policy series
vol 1

Responding To Liability:

Evaluating and Reducing Tort Liability for Digital Volunteers

by Edward S. Robson, Esq.

Wilson Center | COMMONS LAB

Responding To Liability:

Evaluating and Reducing Tort Liability for Digital Volunteers

by Edward S. Robson, Esq.

RESPONDING TO LIABILITY:
EVALUATING AND REDUCING TORT LIABIITY FOR DIGITAL VOLUNTEERS

Commons Lab
Science and Technology Innovation Program
Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue, N.W.
Washington, DC 20004-3027

www.CommonsLab.wilsoncenter.org

Study Director: Lea Shanley
Editors: Lea Shanley and Aaron Lovell
Cover design: Diana Micheli

Available for download free of charge at
http://www.wilsoncenter.org/publication-series/commons-lab

The Woodrow Wilson International Center for Scholars is the national, living U.S. memorial honoring President Woodrow Wilson. In providing an essential link between the worlds of ideas and public policy, the Center addresses current and emerging challenges confronting the United States and the world. The Center promotes policy-relevant research and dialogue to increase the understanding and enhance the capabilities and knowledge of leaders, citizens, and institutions worldwide. Created by an act of Congress in 1968, the Center is a nonpartisan institution headquartered in Washington, D.C.; it is supported by both public and private funds.

Conclusions or opinions expressed in Center publications and programs are those of the authors and speakers. They do not necessarily reflect the views of the Center staff, fellows, trustees, advisory groups, or any individuals or organizations that provide financial support to the Center.

The Center is the publisher of *The Wilson Quarterly* and the home of both the Woodrow Wilson Center Press and the *dialogue* television and radio program. For more information about the Center's activities and publications, please visit us on the Web at http://www.wilsoncenter.org/.

The Science and Technology Innovation Program (STIP) analyzes the evolving implications of such emerging technologies as synthetic biology, nanotechnology, and geo-engineering. STIP's research goes beyond laboratory science to explore new information and communication technologies, sensor networks, prediction markets, and serious games. The program provides critical yet nonpartisan research for the policymaking community and guides officials in the design of new governance frameworks. It gauges crucial public support for science and weighs the overall risks and benefits of technology for society at large.

COMMONS LAB

The Commons Lab advances research and non-partisan policy analysis on emerging technologies that facilitate collaborative, science based and citizen-driven decision-making. New tools like social media and crowdsourcing methods are empowering average people to monitor their environment, collectively generate actionable scientific data, and support disaster response.

http://CommonsLab.WilsonCenter.org

Commons Lab Staff
Lea Shanley, Director, Commons Lab
Aaron Lovell, Writer/Editor
Joe Filvarof, Program Assistant
Zachary Bastian, Research Assistant
Luisa Castellanos, Research Assistant

The Commons Lab is supported by the Alfred P. Sloan Foundation

About the Author

Edward S. Robson counsels emergency service organizations in a variety of matters, including the development of risk management policies, internal governance, and government relations. He has defended emergency service organizations against civil liability, civil rights, First Amendment, and employment claims. Mr. Robson is also the author of a number of articles addressing the legal issues facing emergency service organizations.

Since 2003, Mr. Robson has worked as an emergency medical technician, and he currently serves as a member of the Board of Directors of a large suburban fire company. He graduated with honors from both Villanova University and Villanova University School of Law and is a member of the Pennsylvania and New Jersey bars.

Acknowledgements

This report has been reviewed in draft form by individuals chosen for their technical expertise. They provided candid comments to help ensure that the published report meets the highest standards for objectivity and evidence. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process, but we wish to thank the following individuals for their review of this report:

- Kate Chapman, Executive Director, Humanitarian OpenStreetMap Team
- Jodi Cramer, Esq., government attorney
- Aram Dobalian, Ph.D., Esq., Director, Veterans Emergency Management Evaluation Center, Veterans Health Administration, and Associate Adjunct Professor, University of California, Los Angeles
- Glen Gilmore, Esq., Adjunct Professor of Digital and Social Media Marketing and Law, M.B.A. Program, Rutgers University and Former Adjunct at the National Emergency Response and Rescue Training Center at Texas A&M University
- Patrick Meier, Ph.D., Director of Crisis Mapping, Ushahidi, and Co-Director and Co-Founder at International Network of Crisis Mappers
- Jeffrey Phillips, M.P.A., Emergency Management Coordinator, Los Ranchos de Albuquerque, New Mexico and Virtual Operations Support Group—New Mexico Team Leader
- Stephen S. Wu, Esq., Cooke Kobrick & Wu and CrisisCommons Member

These reviewers were not asked to endorse the conclusions or recommendations in this report, nor did they see the final draft of the report before its release. Lea Shanley and Aaron Lovell of the Woodrow Wilson Center were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered.

The author also wishes to thank Jen Ziemke, Sara Farmer, Willow Brugh, Pascal Schuback, Shoreh Elhami, and Christine Thompson for agreeing to be interviewed for this project; Jodi Cramer, Esq., Aram Dobalian, Ph.D., Esq., Glen Gilmore, Esq., and Stephen S. Wu, Esq., for agreeing to review it; and Kate Chapman, Patrick Meier, Ph.D., and Jeffrey Phillips for doing both. The author also thanks Erica Fruiterman and Zack Bastian for their efforts. Finally, the author is particularly grateful to Lea Shanley for her assistance and patience throughout.

The author is grateful for the support of these individuals, but neither they, the Wilson Center, or the Sloan Foundation are responsible for the content, views, or data contained in this publication. This report exclusively represents the views of the author, who, of course, retains responsibility for the content, including all errors of fact and interpretation.

Contents

Foreword

Crisis mapping started in response to an unnecessary problem: When a crisis happens, information is available via the Internet and mobile phones, but that information does not reach the people in government and aid agencies who are making such decisions as where to put resources or how to move an individual to safety. In January 2010, something amazing happened. After an earthquake in Haiti killed hundreds of thousands of people and overwhelmed the country and local agencies' ability to respond, groups of technologists and subject matter experts around the world did not just sit and wonder what to do—they set up a short message service (SMS) and online connections and organized themselves into teams to create maps, to route incoming messages to responders, to assess building damage, and to create a single list of missing people from dozens of different sources. They did all this from locations far removed from the crisis zone itself. For many people, including myself, Haiti was the start of an age in which we were no longer passive consumers of information about crises, but could generate information and help process it ourselves.

There has been much written about the data response in Haiti. It was not the first time that global teams had come together to manage crisis data (the 9/11 Listserv and Sahana response to the 2004 Boxing Day tsunami came earlier), but it was the first massive global volunteer response to a sudden onset crisis. And the mappers have not gone away. Since 2010, crisis mappers like myself have responded with maps, data, and local coordination to floods (Pakistan, 2010), earthquakes (New Zealand, 2011), tsunamis (Japan, 2011), tornadoes (United States, 2011), hurricanes (United States, 2011), cyclones (Australia, 2011), drought (Somalia, 2011), cold/snow (Balkans, 2012), oil spills (United States, 2010), conflict (Libya, 2011), conflict migration (Somalia, 2011), elections (Sudan, 2011), post-disaster recovery (Libya, 2011), and riots (London, 2011); they have also helped map smaller incidents all over the world (Humanity Road 2010-2012). In addition, they have helped train traditional responders to do this themselves by working together on crisis responses and on several international disaster simulations.

But with this new ability comes issues: how to work effectively with traditional and on-the-ground responders; how to build and use systems that are needed rather than simply possible; how to protect the privacy of vulnerable people; and how to keep the volunteers and their leaders safe from physical, virtual, or legal harm. I have struggled with each of these questions during my times with Crisis Camp London, CrisisCommons, the Standby Task Force, Open Crisis, Humanity Road, Geeks Without Bounds, and—in a slightly different field—during my stint as Chief Architect at United Nations Global Pulse. Progress has occurred in many of these areas. The crisis-mapping community has built links to response agencies and activation protocols for working with them. It has supported efforts like Random Hacks of Kindness and Geeks Without Bounds that are dedicated to building useful and usable technologies. Other groups, such as the Missing Persons Community of Interest, have worked hard on standards to protect people's data in missing persons' databases, and the community has addressed its own needs by developing safety measures such as ways to deal with post-traumatic stress disorder and security protocols for activations in hostile environments, such as the 2011 Libya deployment.

Worry about legal liability has remained, however. When a crisis hits, we do what is needed in the most sensible way we can. But what if our data are misused? What if a volunteer gets hurt? Are we legally responsible for the contents of our data? What is the legal status of a loosely formed group of people who want to help? When I was approached to help with this report, my first thought was, "Phew, we can finally know best how to help protect our people." On reading the final version, I really do think that we can.

Sara Farmer
Chief Technology Officer
Utopia Way

Executive Summary

Major emergencies and crises can overwhelm local resources. In the last several years, self-organized digital volunteers have begun leveraging the power of social media and "crowd mapping" for collaborative crisis responses. Rather than mobilizing a physical response, these digital volunteer groups have responded virtually by creating software applications, monitoring social networks, aggregating data, and creating "crowdsourced" maps to assist both survivors and the formal response community.

These virtual responses can subject digital volunteers to tort liability. Digital volunteers are at risk if they fail to use reasonable care in making their responses. Problems could arise from disseminating false information, developing software in a sloppy manner, failing to act in a manner commensurate with similarly situated professionals, or failing to properly vet and supervise volunteers.

Digital volunteers may also be subject to liability if they fail to act when they have a duty to do so. Such a "duty to rescue" can arise if a digital volunteer creates a hazardous condition, begins to render assistance, or forms a special relationship with survivors. Certain states have statutes that may mandate a response. Statutory protections are available for certain digital volunteers. Individual states provide varying degrees of immunity for digital volunteers who have established appropriate organizational structures. Because many digital volunteers make interstate responses and choice-of-law doctrine is applied unpredictably, the utility of state immunity laws may be limited.

A federal statute, the Volunteer Protection Act of 1997 (VPA), offers more predicable protection to a broader range of digital volunteers. Like its state counterparts, the VPA requires that digital volunteers adopt particular organizational structures to come within its protections and imposes limits on volunteer compensation, which can be inadvertently exceeded.

Contrary to the belief of many digital volunteers, so-called Good Samaritan laws offer little, if any, protection for digital volunteers. Good Samaritan laws typically require that the volunteer

rescuer be responding, in person, to a medical emergency that he or she came upon by happenstance. The digital volunteer model does not satisfy these requirements.

In addition to statutes that limit or eliminate liability, there are several other strategies that digital volunteers can use to mitigate their risk. Groups should engage in a high-level risk assessment to determine where they are most at risk for liability and install appropriate protections. The development and enforcement of operational policies can help to mandate reasonable behavior and create an industry practice across groups. Digital volunteers should also organize nonprofit corporations to avail themselves of statutory protections and to reduce vicarious liability among individual volunteers. Insurance may be available to digital volunteers for certain types of liability. Groups can also utilize disclaimers and contracts of adhesion to discourage reliance or limit liability. Finally, groups should seek professional legal counsel.

The report concludes that evaluating the precise contours of potential liability for digital volunteers can be difficult because of the novelty of issues and the lack of court guidance. Deliberate planning and organization can mitigate many of the potential liabilities, allowing digital volunteers to proceed with confidence.

Introduction

Major emergencies and crises can overwhelm local resources. This problem is traditionally addressed with support from state and federal governments, nongovernmental organizations (NGOs), and the private sector. Notwithstanding this support, addressing the acute needs of people in disaster zones is often a challenge for non-local responders, as it may take days or weeks to organize and travel to the disaster site.

