destroyed through a thorough shredding process upon publication of study results.

9.2.5 Consent Procedures
For in-person interviews, the interviewer will explain the study to the subject, the consent will be read, and the subject’s questions answered. The subject can opt to sign a consent form or provide oral consent. If they would like to sign a consent form, he or she will initial all pages, and then sign the consent form. A dated and signed copy will be given to the subject. For instant messaging and online chat-based interviews, the interviewer will email the Consent Form to Participate in the Research study to the participant prior to the interview. Within the chat box, the interviewer will ask if the participant has read, understood, and agrees to the terms in the consent form. The interview will commence only if the participant agrees. The subject’s questions will be answered. For telephone-based interviews, the consent form will be emailed to them prior to the interview. The script for telephone and audio recording consent will be read to them, explaining
the study to the subject and asking for their consent. Their questions will be answered. If they agree to participate in the study, the interviewer will continue with the questions. If they do not agree, the interviewer will immediately hang up the phone. The participants can opt out of the study at any time without any penalty to them.

9.2.6 Potential Benefits
Upon completion of the study, each participant will receive $20 gift card compensation. However, their participation may help us better understand ways of using social media to improve emergency response.

9.2.7 Potential Risks
Since it is confidential, there are no foreseeable risks to participating in this study. The subjects’ participation is completely voluntary. As such, subjects only have report or track information or feelings to which they feel comfortable answering. They can choose not to participate at any time during the study without any penalty and their interview answers will be deleted and destroyed immediately.

9.2.8 Protection of Subjects/ Private and Identifiable Information
As stated previously, the data is collected from interviews conducted by the researchers. We will only interview users who have provided permission to allow researchers to ask them questions regarding their participation in the AWSM Challenge.

Interview responses will be coded with a numerical identifier and then transcribed accordingly. The respondents’ team data will receive the same numerical identifier. Participants’ names will appear only on a list of subjects, but will not be linked to the code number that is assigned to responses or recordings.

The recording(s) will be used for analysis only by the research team. All drafts of findings will not include identifying information of participants.

The recording(s) will be stored in a locked file cabinet and will be retained up to three years and then destroyed upon publication of study results.

9.2.9 Analysis and Methodology
We plan to interview Hat Chase participants and ask them questions regarding their overall experience of the event, their use of social media, and their general communication practices. Researchers will identify major themes and patterns which will manifest themselves based on the responses from the participants.

9.2.10 The Risk/Benefit Ratio
This is a minimal risk study since subjects’ participation is completely voluntary and may opt out at any time. A direct benefit to participating in this study will be $20 compensation.

Again, participants can choose not to participate at any time during the study without any penalty and their interview answers will be deleted and destroyed immediately.
The participation in this study will help researchers learn more about ways of using social media to improve emergency response.

The risks of harm anticipated in the proposed research are not greater, considering probability and magnitude, than those ordinarily encountered in daily life as the data involves their everyday. Since the study is confidential, there are no foreseeable risks to participating in this study. Participation is completely voluntary. Participants may withdraw at any time during the study without any penalty and interview answers will be deleted and destroyed. Participants only have to answer the questions they feel comfortable answering. All participants can choose not to participate without any penalty.

9.3 Consent Form to Participate in a Research Study
Title of Study: Interviews with HatChase Participants

Principal Investigator: Dr. Mor Naaman, Assistant Professor

9.3.1 INTRODUCTION
You are invited to participate in a minimum risk research study, conducted by NameOfUniversity Assistant Professor, Dr. Mor Naaman in the Dept. of Library and Information Science. Before you agree to participate in this study, you should know enough about it to make an informed decision. If you have any questions, ask the investigator. You should be satisfied with the answers before you agree to be in the study.

9.3.2 BACKGROUND/PURPOSE
The purpose of the study is to gain information about ways social media can be used to improve emergency response.

9.3.3 INFORMATION
To participate in this study, you must have been a team leader or a team member in the AWSM Challenge (also known as “Hat Chase”). You must be at least 18 years old to participate in the study. All you need to do is answer some questions, which should take about 30 minutes, depending on the length of your responses. Questions will ask about the communication tools you used during the event, including Facebook, Twitter, email, and text messaging.

If you agree to take part in the study, your responses will be kept and your responses will be coded with a number. Your name will appear only on a list of subjects, but will not be linked to the code number that is assigned to your recording(s) or data provided.

9.3.4 RISKS
Since it is confidential, there are no foreseeable risks to participating in this study. However, your participation is completely voluntary. You can choose not to participate without any penalty to you. If you do choose to participate, you may withdraw at any time during the study without any penalty and your interview answers will be deleted and destroyed. You only have to answer the questions you feel comfortable answering.

9.3.5 BENEFITS

Subject’s Initials _____
The interview is completely free of cost. There is $20 gift card given to you after your participation. Also, the knowledge that we obtain from your participation, and the participation of other volunteers, may help us better understand how emergency response information can be disseminated through social media.

