NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**UTILIZING SOCIAL MEDIA TO
FURTHER THE NATIONWIDE SUSPICIOUS ACTIVITY
REPORTING INITIATIVE**

by

Lynda A. Peters

September 2012

Thesis Co-Advisors: Patrick Miller
David Brannan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.		
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis
4. TITLE AND SUBTITLE Utilizing Social Media to Further the Nationwide Suspicious Activity Reporting Initiative		**5. FUNDING NUMBERS**
6. AUTHOR Lynda A. Peters		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.		
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The NSI process delineates that frontline personnel can solicit relevant behaviors observed by the public through in-person or telephonic interviews or online etips forms. It does not, in its current form, include the use of less formal social media tools such as text messaging, mobile-phone apps and social-networking sites like Facebook and Twitter, although some agencies are doing so. The literature demonstrates that the majority of people use social media and social networking sites to communicate every day, and more than three-quarters use it to participate in at least one community-focused group. Including social media technologies as an option for communicating a tip provides another means by which interested individuals can provide information about their observations.

Several case studies demonstrate that citizens motivated by the unselfish desire to contribute will do just that, whether or not solicited. Law enforcement agencies can leverage that enthusiasm by incorporating social media into efforts to develop SARs. The strategy requires that an agency devote resources sufficient to develop policies and to provide training to guide personnel and citizens. It also requires that agencies respond to received transmissions, recognize useful contributions, and make efforts to encourage further participation.

14. SUBJECT TERMS Homeland security, social media, law enforcement, suspicious activity report (SAR), nationwide suspicious activity report initiative (NSI), Web 2.0			**15. NUMBER OF PAGES** 135
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

i

THIS PAGE INTENTIONALLY LEFT BLANK

UTILIZING SOCIAL MEDIA TO FURTHER THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

Lynda A. Peters, Civilian
A.B., University of Michigan, 1982
J.D., DePaul University College of Law, 1986

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2012**

Author: Lynda A. Peters

Approved by: Patrick Miller
                 Thesis Co-Advisor

                 David Brannan
                 Thesis Co-Advisor

                 Daniel Moran, PhD
                 Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The NSI process delineates that frontline personnel can solicit relevant behaviors observed by the public through in-person or telephonic interviews or online etips forms. It does not, in its current form, include the use of less formal social media tools such as text messaging, mobile-phone apps and social-networking sites like Facebook and Twitter, although some agencies are doing so. The literature demonstrates that the majority of people use social media and social networking sites to communicate every day, and more than three-quarters use it to participate in at least one community-focused group. Including social media technologies as an option for communicating a tip provides another means by which interested individuals can provide information about their observations.

Several case studies demonstrate that citizens motivated by the unselfish desire to contribute will do just that, whether or not solicited. Law enforcement agencies can leverage that enthusiasm by incorporating social media into efforts to develop SARs. The strategy requires that an agency devote resources sufficient to develop policies and to provide training to guide personnel and citizens. It also requires that agencies respond to received transmissions, recognize useful contributions, and make efforts to encourage further participation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CHS   U.S. House of Representatives Committee on Homeland Security

CHDS   Center for Homeland Defense and Security

CIA   Central Intelligence Agency

CIIM   Community Internet Intensity Map

CIO   Chief Information Officer

CRS   Congressional Research Service

DHS   Department of Homeland Security

DYFI   Did You Feel It?

FEMA   Federal Emergency Management Authority

HUMINT   Human Intelligence

IACP   International Association of Chiefs of Police

IC   Intelligence Community

ILP   Intelligence-Led Policing

JTTF   Joint Terrorism Task Force

NASCIO   National Association of State Chief Information Officers

NSI   Nationwide Suspicious Activity Report Initiative

NYPD   New York Police Department

OSINT   Open Source Intelligence

P2P   Peer to Patent

SAR   Suspicious Activity Report

SMS   Short Message (or Messaging) Service

URL   Uniform (or Universal) Resource Locator; an address on the World Wide Web

USGS   U.S. Geological Survey

USPTO   U.S. Patent and Trademark Office

ACKNOWLEDGMENTS

First and foremost, I would like to thank my family and friends, whose incredible patience and support enabled me to make it through the rigors of the CHDS Master's Program. I look forward to emerging from my academic cocoon and rejoining you. In addition, I would like to express gratitude to three of my work colleagues, Karen Coppa, Yvonne Lagrone and Judi Gorske. Knowing that my Division at the Chicago Law Department was left in such capable hands allowed me to fully immerse myself during each in-residence session of classes in Monterey.

I would also like to thank the wonderfully talented instructors and staff at CHDS for helping me through the thesis process. To a person, everyone enthusiastically took the time to answer questions, offer helpful suggestions, provide amazing resources and insight, and share connections to folks around the country involved with the same issues. To those in Cohorts 1101 and 1102, I look forward to continuing to develop our professional and personal relationships without worrying about the next post or paper due on the Moodle. You are a truly amazing group of individuals, and I am grateful to count you as colleagues.