In the last several years, self-organized digital volunteers have begun leveraging the power of social media and "crowdmapping"[1] for collaborative crisis response.[2] Rather than mobilizing a physical response, these digital volunteer groups have responded virtually by creating software applications, monitoring social networks, aggregating data, and creating "crowdsourced"[3] maps to assist both survivors and the formal response community.[4]

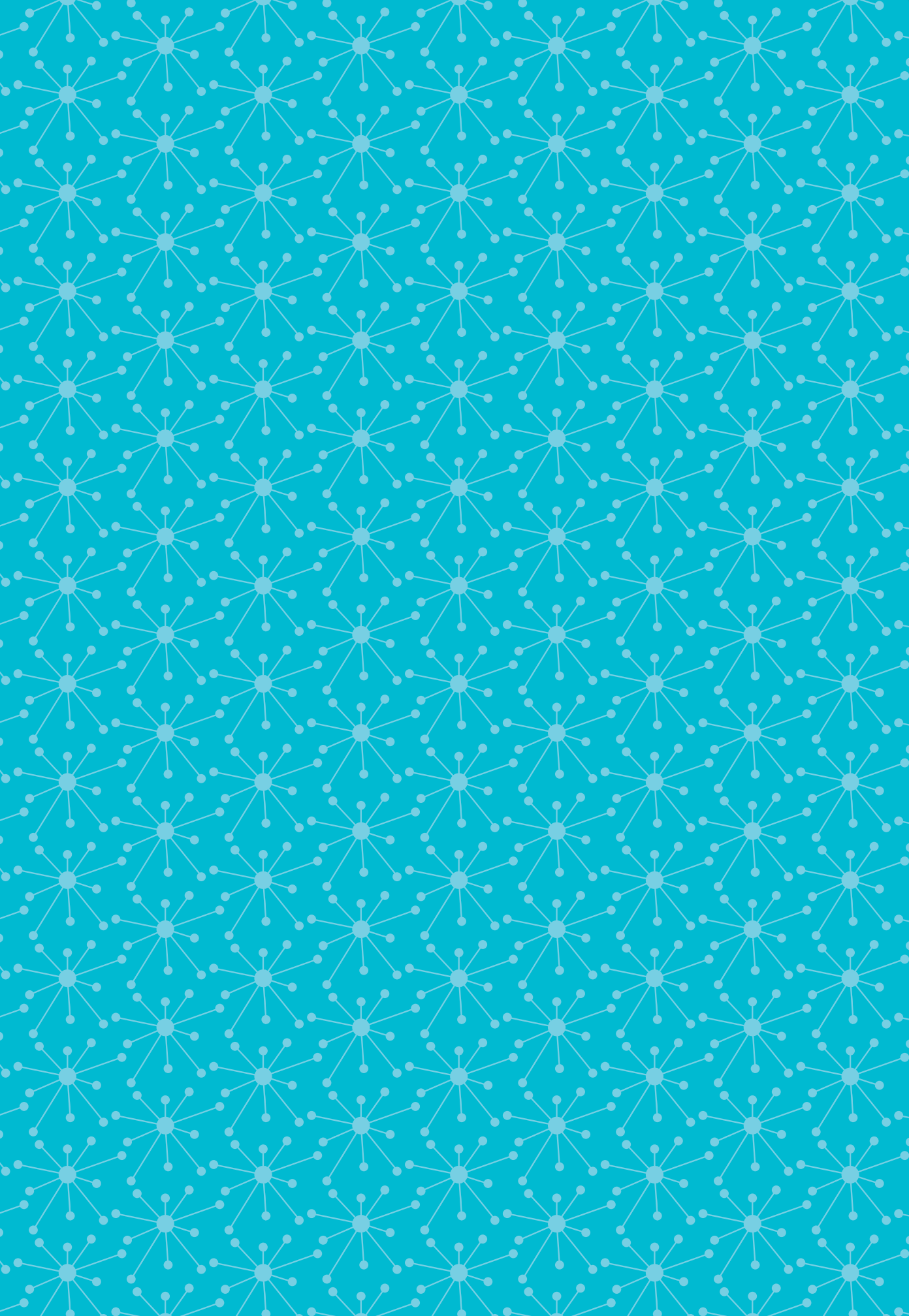
Digital volunteer groups have responded to every variety of crisis, including earthquakes, floods, civil uprisings, and snowstorms. Some of these groups are single-purpose organizations focused on a specific event in a local area, but the majority respond globally to a variety of events.[5] They are "activated" by requests from the general public, formal response organizations, and members of the groups themselves.[6] The length of response varies from hours to weeks.

These virtual responses pose liability questions that the courts have yet to address. Some digital volunteers and emergency managers are trying to understand the risks that these virtual responses present and to develop strategies that will reduce liability.[7]

This report attempts to address these concerns by evaluating the tort liabilities that digital volunteers face and proposing strategies to combat those risks. The report's scope is limited to digital volunteers subject to the jurisdiction of state and federal courts in the United States applying state and federal law. This could include U.S. citizens responding to crises both inside and outside of the United States and to foreign nationals responding to crises inside the United States. Although this report does not address foreign law,

digital volunteers should consider the possibility that they may be subject to foreign law and/or to the jurisdiction of courts in other countries. They should also consider the possibility that U.S. courts may apply foreign law pursuant to choice-of-law doctrines.

This report does not attempt to address potential liabilities arising from intellectual property infringement, invasion of privacy, or disclosure of confidential information. The application of these issues to digital volunteers is an appropriate subject for additional research.



Digital Volunteers: What Do They Do?

1

Digital volunteers engage in a wide variety of activities. In the event of a lawsuit, liability will turn on a detailed factual inquiry into the exact activities of particular defendants. To explore the types of potential liability that may arise from particular types of activity, it is helpful to divide these activities into several categories: data aggregation, software development, crisis mapping, data verification, and communication with affected parties. Some groups engage in only a single category of activity, but most engage in elements of each.

Data Aggregation

Digital volunteer groups aggregate data from a variety of unconnected publicly available information sources, including traditional media outlets, social media feeds such as Twitter and Facebook, short message service (SMS) messages, and data from online missing persons registries.[9] They collect, translate, aggregate, and provide this information to the public and formal responders to increase situational awareness of changing conditions and to facilitate rescue and recovery efforts. Although this work is performed virtually from wherever a particular volunteer is physically located, it is often labor-intensive, requiring volunteers to "cut and paste" information from one data source to another.

Software Development

Digital volunteers develop software applications or modify existing open-source software to perform various response tasks, including "crisis mapping,"[10] language translation, and data aggregation. The best known software tools are those that facilitate crowdsourced mapping of disaster areas.[11]

Unlike commercial software developers, digital volunteers create and modify open-source software. Open-source licenses permit anyone to access and modify the structure and functionality of an application. Software developed by digital volunteers is often created by unrelated parties, each contributing his or her own tweak or innovation to the code.[12] Even in the case of open-source software distributed by a centralized organization, there may be many different versions in use as various volunteers make modifications.[13]

In addition to traditional media outlets, volunteers rely on nontraditional resources, such as trusted individuals with handheld global positioning system (GPS) units,satellite imagery, and SMS messages and Tweets from unknown sources.

Crisis Mapping

Digital volunteers use open-source and proprietary software to develop crowdsourced maps that the public or formal responders can use to facilitate rescue and recovery. In addition to creating accurate base maps with information on the location of roads,[14] crisis maps include the location of both life-safety threats[15] and resources.[16]

Crisis mapping volunteers rely on a variety of sources to produce crowdsourced maps. In addition to traditional media outlets,[17] volunteers rely on nontraditional resources, such as trusted individuals with handheld global positioning system (GPS) units,[18] satellite imagery,[19] and SMS messages and Tweets[20] from unknown sources. These data are plotted on a preexisting map or used to create the map itself. As with data aggregation, volunteers often map "manually" by taking each piece of sourced data and plotting it on the digital map.[21]

Data Verification

Crisis mapping volunteers sometimes attempt to verify the integrity of the incoming data by using one or more techniques. These techniques fall into two categories—passive verification and active verification.

Passive verification involves evaluating sourced, publicly generated data to determine the accuracy of the information. For example, requiring multiple independent reports of life-safety threats before posting that information on a crowdsourced map is a passive verification technique. Another is compiling lists of prescreened local sources with a history of legitimacy and accuracy, such as traditional news outlets, local contacts, and digital volunteers.[22] Passive verification does not involve contacting the original data provider or directing third parties to go to the incident location. Although volunteers try to obtain additional data to verify a particular piece of information, the techniques rely on passive observation.[23] Some volunteers use sophisticated data-mining and analytical tools to develop and verify information.[24]

Active verification techniques involve communication between a volunteer and a data source. Typically, this means


Photo credit: Bill Myers

contacting the data source to evaluate its credibility[25] or attempting to direct sources into a position where they can confirm or deny a report.[26] For example, directing local sources to observe a life-safety threat and report back with a digital image is an active verification technique.

Some digital volunteer groups use no verification techniques whatsoever. They aggregate, map, or transmit any data they receive without curation. Non-curating groups rely on the sheer volume of data to infer the truth. These groups take the position that false data will be minimized both by the high volume of correct data and the self-policing of the crowd. During a large disaster, small digital volunteer groups often do not have sufficient staffing to employ either active or passive verification techniques in a timely way.

Communication with Affected Parties

Some digital volunteers actively communicate with disaster survivors and data sources for more than just data verification. They provide survivors with situational information and respond to requests for aid by directing professional responders and offering helpful information.[27] These groups provide assistance to survivors as a class, rather than providing individualized advice.[28]

Other digital volunteer groups take a different approach. Citing their lack of training to operate in such a role, the prime directive of these groups is to "not interact with disaster-affected populations."[29] Instead, they focus on supporting the needs of the formal response community and humanitarian organizations.

Organizational Structure and its Significance

2

Digital volunteers typically do not need to travel to a disaster area to render aid. Instead, most "respond" virtually using personal computers and mobile devices connected to the Internet. Although group leaders often have technical or humanitarian experience, most digital volunteers have little specialized training or expertise.

Like other grassroots movements, digital volunteer groups grew in an ad hoc fashion, often in response to an isolated incident. Reinforced by the positive results that their work achieved, they have tended to become less transient and more organized.

Organizational Models

Groups fall into four categories, each of which has a unique impact on the potential liability of individual members: exchange model, partnership model, traditional model, and integrated model.

Exchange Model

Digital volunteer groups operating through an exchange model maintain their grassroots origins and have minimal or nonexistent centralized management, few or no assets or funds, and no physical location. These "groups" are composed of dispersed individuals who collaborate in virtual forums or at conferences. The virtual forums also often serve as a repository of user-generated information, procedures, workflows, and the collective knowledge of the members.

It is unlikely that exchange model groups are cohesive enough to have any legal existence or significance beyond the individual members. Exchange model members should expect to be held liable for their own actions or inactions, but without a more direct connection to other members, they are unlikely to be held accountable for the conduct of other members in their group. In other words, membership in an exchange model group is unlikely to either increase or mitigate liability for individual volunteers.

Partnership Model

More centrally organized than exchange model groups, partnership model digital volunteer groups often have an inner circle of regular members who refer to themselves as a "board of directors," "board of advisors," "board of consultants," "management team," or "core team." These groups have not formed nonprofit corporations, but the inner-circle members collectively develop protocols and procedures for use by other volunteers and share responsibility for successes.

Additional volunteers join the core group during disaster events. During a response, the governing members assert varying degrees of control over the event volunteers, either mandating the use of standardized operating procedures or by generally directing their activities.

The partnership model has serious negative implications for individual members. The law treats these groups as "unincorporated associations," that is, groups of individuals who have voluntarily agreed to join together for a common purpose and do not have a corporate charter.[30] An unincorporated association is similar to a business partnership formed for purposes other than making a profit. An agreement to join together for a common purpose determines the existence of such an association.[31] Such an agreement need not be in writing; courts can find an implied agreement from the conduct of the members.[32] Because no writing or particular set of procedures is necessary, individuals are often unaware that they have formed an association or that there are significant legal consequences associated with that designation.