9.3.6 CONFIDENTIALITY
This research is confidential. Confidential means that the research records will include some information about you, like your team’s communication information you provided (with identifiable information removed). In addition, this information will be stored in such a manner that some linkage between your identity and the response in the research exists. Please note that we will keep this information confidential by limiting individual's access to the research data and keeping it in a secure location. The research team and the Institutional Review Board at NameOfUniversity University are the only parties that will be allowed to see the data, except as may be required by law. If a report of this study is published, or the results are presented at a professional conference, only group results will be stated, unless you have agreed otherwise.

9.3.7 CONTACT
If you have questions at any time about the research or the procedures, you may contact the researcher, Dr. Mor Naama at mor@NameOfUniversity.edu (Office 305, School of Communication and Information, NameOfUniversity, 4 Huntington Street New Brunswick, NJ 08901, Tel: 732-932-7500 ext. 8284). If you have any questions about your rights as a research subject, you may contact the IRB Administrator at:

NameOfUniversity Institutional Review Board for the Protection of Human Subjects
Office of Research and Sponsored Programs, 3 NameOfUniversity Plaza, New Brunswick, NJ 08901-8559
Tel: 732-932-0150 ext. 2104, Email: humansubjects@orsp.NameOfUniversity.edu

Your participation in this study is voluntary; you may decline to participate at any time without penalty to you. If you decide to participate, you may withdraw from the study at any time without penalty and without loss of benefits to which you are otherwise entitled. If you withdraw from the study before data collection is completed your data will be removed from the data set and destroyed.

Sign below if you agree to participate in this research study. You will be given a copy of this form to keep. If the interview is conducted through an online chat and you agree to participate in this research study, please type your name on the signature line and check the box.

Subject's signature ____________________________ Date _________________

Check the box if you agree to participate in this research study.

Investigator's signature ________________________ Date _________________

Legally authorized representative's signature _____________________
Date _________________ (if applicable)
You have already agreed to participate in a research study entitled: *AWSM Project* conducted by NameOfUniversity Assistant Professor, Dr. Mor Naaman in the Dept. of Library and Information Science. We are asking for your permission to allow us to audiotape (sound) as part of that research study. You do not have to agree to be recorded in order to participate in the main part of the study.

The recording(s) will be used for analysis only by the research team. The recording(s) will not include your name but a numerical code as the only identifier. Your name will appear only on a list of subjects, but will not be linked to the code number that is assigned to you.

The recording(s) will be stored in a locked file cabinet and will be retained up to three years and then destroyed upon publication of study results.

Your signature on this form grants the investigator named above permission to record you as described above during participation in the above-referenced study. The investigator will not use the recording(s) for any other reason than that/those stated in the consent form without your written permission.

**Subject (Print )** __________________________

**Subject Signature** __________________________ **Date** __________________________

**Principal Investigator Signature** __________________________ **Date** __________________________
9.5 Sample Oral Consent Script

You are invited to participate in a research study about ways of using social media to improve emergency response. You will be asked to participate in an interview. There are no risks associated with this interview.

Have you read and understood the details of the consent form emailed to you?

[ ] Yes  If Yes..... Continue with “Do you have any questions?” section below.
[ ] No  If No... Read below.

To participate in this study, you must have been a team leader or a team member in the AWSM Challenge (also known as “Hat Chase”). You must be at least 18 years old to participate in the study. All you need to do is answer some questions, which should take about 30 minutes, depending on the length of your responses. Questions will ask about the communication tools you used during the event, including Facebook, Twitter, email, and text messaging.

If you agree to take part in the study, your responses will be kept and your responses will be coded with a number. Your name will appear only on a list of subjects, but will not be linked to the code number that is assigned to your recording(s) or data provided.

This research is confidential. Confidential means that the research records will include some information about you, like your team’s communication information you provided (with identifiable information removed). In addition, this information will be stored in such a manner that some linkage between your identity and the response in the research exists.

You have the right to withdraw your consent or discontinue participation at any time without penalty or loss of benefits to which you are otherwise entitled. I will provide you with my contact information if you have any questions for me about this study, or anything else.

There is $20 given to you after your participation. Also, the knowledge that we obtain from your participation, and the participation of other volunteers, may help us better understand how emergency response information can be disseminated through social media.

If you have any questions about your rights as a research subject, you may contact the IRB Administrator or the NameOfUniversity Institutional Review Board for the Protection of Human Subjects Office of Research and Sponsored Programs, 3 NameOfUniversity Plaza, New Brunswick, NJ 08901-8559 Tel: 732-932-0150 ext. 2104, Email: humansubjects@orsp.NameOfUniversity.edu

For questions about the study, you can contact Dr. Mor Naaman, Associate Professor at the NameOfUniversity School of Communication and Information at mor@NameOfUniversity.edu or 732-932-7500x8284.

Do you have any questions?
Do you agree to voluntarily participate in this survey process?

[ ] Yes     If Yes.....     Continue
[ ] No      If No...     Good-bye.

Do you agree to be tape recorded (audio only)?

[ ] Yes     If Yes.....     Continue
[ ] No      If No...     Take notes