State laws vary widely on their treatment of unincorporated associations. Some states treat members as each other's agents for liability purposes.[33] In those states, if a member injures a third party through conduct encouraged or ratified by the association, each member will be liable to the third party to the full extent of the innocent member's assets. This could include personal possessions and real estate.[34] For example, if a member of a partnership model group that conducts crowd mapping negligently injures a disaster survivor by posting obviously false information on the map, each member of the group would be liable for the full cost of the injury that the other member caused. This is true even if the innocent member had no knowledge of the injury-causing member's negligent conduct and no opportunity to prevent it.

Other states treat unincorporated nonprofit associations more favorably, limiting liability for those uninvolved in the tortious conduct. Several states have adopted the Uniform Unincorporated Non-Profit Association Act (UUNPAA).[35] This act expressly limits imposition of tort and contractual liability on group members arising solely from the actions of other group members, thus providing some of the protections associated with a nonprofit corporation without the expense, formality, or procedures.[36]

From a liability perspective, the partnership model is inappropriate for digital volunteer groups. It unnecessarily exposes members to unlimited liability for the

actions of other members, and the activities of digital volunteers can be high risk.[37] Even worse, members of partnership model organizations may not realize that their participation has the potential to expose them to such liability.

Although the UUNPAA provides some protections, it is unclear which law will apply when members are dispersed across various states or countries and are responding to crises there. Even if digital volunteers reside in a state that has adopted the UUNPAA, a court may not apply it to injuries caused in another state

Traditional Model

Digital volunteer groups in a traditional model have formally organized nonprofit corporations within a particular state and obtained nonprofit status with the Internal Revenue Service and state taxing authorities. These groups maintain a structure similar to that of traditional nonprofit organizations with a board of directors and officers. The law recognizes a traditional model group as existing separately from any of its members.[38] It can sue and be sued, own separate assets, and enter into contracts in its own name.

From a liability perspective, this separate existence offers the most protection for individual members. If a nonprofit corporation negligently injures a third party, the injured person may recover only against the assets of the nonprofit, not against the personal assets of any of its members.[39] Similarly, members of nonprofit corporations are not liable for the actions of other members.

Although a member may still be sued individually for his or her own conduct, the existence of a nonprofit provides practical cover for such suits, particularly if the nonprofit is sufficiently capitalized and maintains insurance. Injured plaintiffs are more likely to sue an insured and well capitalized nonprofit corporation than an individual volunteer.

The federal government and some states limit or eliminate liability for the volunteers of certain nonprofit corporations engaged in particular kinds of conduct.[40] Volunteers operating without an organized nonprofit cannot avail themselves of these protections.

Although the traditional model offers the most protection for digital volunteers, many groups do not utilize it. This lack of adoption is likely attributable to the transitional nature of the groups, the procedural and technical requirements for governance and organization, the dispersed and transient nature of members, a desire to remain agile and flexible, and a general lack of awareness of liability. There are also costs associated with the formation and maintenance of nonprofit corporations that many groups are unable to bear.

Integrated Model

Most digital volunteer groups spawned from gatherings of like-minded people eager to bring their talents to humanitarian crises. Digital volunteer groups typically operate outside of the formal response model, making it unclear as to how the volunteers should interface with the formal response community. There is ongoing debate about how

Digital volunteer groups have certain responsibilities and obligations with regard to their volunteers. Indeed, digital volunteer groups and their members may be exposed to liability for the actions of group members.

emergency managers can best utilize digital volunteers and how digital volunteers can organize themselves to add value to a response.[41]

In contrast to the grassroots development of most groups, some groups have been created by emergency managers attempting to develop teams of virtual responders.[42] These integrated model groups are necessarily incorporated into the formal response structure from the outset. This top-down structure has a clear leader and a clear audience—the emergency manager—for the data it provides.

Depending on state law and the level of organization, digital volunteers operating in the integrated model may be treated in different ways. In some instances, state law treats certain volunteers as state or municipal employees for liability purposes, allowing them to avail themselves of whatever protections the state provides for its own employees.[43] On the other hand, where integrated model groups have not availed themselves of the formalized volunteer intake process or when no such laws exist, integrated model groups can have the status of exchange, partnership, or traditional model groups. Absent state laws allowing for the incorporation of volunteers, integrated model status is liability-neutral, and it is necessary to evaluate which other category the group fits.

Legal Significance of Organization

Digital volunteer groups have certain responsibilities and obligations with regard to their volunteers. Indeed, digital volunteer groups and their members may be exposed to liability for the actions of group members.

Depending on how a digital volunteer group is organized, individual volunteers associated with the group or responding to a crisis with the group may be considered “agents” of the group or its members. “Agency” is a legal status that describes the authority of one person to act on behalf of another and determines the way in which liability should be apportioned among them. The existence of an “agency relationship” is significant, because liability for the actions of an agent attaches to his or her “principal,” the individual or

group for which the agent is acting, in certain circumstances.

Agents can impose significant liability on their principals. Principals are liable for the actions of their agents under the doctrine of *respondeat superior*, meaning "let the master respond." This doctrine imposes liability on the principal for the conduct of the agent if the agent was acting in the course and scope of his or her duty. Liability may exist regardless of whether the principal knew that the specific conduct was occurring.

There are several ways to create an agency relationship: agreement, estoppel, and operation of law.[44] An agency relationship can be created by either an express or an implied agreement between the individual volunteer and the group.[45] The agreement need not be written or even discussed, because an agreement can be implied by conduct. For example, if a member of a digital volunteer group speaks at events or applies for grants on behalf of the group and the group accepts the benefit, the volunteer and the group have an agency relationship by implied agreement.

Agency relationships can also be created by estoppel. Derived from the French word meaning "to stop," [46] estoppel is a flexible legal concept that prohibits a person from taking advantage of a situation that he or she created.[47] As applied in an agency context, an organization (i.e., the principal) may not deny that a person is its agent if the conduct of the organization leads a third party to reasonably believe agency exists.[48] For example, if a digital volunteer group posts a list of its members on its site during a response and one of those members acts negligently and causes injury to disaster survivors during a response, a court may find an agency relationship exists by estoppel—even if there is an express written agreement between the group and the volunteer that no such agency exists. A court may hold the principal liable for the actions of the volunteer. A court is more likely to find such a relationship if the individual volunteer is unable to fully compensate the survivor for his or her injuries.

Finally, agency relationships are sometimes created by operation of law.[49] Members of a partnership are deemed to be agents of one another. Similarly, members of an unincorporated nonprofit organization, like those in partnership model groups, are each other's agents for liability purposes.

The existence of an agency relationship depends largely on which organizational structure a group adopts. Exchange model organizations, for example, are not cohesive enough to have an independent legal existence separate from that of their members. This loose structure makes it unlikely that an agency relationship arises simply from being a member of such a group. The law presumes that members of unincorporated nonprofit associations are each other's agents for liability purposes. In partnership model groups, therefore, members may be liable for the actions of any other member acting in the scope of his or her duties. In traditional model groups, the law presumes that members of nonprofit corporations are the agents of the nonprofit but not of

other members. Traditional model groups should expect to answer for the negligent actions of their members.

A principal is generally liable only for acts that an agent commits in the scope of his or her responsibilities. Courts examine a variety of factors to determine whether a particular act occurred in the scope of the agent's responsibilities: (1) whether the act was authorized by the principal; (2) the time, place, and purpose of the act; (3) whether the act was one commonly performed by agents on behalf of their principal; (4) the extent to which the principal's interests were advanced as a result; (5) the extent to which the private interests of the agent were involved; (6) whether the principal furnished the means or instrumentality by which the injury was inflicted; (7) whether the principal had reason to know that the agent would perform the act in question and whether the agent had ever done it before; and (8) whether the act involved the commission of a crime.[50]

Assume a partnership model group has a core group of volunteers who have responded to a variety of disasters. Each member participates in the day-to-day operation of the response. On a particular disaster response, one volunteer communicates with a disaster survivor without the other members' knowledge and gives the survivor bad advice, which results in serious injury. Since the law implies agency between members of a partnership group, each member stands as the principal of the others. The negligent member who caused the injury was likely acting in the scope of his or her duties and advancing the group's mission when the

injury occurred; therefore, each member of the group can be held liable to the injured survivor to the full extent of each member's personal assets. This is true even if the group has a policy against communicating directly with survivors, as the act was committed during the course of a group response and the group created the opportunity.

Regardless of whether an agency relationship exists, individual digital volunteers cannot eliminate or reduce liability for their own actions or inactions simply by being a member of a digital volunteer group.[51] To the extent that he or she negligently causes injury, an individual volunteer is liable to the full extent of his or her personal assets, including home, bank accounts, and car.[52]

Jurisdiction and Choice-of-Law Issues

3

To understand the potential liability for digital volunteers, one must understand in which courts volunteers can be sued and which law a court will apply. These concepts are referred to as jurisdiction and choice of law, respectively. Both of these concepts are hyper-legal and applied inconsistently. Moreover, jurisdiction and choice-of-law doctrines are areas where the law has struggled to take into account new technology, thereby compounding uncertainty for digital volunteer groups. As a result, digital volunteers may be haled into court in unexpected places and be subject to unexpected law.

Jurisdiction for Digital Volunteers

Jurisdiction refers to a court's power to resolve certain classes of disputes between people of various states and national citizenships. Although this is a complex and technical area of the law, it is important for digital volunteers to have a basic understanding of jurisdiction so that they may conduct activities in such a way as to reduce the number of courts where they may be sued. The fewer courts with jurisdiction, the more difficult it is for potential plaintiffs to assert their claims.

In order to have jurisdiction, a court must have both subject-matter jurisdiction and personal jurisdiction. Subject-matter jurisdiction, as its name suggests, is a court's power to hear disputes of a particular type. Personal jurisdiction refers to a court's power over the people or things in a dispute.

State courts always have subject-matter jurisdiction over tort law claims. In some instances, federal courts may also have subject-matter jurisdiction. Since subject-matter jurisdiction is largely a given, this section will focus on how courts exercise personal jurisdiction.

Personal Jurisdiction Basics

Traditionally, a person[53] becomes subject to the jurisdiction of a particular court when he or she is physically present in the state where the court sits.[54] Although this remains a viable way for a court to exercise jurisdiction, the Supreme Court

has expanded the concept of personal jurisdiction. Modern rules allow a court to exercise jurisdiction over a person even when he or she is not physically present in the state where the court sits and even if he or she has never visited the state.[55] This type of extraterritorial jurisdiction is most relevant to digital volunteer groups.

Courts engage in a two-part analysis to determine whether they have personal jurisdiction over parties that are not physically present in the state where the court sits. First, the court must ask whether the state legislature has authorized it to exert its power over the defendant through what is called a "long-arm statute." Although long-arm statutes vary by state, they typically aim to define the type of conduct that would subject a defendant to jurisdiction.[56] They consistently allow courts of one state to exercise jurisdiction over out-of-state defendants who have caused injury to persons or property in the state where the court sits, even if the defendant has never visited the state.

Second, if the court determines that the long-arm statute authorizes it to exercise jurisdiction, it must determine whether exercising jurisdiction is consistent with the procedural due process rights afforded to defendants by the Fourteenth Amendment of the Constitution. The Fourteenth Amendment protects a defendant from being subject to the jurisdiction of a court when the defendant cannot reasonably expect to be sued there.[57]

To determine whether the exercise of jurisdiction complies with the Fourteenth Amendment requirements, courts engage in a three-part analysis. First, "there [must] be some act by which the defendant purposefully avails itself of the privilege of conducting activities with the forum state."[58] This includes a defendant's intent to cause a particular result within a state, even if the defendant has no direct contact with the state.[59] Second, there must be a relationship between a defendant's contact with the state and the injury caused. The "tighter" the relationship, the fewer contacts are needed to establish jurisdiction. Third, the exercise of jurisdiction must not "offend traditional notions of fair play and substantial justice."[60] In other words, jurisdiction must be reasonable based on a number of factors, including the burden on the defendant, the state's interest, and the plaintiff's interest in a convenient forum.

The first prong of this analysis—"whether the defendant purposefully established" contacts with the state—is the most important of the elements.[61] Traditionally, the contacts that a person made with a state were easily ascertained. Recognized methods of establishing contact included buying or selling goods, living there, hiring employees, injuring someone, entering into contracts, and advertising or soliciting in the state. The Internet, however, challenges our understanding of what it means for a defendant to purposely establish direct contact with a state.

Some early cases held that a court could exercise jurisdiction over a defendant simply because the defendant maintained a Website that could be accessed within the state.[62] Under such a formulation, the owner of a Website

The more interactivity, the more likely jurisdiction exists.

would be subject to jurisdiction in every state where people had access to the site. Such an extreme understanding of virtual "contacts" has been largely supplanted by the *Zippo* analysis.[63]

Zippo Manufacturing Co. v. Zippo Dot Com, Inc.[64] was the first case in which a court formulated an Internet-specific analysis of jurisdictional contacts. *Zippo* contemplates a spectral assessment of Internet contacts.[65] At one end, there is the defendant who uses a Website to actively engage in business in a particular state. Such a defendant might repeatedly transmit files to that state, specifically directing marketing efforts to consumers in that state or contracting with individuals located there using the Website.[66] In this situation, a court clearly has jurisdiction. At the other end, a defendant who passively posts information on a Website with little interactivity is unlikely to be subject to jurisdiction.[67] Between these extremes are interactive Websites that allow those visiting the site to exchange information with the site.[68] The more interactivity, the more likely jurisdiction exists.

The rules that determine whether a United States court has jurisdiction over an individual or an organization are the same regardless of whether the group is based in or is operating in the United States. For example, a group organized in Canada that intentionally directs volunteer activities to Michigan as part of a response may be subject to jurisdiction in Michigan because it likely has a constitutionally significant connection with Michigan. Similarly, a group organized in Pennsylvania that makes a response in Europe can be sued in Pennsylvania because it is present in the state.

Presence, Virtual Contacts, and Jurisdiction over Digital Volunteers

What kinds of activities would subject a digital volunteer group to the jurisdiction of courts in a particular state? Presence in a state is the simplest way for courts to obtain jurisdiction. Depending on which organizational model the digital volunteer group adopts—exchange, partnership, traditional, or integrated—presence has different meanings.

In partnership model groups, jurisdiction exists in every state where a member is physically present.

In the case of the exchange model, presence means the physical presence of a digital volunteer within a state. Since the exchange model does not have a legal significance, this would be the case even if a digital volunteer were not a member of an exchange model group. Similarly, a court's jurisdiction over one exchange model member will not allow it to automatically exercise its jurisdiction over other members.

In partnership model groups, jurisdiction exists in every state where a member is physically present. Although not the case with exchange model groups, a court with jurisdiction over one member of a partnership model group may have jurisdiction over every member of the group. Thus, if a partnership model group has nine members in Pennsylvania and one member in North Dakota, a court in North Dakota may exercise jurisdiction over the nine Pennsylvania members also.

A traditional model nonprofit corporation is present in the state where it is incorporated. The presence of members in other states does not constitute the presence of the nonprofit corporation there. If a traditional model group is incorporated in Pennsylvania and has members in North Dakota, the group is not present in North Dakota for jurisdictional purposes.

Even if a group is not present in a state, a court may exercise jurisdiction if the group has minimum contacts with a state and those contacts satisfy the constitutional requirements discussed previously. As of May 2012, no court has evaluated the type of contacts or the level of contacts that a digital volunteer group must have with a state before the group can be subject to jurisdiction in that state. Notwithstanding this lack of precedent, the *Zippo* interactivity spectrum is a helpful analytical tool.

Groups that do not allow citizens of a particular state to interact directly with them are unlikely to be subject to jurisdiction in that state. For example, a group that monitors Twitter feeds and missing persons' registries from a disaster area in another state, aggregates the data, and publishes the information on the Internet for public consumption is not likely to be subject to jurisdiction in the state where the disaster occurred. It

would be as if the group were standing just across the border from the affected state, listening to what was happening on a radio, and publishing its findings on the Internet. Even if the group was aware that the information was being used in the disaster affected state, the group has not purposely directed anything into the state. The data are openly available to anyone on the Internet, and there is no interactivity with survivors in the state. In such a case, the group has little jurisdictionally significant contact with the state.

At the other extreme, groups that allow a high level of interactivity with people in the affected state will likely be subject to jurisdiction in that state if members' actions cause injury there. If members of a digital volunteer group located in Pennsylvania were engaging in two-way communication with disaster survivors in Kansas and their advice caused injury in Kansas, the group would almost certainly be subject to the jurisdiction of the Kansas state courts.

Between these extremes, a court would face the challenge of assessing the level of interactivity between group members and survivors. Activities such as advertising the existence of a group to disaster survivors, offering software tools to people, allowing survivors to modify information on the site, or providing information tailored to survivors or responders in a particular state increase the probability that a group would be subject to the jurisdiction of a court in that state.

Choice of Law for Digital Volunteers

A court determines which law to apply to a dispute, whether it be that of the state where the court sits or that of another state or country, in a choice-of-law analysis.[69] Since there is little uniformity in choice-of-law doctrines across states,[70] scholars routinely refer to it as a legal "mess."[71] Courts have adopted five "systems," all of which are inconsistently applied, to resolve choice-of-law questions.[72]

Although discussion of these systems is beyond the scope of this article, digital volunteer groups should appreciate that they may be subject to the laws of another state or country. Which law a court applies can determine the outcome of a case. For example, a court might choose to apply the law of a state that statutorily eliminates liability for volunteers rather than the law of a different state without such protections.

Unfortunately, groups can do little or nothing to predictably control which law will apply. Even the terms of use or contracts of adhesion that attempt to specify which law applies are not consistently enforceable. At a minimum, groups should recognize that they may be subject to the law of the place where the injury occurred, where the digital volunteer group operates, and where the potential plaintiff resides.

Tort Liability for Digital Volunteers

4

In its simplest form, a tort is a civil wrong. A person or group commits a tort when the actions or inactions of that person or group unfairly cause injury to another. In such cases, the law provides a remedy for the injured person, most commonly in the form of a monetary award.

Most civil lawsuits involve unintentional, negligence-based claims rather than intentional torts where the defendant intended to cause an injury. Benevolent intent is no defense to liability if an organization acts negligently. Indeed, formal responders may also be liable on negligence-based theories.

Negligence claims arise in a variety of contexts, but they share the same core elements. To assert a claim for negligence, an injured party must prove that (1) the defendant owed the plaintiff a legal duty of care; (2) the defendant breached that duty; and (3) the breach caused the injury.[73]

Duty of Digital Volunteers

Generally, everyone has a legal duty to act as a "reasonable person" would act in order to avoid injury to others.[74] In the United States, this has become a common-sense proposition. If a person who is speeding and weaving between cars on the highway causes an accident, society agrees that the injured person should recover for that injury even if the defendant did not intend to cause injury. When evaluating how a reasonable person would act, the law compares a defendant's conduct with societal norms. The existence and scope of a duty are matters of law for a judge, not a jury, to determine.

Although there are no hard and fast rules that define reasonable behavior, many courts employ an economic analysis to identify reasonable conduct. Under such an analysis, there is a direct relationship between the magnitude of the potential harm and the probability that it will occur on the one hand, and the burden of taking precautions against the harm on the other. The higher the potential for major harm, the more

Compliance with industry standards does not automatically absolve a person of negligence. Rather, "customary practice is not ordinary care; it is but evidence of ordinary care."

precautions a reasonable person would take to prevent the harm. When the magnitude of the harm, amplified by the probability that it will occur, exceeds the burden of taking precautions to prevent the harm, then the defendant has not acted reasonably.

Under some circumstances, the law imposes a higher duty. Individuals with special skills or knowledge owe a duty to act as a reasonable person with the same skills or knowledge would act.[75] This proposition also aligns with common sense. In determining whether a surgeon was negligent, the surgeon's conduct should be compared with that of other similarly skilled physicians and not to that of laypeople. A person need not be a member of a profession or have any particular certification, but can be subject to a higher duty simply because of particular experience or training in an area.

Courts also look to industry standards to determine the appropriate duty in a particular situation. A defendant's failure to conform to industry standards suggests negligence.[76] If 90 percent of the companies that make aeronautical navigation charts use a new technique for accurately identifying the location of broadcasting towers, a court is likely to find that a company that did not use the new technique and misidentified the location of a tower did not act as a reasonable person would.

Compliance with industry standards does not automatically absolve a person of negligence. Rather, "[c]ustomary practice is not ordinary care; it is but evidence of ordinary care."[77] Courts perform an independent analysis of the reasonableness of the industry standard. If the standard is found to be unreasonable, a defendant may not avoid liability simply because the defendant's action was in compliance with that standard. In a well-known case, a tugboat company was held liable for losing barges towed by one of its tugboats because the tugboat was not equipped with a weather radio.[78] The tugboat company presented evidence that weather radios were not widely used in the industry at the time and argued that its failure to use one was not a breach of its duty of reasonable care.[79] The court rejected this argument, stating that "[c]ourts

must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."[80]

The outcome of negligence cases often turns on which duty a court applies. The higher the duty, the more likely it is that a defendant failed to live up to that duty. In the context of digital volunteer groups, however, it is not clear what duty they owe and to whom they owe it. There are no court decisions addressing the issue to provide guidance, so it is necessary to extrapolate from existing law.

To Whom Do Digital Volunteers Owe a Duty?

As a starting point, digital volunteers owe a duty to anyone who could foreseeably use the information that they deliver. It can be difficult to determine whether a particular person is a foreseeable user of information, as many digital volunteer groups make their information publicly available to anyone with an Internet connection. Nevertheless, this foreseeability limitation does eliminate some plaintiffs. For example, the foreseeable users of information provided by a group that is mapping a hurricane might include formal responders, survivors, and the families of survivors. The group would owe a duty to each of these classes of potential users, even if only minimal. On the other hand, researchers may not be foreseeable users of the information, and the group would owe them no duty at all.

How Does a Digital Volunteer Act Reasonably?

Digital volunteers must act as a reasonable person would act in like circumstances. They should apply the magnitude/probability of harm versus the burden of prevention approach described earlier. Assume heavy rains and flooding have forced people from their homes and concentrated them in a storm shelter. A digital volunteer group is collecting information from Twitter and SMS and plotting the information on a crisis map. The group receives an SMS message that a levy has ruptured near the shelter and the shelter will soon be flooded. Throughout that day, the group has received similar false reports submitted as pranks. Posting this information on the map will likely cause a stampede or riot at the shelter.

Before publishing the report of the ruptured levy, the digital volunteer group must weigh the burden of taking precautions against the probability and magnitude of the potential harm. Although the probability that there has been a rupture in the levy is low (because of the volume of phony reports), the potential magnitude of injury is high and could be compounded by the delay associated with extra precautions. A group might be able to discharge its duty by aggressively attempting to verify the information before posting it to the map, reporting the information to professional responders rather than directly to the public, or posting the information with a conspicuous disclaimer indicating that the report is unverified. On the other hand, a report of a lost pet would not require such pre-

cautions, because less harm could occur from posting a false report.

Even without a professional certification or full-time employment, digital volunteers with particular knowledge or skill could be held to a higher standard. For example, a court may find that a professional emergency manager serving as a digital volunteer has a duty to act as a reasonable emergency manager would act under like circumstances.[81] Similarly, geographic information systems (GIS) professionals or social media experts engaged in crisis mapping could be held to the standard of other GIS professionals or experts rather than that of a first-time volunteer.

Courts may also look to industry standards to determine what the appropriate level of care is for digital volunteers. If it becomes clear that mapping groups are using a particular verification technique to confirm the existence of life-safety threats, an outlier group that refuses to use the technique may have breached its duty of care. Because digital volunteer activities are new, ever changing, and diverse, it is difficult to identify what the "industry" standard is for digital volunteers. As groups become more established and formal, the industry will become more defined.

Not all digital volunteer activities are entirely novel. Even without the benefit of case law specific to digital volunteers, courts have addressed the liabilities associated with some group activities, albeit in more commonplace contexts. These lessons are applicable to digital volunteers.

Negligent Design and Production of Software

An increasing number of cases deal with the negligent design or production of software. This liability exists for digital volunteers also. Injuries caused by negligently designed software range from poor function to the release of sensitive data to serious personal injury. In a dramatic case involving a radiation machine used for treating cancer, a software design problem resulted in deadly radiation burns to a patient.[82]

Digital volunteers must take extra care when designing and producing software if the software has a high potential of doing serious harm. Assume a group of digital volunteers developed a software tool that aggregated data from a variety of sources. They are aware that professional rescuers and family members of survivors are using the aggregated list to locate and rescue survivors. Because serious injury could result from an inaccurate list, the group has a duty to take extra precautions in the design and development of the software tool. These precautions might include delaying the release of the software product until a thorough debugging process can occur and standardizing quality control procedures.

There are also a number of cases in which plaintiffs have asserted claims against software companies for negligent design or production of software that allowed hackers or other cybercriminals to access confidential information. Although these cases have generally not been very successful because it can be difficult to establish a causal relation-

ship between the breach of duty and the damage, their frequency suggests a growing trend.[83] For example, a group's assistance to a government agency mapping critical infrastructure may create a duty for the digital volunteers to design or modify the mapping software to make it difficult for unauthorized individuals to access the map. If the group fails to take adequate precautions and terrorists use the information to attack the infrastructure, the group could be liable for the breach.

Industry practice may set a level of duty that is higher than digital volunteers expect. There are procedures for quality control within the larger software industry. Courts may look to those quality control procedures to evaluate whether digital volunteers have lived up to their duty.

Duty to Rescue

As a general proposition, the law does not obligate a person to come to the aid of another person, even if the assistance could be rendered with little or no risk to the rescuer.[84] The law colorfully describes this concept: The result of the rule has been a series of older decisions to the effect that one human being, seeing a fellow man in dire peril, is under no legal obligation to aid him, but may sit on the dock, smoke his cigar, and watch the other drown.[85]

The justification for this harsh rule is that it reflects a strong preference for individual rights and the law's unwillingness to conscript people into acting. It also seeks to limit the scope of potential defendants liable for failing to rescue. If a person is drowning on a crowded beach, should everyone on the beach be liable for failing to rescue? Although there are exceptions to this general proposition, it remains the rule in all but a few states.

Uncomfortable with the rule's harsh effects, courts have created a number of exceptions that would require a person to act. First, a duty to rescue arises if the potential rescuer causes the harm, even if not acting negligently.[86] Courts have reasoned that the creator of the peril is often best situated to take harm-reducing measures.

Second, a duty to rescue arises when a person undertakes a rescue.[87] A person who begins a rescue must act reasonably in performing it and may not abandon it. Courts reason that once a person undertakes a rescue, it discourages others from undertaking the rescue and, if performed negligently, could leave the survivor worse off than if no attempt had been made in the first place.

Third, a duty to rescue arises when there is a special relationship between the survivor and the potential rescuer.[88] These relationships, usually involving some sort of reliance, include common carrier–passenger, hotel operator–guest, business-customer, parent-child, and teacher-student relationships. More recently, courts have recognized special relationships in a variety of contexts, emphasizing the dependence of one party on the other.[89]

Fourth, some states have enacted statutes that create a duty to rescue in certain circumstances. These states—Florida, Massachusetts, Ohio, Rhode Island, Washington, Wisconsin,

Minnesota, Vermont, and Colorado—are in the minority and impose little or no penalty for failing to rescue.[90]

Once a duty to rescue arises, the rescuer must act reasonably to perform the rescue. A reasonable rescue is one that a reasonable person would engage in under like circumstances. What a reasonable person would do depends on the seriousness of the situation, the danger involved in performing the rescue, and the rescuer's qualifications. In many cases, a reasonable "rescue" is simply calling professional rescuers.

The activities of digital volunteer groups can potentially call each of these exceptions into play. Groups that engage in two-way communication with survivors are at the highest risk. Assume a volunteer group encourages survivors to make requests for help to the group, which will then relay the requests to formal responders. The group receives a variety of such requests, and some are not communicated to the appropriate responders. Some survivors wait for help that never comes and are injured as a result. The digital volunteer group could be liable under either the "undertaking rescue" or the "reliance–special relationship" exceptions, because encouraging survivors to direct their request for aid to the group could reasonably be construed as undertaking a rescue or creating a reliance relationship.

Even more passive digital volunteer activities may create a duty to rescue under the "reliance–special relationship" exception. The more survivors reasonably rely on groups to provide rescue, the more likely it is that such a duty might arise.

If a volunteer group sets up an SMS number and distributes flyers instructing people to send their location and needs in the aftermath of a natural disaster to that number, survivors may rely on the number to their detriment when they put in a request for help, thinking that the number is associated with formal responders. In such an event, a court may find a reliance relationship that gives rise to a duty to rescue.

Digital volunteer groups are also at risk for the "created danger" exception.[91] For example, if a group provides incorrect substantive advice on how to purify drinking water in a disaster, a duty to rescue those who might be injured by the use of that information could arise under the "created danger" exception—even if that group acted as a reasonable person would in providing the advice initially. In this context, a rescue might mean quickly acknowledging the error and posting corrective advice.

Negligent Hiring and Supervision

Groups can be liable for the actions of their volunteers acting in their roles as digital volunteers. Groups may also be liable for the actions of agents acting outside the scope of their duties on a theory of negligent hiring or supervision.[92] Volunteer groups, like for-profit companies, have a duty to use reasonable diligence in hiring and supervising their volunteers. To have a claim for negligent hiring, a plaintiff must demonstrate that the digital volunteer group was negligent or reckless in the employment of or association with the volunteer.[93] Similarly, a volunteer group may be liable for the injuries caused

Liability for negligent hiring or supervision can be particularly problematic for digital volunteers because of the difficulty of authenticating the identity or qualifications of individual volunteers.

by a volunteer if the group negligently failed to supervise the volunteer. Just as with other negligence-based claims, the greater the risk of injury, the more precautions a group must take to satisfy the duty of care.

Assume a state emergency management agency was to hire an administrator to manage human relations and other employment matters. The new hire has no emergency management training, but routinely directs relief efforts and gives instructions to responders without the office's knowledge or permission. If the administrator's advice causes injury to survivors or responders, the agency could be liable for negligent supervision. The fact that directing relief efforts is not in the scope of the administrator's duties does not excuse the agency from liability based on a negligent supervision theory. Courts often state that the purpose of the tort is to provide recovery for those injured by agents acting outside of their duties.

Liability for negligent hiring or supervision can be particularly problematic for digital volunteers because of the difficulty of authenticating the identity or qualifications of individual volunteers. The fact that volunteers interact virtually and are often spread globally can make it difficult to verify even the most basic information. Assume a group is mapping protests. An activist volunteer with an extensive criminal record attends a response event and provides the organizer with a false name. Asking the volunteer to produce a simple photo identification and running a background check would have revealed several outstanding warrants. If the activist were to make false postings regarding police brutality that incited a riot, the group could be held liable for negligently hiring or supervising the volunteer.

Missing the Mark—Breaching the Duty

A defendant breaches a legal duty when his or her conduct fails to conform to the relevant duty. Whether a person or group has breached a duty is typically determined by a jury, rather than a judge, and is a fact-specific inquiry. Whether a breach has occurred is intertwined with the duty itself—the greater duty a court imposes, the more likely a breach has occurred.

Bad Relations—Causation

If the defendant is to be liable, the law requires that a defendant's breach caused the plaintiff's injuries.[94] There are two types of causation under this analysis. First, the defendant's breach must have been the cause in fact of the plaintiff's injury; that is, the plaintiff must be able to show that, but for the defendant's breach, plaintiff would not have been injured. Second, the defendant's breach must have been the proximate cause of plaintiff's injury. To show proximate cause, a plaintiff must demonstrate that his or her injury was a reasonably foreseeable result of the defendant's breach.[95]

Two or more defendants can be the cause of a person's injury.[96] Assume a person is negligently speeding on the highway when a second motorist negligently cuts the speeder off. The speeder swerves to avoid the second motorist and hits a pedestrian. In such cases, the law will impose liability on both the speeder and the second motorist. Courts in some jurisdictions will allow the injured pedestrian to recover the full amount of his or her damages from either the speeder or the second motorist. Those in other jurisdictions will attempt to apportion the liability between the speeder and the second motorist, depending on their respective levels of fault.

Whether causation exists is a fact-intensive inquiry, and it is difficult to anticipate the scenarios in which it can become an issue. Digital volunteer groups should recognize that the existence of more than one cause for a person's injury will not insulate them from liability. Indeed, most injuries that could result from the activities of digital volunteers will have multiple causes. Assume a construction company negligently failed to add a particular

ingredient to concrete used in a bridge, allowing the bridge to become damaged in an earthquake. A digital volunteer group then negligently posts false information that sends people across the bridge when the group should have known that the bridge was damaged.

Because both the error by the construction company and the error by the volunteer group caused injury, both will be held liable.

Protection for Digital Volunteers

5

There are statutes at both the state and the federal level that may offer protection for digital volunteers under certain circumstances.[97] These protections typically provide immunity to volunteers from negligence claims, but do not reduce liability when a volunteer has acted in a grossly negligent fashion. "Gross negligence" is defined as the failure "to exercise even that care which a careless person would use."[98] Since demonstrating gross negligence is much more difficult than showing simple negligence, these laws insulate volunteers from liability for all but the most egregious acts or omissions.

State Immunity Laws

In some states, formal responders can rely on sovereign immunity to limit their liability for certain acts performed in the course of their duties.[99] Sovereign immunity is derived from the common law principle that the "king can do no wrong." In other words, where immunity exists, citizens are not permitted to sue their government. Although all fifty states now allow suits against themselves in some circumstances, those circumstances are often limited. Some states with a tradition of emergency service volunteerism have extended, by statute or court decision, state immunity to private nonprofit organizations or individual volunteers performing government functions.[100]

In states where they are available, state immunity statutes can offer well-tailored and ready-made solutions for groups. Since immunity statutes do not typically require volunteers to be citizens of the state or even to be present in the state, groups that make virtual responses may be able to take advantage of the protections if they meet the statutory requirements. For example, ad hoc volunteers or national groups without a presence in a state may need to form or associate with an in-state nonprofit organization.

A variety of limitations make these protections unavailable for certain groups. First, some states require that groups or individual volunteers be named on a roster and approved by the relevant emergency management agency prior to an emergency if they are to be

The Good Samaritan laws clearly exclude digital volunteer groups from their coverage, and digital volunteers should not rely on these laws in any way to shield them from liability.

protected. As many groups do not have consistent members, this may be difficult. Second, in some states immunity exists only when the appropriate state agency or emergency manager requests the assistance of the digital volunteers. Groups that self-activate or activate at the request of the public will receive no protection. Third, protection applies only to groups operating within a particular state, limiting use for groups with a national or international focus. Fourth, the application of choice-of-law principles becomes paramount. If a court determines that the law of a state without immunity applies, groups will have a greater risk of liability. As discussed previously, the application of choice-of-law principles can be unpredictable.

Good Samaritan laws are another example of expanded immunity. Every state has enacted legislation that limits liability for those rendering emergency care without a preexisting duty to do so.[101] These laws were originally intended to encourage physicians and other trained medical personal to render aid to survivors outside of a hospital environment by reducing liability concerns. In many states, these laws also protect any person who voluntarily renders aid.

Although Good Samaritan laws vary by state, they typically require that the volunteer responder be physically present at the accident scene, come upon the scene of the accident by chance, and render emergency care.[102] Many Good Samaritan laws specifically define "emergency care" as medical care.

The Good Samaritan laws clearly exclude digital volunteer groups from their coverage, and digital volunteers should not rely on these laws in any way to shield them from liability. Digital volunteers are not generally physically present at emergency scenes, do not respond by happenstance, and do not render emergency care in the way that the Good Samaritan laws contemplate. This lack of coverage is contrary to the expectations of many digital volunteers who mistakenly believe that these laws do offer protection.[103] Moreover, it is practically impossible to expand the scope of Good Samaritan laws though lobbying efforts. Good Samaritan protections are creatures of state law. Digital volunteers' interstate responses, coupled with the

unpredictability of choice-of-law doctrines, means that the Good Samaritan laws of all fifty states would need to be expanded to offer reliable protection.

Volunteer Protection Act of 1997

In response to concerns that fear of liability was deterring citizens from volunteering in a crisis, Congress enacted the Volunteer Protection Act of 1997 (VPA).[104] The VPA shields individual volunteers from personal liability for acts performed for a nonprofit corporation.[105] In order to prevail against a VPA-covered volunteer, a plaintiff must prove that a volunteer was grossly negligent.[106] The act also eliminates the imposition of punitive damages against a volunteer acting within the scope of his or her responsibilities.[107]

The VPA also has several significant limitations. It provides no liability protection for the nonprofit organization itself, suggesting the need for insurance.[108] Volunteers who receive more than $500 per year for their services, excluding reimbursements for reasonable expenses, receive no protection under the VPA. States can opt out of the law's limitation of liability when the plaintiffs and defendants are citizens of the same state.[109]

Although the VPA offers significant protection from liability, its restrictions make it unsuitable for some groups. It does not have the limitations that make the Good Samaritan laws inapplicable and appears to cover the activities of digital volunteers. The law's national scope also makes choice-of-law issues less of a concern. On the other hand, the VPA requires that volunteers perform services for nonprofit corporations and so offers no protection to exchange or partnership model volunteers. The $500 per year compensation ceiling includes non–cash-based compensation that can unknowingly be satisfied with fringe benefits sometimes associated with volunteer work, including meals, t-shirts, and small gifts.

Liability-Reducing Strategies

6

The potential for liability for digital volunteer groups would not surprise most members of the community. Some groups have attempted to mitigate these risks in various ways, whereas other groups appear to have made no attempt to reduce liability whatsoever. Regardless of the approach currently taken, groups should become aware that a variety of relatively simple, liability-reducing steps are available to them.

In light of the fact that most groups are underfunded, some may perceive the suggested strategies as too expensive to be workable. Many of the suggested strategies, however, require little or no funding, and most of the volunteer groups surveyed for this report have already begun to adopt one or more of these approaches.

Current perceptions also presuppose that groups will remain ad hoc grassroots organizations indefinitely. In the same way that modern fire departments have evolved from "bucket brigades," digital volunteer groups are likely to evolve into more regular organizations. This evolution will make them more enticing targets of lawsuits, and groups will have no choice but to integrate liability-reducing strategies into their operations. Early adoption of these measures, in particular the costless policy strategies, should help to ease organizational growing pains and offers immediate protection in the meantime.

Some members of the community may view some of these strategies as antithetical to the grassroots nature of the model. Critics may argue that it is precisely because anyone can volunteer his or her time without previous experience or ongoing commitment that this system is so powerful. Attempts to impose structure on that model, they may argue, will kill it in the process.

This argument creates a false dichotomy. Some of the suggested strategies change the response methods of some groups, but none would fundamentally change the model. The common theme of these strategies is structural improvement, thoughtful planning, and better organization. These concepts do not somehow prohibit groups from tap-

ping into the power of crowdsourcing; rather, they help to ensure protection for volunteers. Although difficult to verify with empirical evidence, Congress and state legislatures have readily acknowledged that a fear of liability is a deterrent to volunteerism, particularly among the most senior and skilled volunteers.[110] The strategies described in the following may help provide the measure of confidence necessary to make operating digital volunteer groups a lasting model.

Liability-reducing strategies for digital volunteer groups fall into several categories: (1) policy creation, (2) informed choice of organizational structure, (3) purchase of insurance, (4) use of agreements and disclaimers, and (5) consultation with counsel.

Policies

Policies help to avoid negligence by giving volunteers a formulaic way to conduct themselves as a reasonable person would under a particular set of circumstances. When developed prior to a response, standardized policies take much of the guesswork out of acting in a responsible way during a rushed and stressful situation.

Policies also help to develop the standard of care. As discussed earlier, courts have not addressed the scope of a digital volunteer's duties. When the first court does, it may compare a group's policies with the policies of similar groups to help define the appropriate level of duty. Courts are less likely to find that volunteer groups that have and enforce operational policies have breached their duty, as the courts may consider those policies as coextensive with the duty of care.

Unenforced or disregarded policies can have the opposite effect. If a group's operational policies embody the standard of care, routinely disregarding them will fall below that duty. Moreover, having and ignoring policies creates the appearance that the group was aware of the existence of a duty and chose to disregard it.

A group without any operational policies has other issues. Without any policy guideposts, a court is more likely to set a standard of care that is inconsistent with reality. Such a ruling could not only have a negative result for the defendant volunteers in the case, but also set a bad precedent for other digital volunteer groups.

Developing Operational Policies

Developing specific policies is an ongoing process that must evolve according to a group's activities, organizational structure, and past experiences. Although each group needs to develop policies appropriate for the activities that they carry out, some common best practices can help to reduce liability. It is self-evident that policies and organizational structure cannot be developed in the midst of a disaster. Attempting to do so risks delaying response and generating short-sighted or ineffective policies. Rather, groups must deliberately and carefully develop their procedures during non-emergency time.

Working together to develop common policies for common risks will help groups to create an "industry standard" that shapes the duty of care.

Groups should begin the policy development process with a high-level risk assessment that classifies risks according to their magnitude, determines the probability that they will occur, and allocates the costs associated with mitigating them. A simple matrix is helpful. The worse the potential harm, the more precautions a group must take. It is important that the risk assessment process result in a written document that middle- and upper-level volunteers can reference and update as appropriate. This document can also be helpful for litigation purposes.

Working together to develop common policies for common risks will help groups to create an "industry standard" that shapes the duty of care. Yearly conferences in which group leaders exchange policies and trade notes on successes and failures may help achieve some consistency. The more consistency in policies across groups, the more likely a court will recognize industry practice as the standard of care.

Specific Operational Policies

Since activities vary by group and response, it is difficult to develop an exhaustive list of specific operational policies. It is possible, however, to suggest policy themes for the various activities of the digital volunteer groups.

All groups should be mindful of jurisdictional issues and should attempt to reduce the number of states where a court may be able to obtain jurisdiction over them. Converting from an exchange or partnership model to a traditional model organization reduces the number of states where a group has jurisdictional "presence." Moreover, the fewer interactions a group has with disaster survivors, the less likely a group will be subject to jurisdiction under the *Zippo* analysis.[111]

Reducing interactive contacts with survivors also reduces substantive liability. Although there is generally no duty to rescue, such a duty arises when a group voluntarily undertakes a rescue or creates a reliance relationship between the rescuer and the survivor. Eliminating or limiting direct communication with survivors reduces this liability. Assume

Although making data open to the public is critical to the models of many groups, limiting access to data sharply reduces the number of potential plaintiffs.

a group receives a report that a person needs assistance. The group alerts the survivor that help is on the way and removes the person's need for help from the crisis map that it maintains, but it fails to alert formal responders. The digital volunteer group might be liable under a duty to rescue theory for failing to take appropriate steps to ensure a response. Now assume the same facts, except that the group does not alert the person that help is on the way. Even if the outcome is the same, the group would not be subject to liability for failing to rescue the person because it never established a reliance relationship.

Groups should minimize the number of people who have access to the information they provide. Although making data open to the public is critical to the models of many groups, limiting access to data sharply reduces the number of potential plaintiffs. Groups should carefully evaluate their core mission and limit the availability of information to those who must use it for the mission. If a group's mission is to support the distribution of food aid to disaster-affected groups, for example, developing a relationship with a traditional humanitarian organization and providing the organization with password-protected data accomplishes the group's goal while limiting potential plaintiffs.

Mapping or data-aggregating groups should develop comprehensive procedures to ensure the integrity of their data. Such procedures should include manual checks and, to the extent possible, software tools. The greater the risk of injury stemming from a potential error, the more verification processes should be in place. Similarly, groups that are developing or modifying software should have production procedures in place to ferret out dangerous bugs in software that deals with critical data. If a group is dealing with non-public maps, groups should implement security controls to prevent unauthorized access to sensitive information.

The risks of negligent hiring and negligent supervision should be a concern for all groups. Procedures and verification techniques are necessary to prevent malicious or incompetent volunteers from causing injury. Just as with other policies, the greater the magnitude of harm that could result from the actions of

a malicious volunteer, the more rigorous the protections must be. Volunteers in positions devoted to simple tasks such as translating SMS messages into English may not require any background checks or verification, as there is a relatively low risk that volunteers performing these tasks can cause much damage. On the other hand, background checks or other more extensive verification may be appropriate for high-level volunteers. Groups also should establish standardized training programs for new volunteers. Training will help reduce liability arising from failure-to-supervise claims and liability resulting from the direct negligence of volunteers.

Adoption of Traditional or Integrated Model Organizational Structure

Statutory protections may insulate digital volunteer groups in certain circumstances. In order to take advantage of these protections, groups should adopt appropriate organizational structures.

Adopting a traditional model organization reduces the liability of digital volunteers by limiting individual liability for the actions of other members, allowing access to the protections of the VPA and its state counterparts, and facilitating the purchase of insurance. The protection offered by the VPA is a particularly attractive feature, because it reduces liability without the need to develop procedures or modify the manner in which the group makes a response. In addition to the liability-reducing benefits, traditional model groups can facilitate funding by allowing the creation of bank accounts in the name of the organization and allowing donors to claim tax deductions. For active groups, these benefits more than outweigh the costs associated with creating and maintaining a nonprofit corporation.

Traditional model organizations can also purchase insurance more easily. Exchange and partnership model groups are often not structured formally enough to purchase insurance. Partnership model groups may not even know that they would find it difficult to buy insurance as they are unlikely to consider the prospect. The formalized organization of the traditional model group allows for a clearly defined, named insured.

Creating a traditional model nonprofit organization is a two-step process that involves both corporate and tax law components. A group must form a nonprofit corporation in a particular state, a process that can occur relatively quickly. From a liability point of view, this step is the most critical, because it allows the group to take advantage of the VPA and limits the liability of members for the actions of other members. The group must then apply for nonprofit status with the Internal Revenue Service and state taxing authorities, which can take longer.

Groups should also consider operating as integrated model groups by associating with emergency managers or in-state nonprofit organizations when available. This may involve registering volunteers with appropriate agencies or entering into mutual aid agreements with in-state groups. In states that extend statutory immunity to those groups, operating as an integrated model

group may offer significant protection. Furthermore, integrated model status does not prohibit the adoption of a traditional model organization, thereby potentially allowing a group to receive the benefit of both the VPA and whatever state protections exist.

Purchase of Insurance

Traditional domestic general liability policies cover bodily injury and property damage caused by the negligent conduct of the insured.[112] Although no courts have addressed the issue, these policies appear to be broad enough to cover injuries caused by the activities of digital volunteer groups. General liability policies are relatively inexpensive and can be supplemented with umbrella policies at little cost; therefore, groups responding to disaster situations in the United States should obtain general liability policies.

These policies, however, have a variety of exceptions and exclusions to coverage that might affect coverage for groups.[113] Groups should take special care to compare their activities with the scope of the policy to confirm that the potential injuries that digital volunteers might cause fall within the coverages in the policy.

General liability policies have geographic coverage areas, and liabilities that arise outside of those areas are not covered.[114] These policies cover only injuries that arise in the United States, Puerto Rico, and Canada and require that claims be brought in the United States. For groups making international responses, injuries caused by digital volunteers abroad will not be covered.

Injuries directly or indirectly caused by war or civil insurrection are also excluded from these policies.[115] Accordingly, digital volunteer groups responding to man-made disasters should not assume that they have coverage.

General liability policies do not cover the loss of electronic data.[116] For example, if a group that develops software destroys data on a system that someone has volunteered for a response, a general liability policy will not cover the loss of these data.

Each one of these exclusions can be covered with other forms of specialized insurance. A variety of companies offer worldwide general liability policies and policies that cover injuries caused by war. Several companies offer data-loss policies. Depending on the scope of coverage, these policies can be expensive. To determine whether the benefits of these specialized forms of insurance outweigh their costs, digital volunteer groups should consult with insurance professionals and legal counsel.

One way for a group to mitigate its insurance costs is to specialize in a particular type of response or geographic area. If a group makes responses only in the United States, a simple general liability policy may offer adequate coverage. Another group might handle only conflicts in a particular area of the world. This limitation might also have the unintended benefit of allowing the group to develop a particular expertise with certain areas, including the development of trusted

sources. For groups that conduct responses everywhere in the world for every type of disaster, insurance costs would be the highest.

Aside from the formal protections associated with appropriate insurance coverage, the purchase of insurance provides a measure of practical insulation from liability for individual volunteers. Even though individual volunteers are never absolved of their own negligent conduct by being a part of an organization, an injured party will often not bother to assert a claim against individual volunteers when he or she can obtain full compensation from an appropriately insured entity. The "deep pockets" of the insurance company will dissuade a potential plaintiff from suing an individual with limited financial assets.

Agreements and Disclaimers

Contracts of adhesion and terms of use may also be helpful as a way to shape the relationship between a digital volunteer group and potential plaintiffs. These devices attempt to create a contract that requires a user to assent to certain conditions before using a group's site. They can be used to limit liability, select the law that will apply, or require a plaintiff to bring claims in a particular court.

Although sometimes helpful, groups should not rely on these agreements as their sole liability-reducing measure. Courts routinely refuse to enforce contracts of adhesion either because they find that the parties never came to a true agreement or because they find such contracts unconscionable. Courts are particularly reluctant to enforce contracts of adhesion that require the prospective waiver or limitation of rights.

Even an enforceable contract of adhesion cannot reach all potential plaintiffs. Assume a group negligently posts false information. One person reads the information on a smart phone and yells it to bystanders, who stampede. In the site's terms of use, all users agree not to sue the group maintaining the site. The person who visited the site may be barred from bringing a claim, but the bystanders injured in the stampede would not be barred, because they never visited the site or assented to the terms of use.

Digital volunteer groups also can reduce liability arising from duty-to-rescue claims through the use of disclaimers that discourage reliance relationships. Depending on a group's activities, disclaimers should indicate that professional responders have not been alerted, that members do not respond to requests for help, or that information is not verified. Similarly, educating data users on the sources of the data and the difficulty or impossibility of ensuring the data's accuracy can help to reduce liability.

Like contracts of adhesion, disclaimers and warnings will not shield groups from all claims. People who have not read a disclaimer will not be barred from bringing claims. Accordingly, groups should make disclaimers clear and conspicuous to information users. Making a brief reference to a larger disclaimer may be insufficient. The better practice is to insert a brief disclaimer

with a reference to a larger disclaimer directly in the stream of disseminated information. For example, a group using Twitter to provide information to disaster survivors should put a brief disclaimer in the "Tweets" themselves (e.g., use a hashtag such as #unverified). Mapping groups should consider putting a disclaimer adjacent to the main crisis map.

Consultation with Legal Counsel

Although this report provides a general overview of the law, it is not a substitute for legal counsel who is familiar with the law related to emergency services or nonprofit organizations. Tort claims turn on highly fact-specific circumstances, and it can be difficult to make meaningful generalizations. An attorney can evaluate which of a group's activities carry the greatest risk and develop operational policies aimed at reducing that risk. Such customized policies may also be less intrusive to a group's activities than "boilerplate" policies, because they modify only the procedures necessary to reduce liability.

Counsel can also assist digital volunteer groups in positioning themselves to take advantage of any state statutory protections that exist. Most states provide some form of liability protection for volunteers who abide by statutorily created requirements. An attorney can also guide groups on how to take advantage of the VPA.

The decision to purchase insurance and the type of insurance to purchase are decisions that should be made only in

conjunction with counsel. Depending on a variety of factors, jurisdictional issues may make it so difficult to maintain a lawsuit against groups making international responses that insurance is unnecessary. An attorney with detailed knowledge of a particular group's activities can help to select the appropriate coverage in conjunction with insurance professionals, when insurance is necessary.

Conclusion

The liabilities that digital volunteers face cannot be understated. Both the formal response community and the public will increasingly depend on the information that these groups provide to make critical decisions. The potential for liability will follow. But the risk for liability should not be overstated either. The widely varying activities of groups and the lack of case law present a broad spectrum of potential claims. As groups specialize and case law develops, however, it will become clearer what risks particular types of responses present, and groups will be in a better position to efficiently mitigate these risks.

No silver bullet will eliminate liability. Rather, liability issues must be addressed with a series of conscious decisions that fit a group's mission and culture. To reduce liability in a meaningful way, groups should engage in a comprehensive review of their organizational structures, their activities, and their volunteers.

Liability-reducing strategies should not be an end in themselves, but shorthand for ways to deliver critical services safely and effectively. Tort law not only is concerned with compensating injured people, but also seeks to have a normative effect on the way people act, encouraging them to avoid behavior with a high risk of injuring others. To the extent that implementing liability strategies seems overly burdensome, digital volunteer groups should consider that they might not be operating with a level of care that is commensurate with the risk associated with their activities.

This report should not be construed as legal advice and does not reflect the law of any particular state. Groups should consult with counsel prior to adopting any of the strategies identified in this report.

Notes

1 "Crowdmapping is the aggregation of crowd-generated inputs such as text messages and social media feeds with geographic data to provide real-time, interactive information on events such as wars, humanitarian crises, crime, elections, or natural disasters (the results are sometimes referred to as *crisis maps*)." Kimo Quaintance, "Concepts to Know: Crowdmapping," accessed July 18, 2012, http://kimoquaintance.com/2011/09/04/concepts-to-know-crowdmapping.

2 See, e.g., Jessica Heinzelman and Carol Waters, *Crowdsourcing Crisis Information in Disaster-Affected Haiti,* Special Report (Washington, DC: United States Institute of Peace, October 2010), available at www.usip.org; John Crowley and Jennifer Chan, *Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies* (Cambridge, MA: Harvard Humanitarian Initiative, 2011).

3 See Daren C. Brabham, "Crowdsourcing as a Model for Problem Solving: An Introduction and Cases," *Convergence* 14 (2008): 75–90, which provides an overview of crowdsourcing, http://con.sagepub.com/content/14/1/75.short; Enrique Estellés-Arolas and Fernando González-Ladrón-de-Guevara, "Towards an Integrated Crowdsourcing Definition," *Journal of Information Science* 38, no. 2 (2012); 1–14, http://www.crowdsourcing-blog.org/wp-content/uploads/2012/02/Towards-an-integrated-crowdsourcing-definition-Estell%C3%A9s-Gonz%C3%A1lez.pdf.

4 Heinzelman and Waters, *Crowdsourcing Crisis Information*; Crowley and Chan, *Disaster Relief 2,0.*

5 Telephone interview with Jen Ziemke, co-founder, International Network of Crisis Mappers, on February 9, 2012. She stated that the International Network of Crisis Mappers has more than 1,700 different associations or groups interested in or using some aspect of "crisis mapping" in their work.

6 Compare Standbytaskforce.com, "Activation Protocols," accessed April 1, 2012, http://blog.standbytaskforce.com/about/activation-criteria/, with Humanityroad.org, "AboutUS," accessed April 16, 2012, http://www.humanityroad.org/AboutUs.htm.

7 See Clarence Wardell, III, and Yee San Su, *2011 Social Media + Emergency Management Camp—Transforming the Response Enterprise* (Alexandria, VA: CNA Analysis & Solutions, September 2012), 21–22, noting that "fear of lawsuits is the number one threat preventing adoption of social media during a crisis." See also Sabrina McCormick and Luisa Castellanos, *New Media for Emergency Managers: An Exploratory Assessment of Obstacles to Adoption and Use* (Washington, DC: Woodrow Wilson Center, in press).

8 This section was developed largely from a series of interviews that the author conducted by telephone with nine members and leaders of digital volunteer groups over the course of several months.

9 Telephone interview with Jen Ziemke, co-founder, International Network of Crisis Mappers, on February 9, 2012, in which she described the activities of various digital volunteer groups.

10 Patrick Philippe Meier, "A Brief History of Crisis Mapping (Updated)," *iRevolution*, March 12, 2009, http://irevolution.net/2009/03/12/a-brief-history-of-crisis-mapping/.

11 See, generally, Heinzelman and Waters, *Crowdsourcing Crisis Information*.

12 Telephone interview with Sara Farmer, chief technology officer, Utopia Way, on February 13, 2012, in which she described the software development processes of digital volunteer groups.

13 Ibid.

14 See OpenStreetMap.org, "About," accessed April 1, 2012, http://hot.openstreetmap.org/about.

15 Life-safety threats are anything that poses a danger to the safety of victims or responders, including fires, riots, and damaged structures.

16 See, e.g., Heinzelman and Waters, *Crowdsourcing Crisis Information,* 1, 4–10.

17 See, e.g., Heinzelman and Waters *Crowdsourcing Crisis Information*.

18 OpenStreetMap.org, "About."

19 Ibid.

20 Twitter Help Center, "The Twitter Glossary," accessed May 25, 2012, http://support.twitter.com/groups/31-twitter-basics/topics/104-welcome-to-twitter-support/articles/166337-the-twitter-glossary#t, where "Tweet" is defined as "a message posted via Twitter containing 140 characters or fewer."

21 Telephone interview with Kate Chapman, treasurer, Humanitarian Open Street Map, on February 7, 2012, who described the mapping process from Humanitarian Open Street Map; see also Heinzelman and Waters, *Crowdsourcing Crisis Information*.

22 Patrick P. Meier, *Verifying Crowdsourced Social Media Reports for Live Crisis Mapping: An Introduction to Information Forensic*, 14–16, available at http://www.crowdsourcing.org/document/verifying-crowdsourced-social-media-reports-for-live-crisis-mapping-an-introduction-to-information-forensics/8811.

23 Ibid.

24 Telephone interview with Shoreh Elhami, co-founder, GISCorps, on May 21, 2012, who described the activities of some GISCorps volunteers.

25 Telephone interview with Christine Thompson, president, Humanity Road, Inc., on March 29, 2012.

26 Meier, *Verifying Crowdsourced Social Media Reports*.

27 Telephone interview with Christine Thompson.

28 Ibid.

29 Telephone interview with Patrick P. Meier, co-founder, International Network of Crisis Mappers, on February 20, 2012.

30 See, e.g., Peoples Gas Sys., Inc. v. Acme Gas Corp., 689 So.2d 292 (Fla. Dist. Ct. App. 1997).

31 See Committee for Idaho's High Desert, Inc. v. Yost, 92 F.3d 814, 820 (9th Cir. 1996); Local 4076, United Steelworkers of America v. United Steelworkers of America, AFL–CIO, 327 F.Supp. 1400, 1402–1403 (W.D.Pa.1971).

32 See, e.g., DeVillars v. Hessler, 70 A.2d 333 (Pa. 1950).

33 See Fast v. Kahan, 481 P.2d 958, 962 (Kan. 1971). .

34 See, e.g., Waklet-Riker v. Sayre Area Educ. Ass'n, 656 A.2d 138 (Pa. Super. 1995); Walsh v. Israel Couture Post, No. 2274 V.F.W., 542 A.2d 1094, 1096 (R.I. 1988), which states, "All members of a joint enterprise are chargeable with the negligence of a member of the joint enterprise when such member acts within the scope of the agency created by said joint enterprise."

35 The UUNPAA is model legislation, which means that it is drafted by attorneys, judges, and law professors, but becomes law only

if it is enacted by a state's legislature. Alabama, Arkansas, Colorado, Delaware, Hawaii, Idaho, North Carolina, West Virginia, Wisconsin, and Wyoming have all adopted the UUNPAA.

36 UUNPAA § 6.

37 In addition to liability concerns, unincorporated associations have other practical drawbacks for digital volunteers. For example, it is difficult for an unincorporated association to obtain nonprofit status with the Internal Revenue Service or to open a bank account.

38 See, e.g., Marzano v. Computer Science Corp., Inc., 91 F.3d 497, 513 (3d Cir. 1996); see, generally, Nina A. Mendelson, "A Control-Based Approach to Shareholder Liability for Corporate Torts," *Columbia Law Review* 102 (2002): 1203.

39 Ibid.

40 The Federal Volunteer Protection Act of 1997 is one example of such a limitation.

41 See, generally, Wardell and Su, *2011 Social Media + Emergency Management Camp*.

42 Telephone interview with Jeffrey Phillips, emergency management coordinator, Los Ranchos de Albuquerque, New Mexico, on March 28, 2012.

43 See, e.g., Ind. Code § 36-8-12-8 (West 2012).

44 See, e.g., Restatement (Second) of Agency §§ 15, 26; Uniform Partnership Act of 1997, Section 301 31.

45 Restatement (Second) of Agency §§ 15, 26.

46 *Black's Law Dictionary*, 4th ed. (St. Paul, MN: West, 1968), 648.

47 Restatement (Second) of Agency § 31.

48 Ibid.

49 See, e.g., Uniform Partnership Act of 1997, Section 301.

50 Restatement (Second) of Agency § 229 (West 2012).

51 There are statutory protections for the volunteers working as part of nonprofit groups. Such protection exists because of Congress' desire to encourage a particular structure of volunteerism, not because of some protection inherent in group membership. Indeed, membership in an exchange model or partnership model group does not shield the individual volunteer from liability.

52 Individual volunteers may have some statutory protections available that would change this result.

53 The term *person* includes legal persons like nonprofit corporations. See *J. McIntyre Machinery, Ltd. v. Nicastro*, 131 S. Ct. 2780, 2787 (June 27, 2011).

54 Pennoyer v. Neff, 95 U.S. 714 (1977).

55 Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476 (1985).

56 50 State Statutory Surveys, *Personal Jurisdiction* (West 2011).

57 Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 774 (1984).

58 Hanson v. Denckla, 357 U.S. 235, 253 (1958).

59 Calder v. Jones, 465 U.S. 783 (1984).

60 Burger King Corp. v. Rudzewicz, 471 U.S. 462, 477 (1985), in which the court quoted *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) [internal citations removed].

61 Ibid., 476 (referring to the first prong as the "constitutional touchstone").

62 See, e.g., Maritz, Inc. v. CyberGold, Inc., 947 F. Supp. 1328, 1333–1334 (E.D. Mo. 1996).

63 See, e.g., ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 713–714 (4th Cir. 2002); Mink v. AAAA Dev. LLC, 190 F.3d 333, 336 (5th Cir. 1999); Rainy Day Books & Café, L.L.C., 186 F. Supp. 2d 1158, 1164–1165 (D. Kan. 2002).

64 925 F. Supp. 1119 (W.D. Pa. 1997).

65 Zippo, 925 F. Supp. at 1125–1126.

66 Ibid.

67 Ibid., 1125.

68 Ibid.

69 Restatement (Second) of Conflict of Laws § 2 (1971).

70 See Restatement (Second) of Conflict of Laws § 5, stating that "[t]he process of formulation and reexamination of these rules requires consideration not only of the specific policies of the relevant local law rules but also of the general policies relating to multi-state occurrences."

71 See, e.g., Kermit Roosevelt, III, "The Myth of Choice of Law: Rethinking Conflicts," *Michigan Law Review* 97 (1999): 2448, 2449 ("Choice of law is a mess. That much has become a truism."); Hillel Y. Levin, "What Do We Really Know About the American Choice-of-Law Revolution?" *Stanford Law Review* 60 (2007): 247, 248, where the author reviewed Symeon C. Symeonides, *The American Choice-Of-Law Revolution: Past, Present and Future* (Salem, OR: Willamette University College of Law, 2006) and quoted: "[M]odern conflicts theory and doctrine is a mess . . . ."). But see Christopher A. Whytock, "Myth of Mess? International Choice of Law in Action," *New York University Law Review* 84 (2009): 719.

72 Whytock, "Myth of Mess?"

73 Restatement (Second) of Torts § 284.

74 Restatement (Second) of Torts § 283.

75 Restatement (Second) of Torts § 299A.

76 Ibid.

77 Northwest Airlines, Inc. v. Glenn L. Martin Co., 224 F.2d 120, 129 (6th Cir. 1955).

78 T.J. Hooper v. N. Barge Corp., 60 F.2d 737 (2d Cir. 1932).

79 Ibid., 739–740.

80 Ibid.

81 A similar enhanced duty arises with physicians rendering aid at emergency scenes. Although not acting in a hospital setting or in the scope of their employment, courts have held them to a higher standard of care. In response to fears that physicians would not render aid to accident victims for fear of liability, many states have passed "Good Samaritan" laws that shield professional medical personnel from such liability. These statutes are unlikely to offer protection to digital volunteers, however.

82 William Plummer, "A Computer Glitch Turns Miracle Machine Into Monster for Three Cancer Patients," available at http://www.people.com/people/archive/article/0,,20095076,00.html; Jody Armour and Watts S. Humphrey, *Software Product Liability* (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, August 1993).

83 Jennifer A. Chandler, "Negligence Liability for Breaches of Data Security," *Banking and Finance Law Review,* in press, available at http://ssrn.com/abstract=998305.

84 Restatement (Second) of Torts § 314.

85 Restatement (Second) of Torts § 314, cmt. c.

86 Restatement (Second) of Torts § 322.

87 Restatement (Second) of Torts § 323.

88 Restatement (Second) of Torts § 314A.

89 See, e.g., Thomas v. County Comm'rs of Shawnee County, 198 P.3d 182 (Kan. App. 2008), in which the court found that a prison guard owed a prisoner a duty of reasonable care to prevent the prisoner from harming himself.

90 See, e.g., Fla. Stat. Ann. § 768.13 (West 2012); Mass. Gen. Laws Ann. ch. 112, § 12B (West 2012).

91 Restatement (Second) of Torts § 321.

92 Restatement (Second) of Agency § 213.

93 Restatement (Second) of Agency § 213.

94 Restatement (Second) of Torts § 430.

95 Some states have adopted the "substantial factor" test for proximate causation. Broader than the "foreseeability" formulation, the substantial factor test asks whether the defendant's negligent conduct was a substantial factor in the plaintiff's injury. If so, the defendant will be liable even though the plaintiff's injury was not a foreseeable result of the defendant's conduct. See, e.g., Derdiarian v. Felix Contracting Corp., 414 N.E.2d 666 (N.Y. 1980); Medcalf v. Wash.

Heights Condo. Ass'n, 747 A.2d 532 (Conn. App. Ct. 2000); Peter Zablotsky, "Mixing Oil and Water: Reconciling the Substantial Factor and Result-Within-the-Risk Approaches to Proximate Cause," *Cleveland State Law Review* 56 (2008): 1003.

96 Restatement (Second) of Torts § 433A.

97 See, e.g., 42 U.S.C. § 14503, stating that no liability exists if "the harm was not caused by willful or criminal misconduct, gross negligence, reckless misconduct, or a conscious, flagrant indifference to the rights or safety of the individual harmed by the volunteer"; Florida Good Samaritan Act, Fla. Stat. §768.13(2)(d), stating that no liability exists for "any person . . . who participates in emergency response activities under the direction of or in connection with a community emergency response team . . . if such person acts as a reasonably prudent person would have acted under the same or similar circumstances"; see, generally, Federal Emergency Management Agency, *Citizen Corps Volunteer Liability Guide: An Overview of the Legal Issues and Approaches to Address Liability for Emergency Volunteers*, available at http://www.citizencorps.gov/downloads/pdf/Citizen_Corps_Volunteer_Liability_Guide.pdf.

98 *Black's Law Dictionary,* 4th ed. (St. Paul, MN: West, 1968), 1185.

99 See, e.g., Ariz. Rev. Stat. Ann. §§ 26-314C, 26-301, which provides immunity for its emergency workers, including volunteers; Federal Emergency Management Agency, *Citizen Corps Volunteer Liability Guide*.

100 See, e.g., Nonprofit Risk Management Center, *State Liability Laws for Charitable Organizations and Volunteers*, available at http://sfcard.org/GoodSamaritanLaws.pdf; Federal Emergency Management Agency, *Citizen Corps Volunteer Liability Guide*.

101 See, e.g., Nev. Rev. Stat. § 41.500(1).

102 See, generally, *Emergency System for Advance Registration of Volunteer Health Professionals: Legal and Regulatory Issues,* Appendix D (May 2006), which identifies Good Samaritan laws and other laws that provide liability protection to volunteers in a specific state, available at http://www.publichealthlaw.net/Research/PDF/ESAR%20VHP%20Report.pdf.

103 See Clarence Wardell, III, and Yee San Su, *2011 Social Media + Emergency Management Camp—Transforming the Response Enterprise* (Alexandria, VA: CNA Analysis & Solutions, September 2012), 21, stating that "'Good Samaritan' laws, which are designed to legally protect citizens who provide help during a time of need, could potentially be used to insulate individuals who participate in VTCs [volunteer technology communities] or act autonomously to spread emergency-related information in good faith during a time of response." This statement is patently false.

104 42 U.S.C. §§ 14501–14505.

105 42 U.S.C. § 14503(b).

106 42 U.S.C. § 14503(a)(3).

107 42 U.S.C. § 14503(e).

108 42 U.S.C. § 14503(b).

109 42 U.S.C. § 14502(b). For example, New Hampshire has opted out of the Act.

110 See 42 U.S.C. § 14501.

111 Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 925 F. Supp. at 1125.

112 Commercial General Liability Coverage Form, § 1(a) (2006), available at http://www.sloanmason.com/files/pdf/ISO%20PDF%20CG%2000%2001%2012%2007.pdf.

113 Ibid., § 2.

114 Ibid., § 1(b)(1).

115 Ibid., § 2 (i).

116 Ibid., § 2 (p).

One Woodrow Wilson Plaza
1300 Pennsylvania Avenue, N.W.
Washington, DC, USA 20004-3027
202-691-4000
www.wilsoncenter.org

The Commons Lab advances research and non-partisan policy analysis on emerging technologies that facilitate collaborative, science based and citizen-driven decision-making. New tools like social media and crowdsourcing methods are empowering average people to monitor their environment, collectively generate actionable scientific data, and support disaster response.

http://CommonsLab.wilsoncenter.org

The Commons Lab is supported by the Alfred P. Sloan Foundation.