I owe a debt of gratitude to my advisors, Pat Miller and David Brannan, for providing encouragement and insight while I composed this thesis, and to Richard Bergin, for providing its genesis. Who knew that our conversation last fall about integrating Web 2.0 technology into law enforcement to improve efforts to protect communities would lead to this?

THIS PAGE INTENTIONALLY LEFT BLANK

I.   INTRODUCTION

Our national preparedness is the shared responsibility of all levels of government, the private and nonprofit sectors, and individual citizens. Everyone can contribute to safeguarding the Nation from harm.

Presidential Policy Directive/PPD-8

A.   PROBLEM STATEMENT

The long term goal of the Nationwide Suspicious Activity Report (SAR) Initiative (NSI) is for law enforcement agencies to participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information that is potentially terrorism related.[1] The SAR process contributes to the nation's security by enabling law enforcement agencies to develop information from citizens and synthesize it with information obtained from other sources. Under the NSI process, frontline personnel document relevant behaviors observed by officers or the public, vet the gathered information, and forward appropriate SARs to other entities. At present, the "information acquisition" portion of the SAR process involves information flowing from citizens to law enforcement personnel via one of several structured mechanisms: etips, telephone calls, or in-person contact with an officer.

The first information acquisition mechanism—etips—requires a citizen user to enter specific types of information into set data fields found on one or more screens via the Internet. Etips mechanisms are available on some agency Web sites and smart phone applications. The system is designed to enhance the accuracy of the information being transmitted by the citizen. Law enforcement is provided the opportunity to guide the flow of information by predetermining the types of data that can be submitted. While having the potential to elicit valuable information regarding criminal and terrorist-related incidents and offenders, the structured design of the information exchange process itself

---

[1] Program Manager, Information Sharing Environment, Nationwide Suspicious Activity Reporting Initiative Concept of Operations, Version 1. Nationwide SAR Initiative. http://nsi.ncirc.gov/ (December 2008), p. 3.

may deter some from using it. A similar type of problem may exist with respect to the other two information acquisition mechanisms, structured information solicitation through telephone calls and in-person interviews of citizens by officers.

The pervasive use of social media in society today has forever changed the way in which we interact and connect with one another.[2] A 2011 Pew Research Center survey report determined that two-thirds of adult Internet users communicate through at least one social networking site—such as Facebook or Twitter—each day, and half of all adults use social media.[3] In addition, various age groups, such as 73% of 18- to 29-year olds, 49% of 30- to 49-year olds, and 21% of those older than 50 years of age, are highly likely to use social media as a means of communication, especially on their cell phones.[4] The existing SAR process does not formally allow for the use of social media technologies as a mechanism for citizens to transmit information regarding the detection and prevention of terrorist acts to law enforcement agencies. As such, the SAR process in its present form lacks the capacity to fully capture and utilize information that is vital to the protection of the homeland.

B.   RESEARCH QUESTIONS

How can social media be utilized to engage members of the community and provide a conduit for citizens to disclose information that may develop into an intelligence product that can assist local law enforcement with the detection and prevention of terrorist acts?

1. How does utilizing a structured mechanism for social media communication, such as an etips (i.e., electronic tips) form for citizens to use to submit information to a law enforcement agency, vis-à-vis a one-way push of

---

[2] Jenise Henrikson, "The Growth of Social Media: An Infographic," Search Engine Journal, http://www.searchenginejournal.com/the-growth-of-social-media-an-infographic/32788/ (August 30, 2011).

[3] Mary Madden and Kathryn Zickurh, "Sixty-five Percent of Online Adults Use Social Networking Sites," Pew Research Center, Internet & American Life Project, http://pewinter.org/ (August 2011), p. 2.

[4] Pew Research Center, "Global Digital Communication: Texting, Social Networking Popular Worldwide," http://www.pewglobal.org/2011/12/20/global-digital-communication-texting-social-networking-popular-worldwide/ (December 20, 2011), p. 5.

information, compare to utilizing an unstructured social media mechanism that enables a two-sided conversation between citizens and law enforcement?

2. What conditions need to exist within a law enforcement agency for social media to provide a conduit for crime and terrorism-related information to flow from citizens?

C.   LITERATURE REVIEW

The body of literature that analyzes law enforcement usage of social media tools to engage the public in an effort to obtain crime and terrorism-related information is somewhat limited. This section will therefore include various government documents, research papers, journal articles, survey reports, news articles, and books that discuss and/or assess the use of social media more generally and by government for a range of purposes. This literature review is done in an effort to gain insight into how law enforcement can leverage this technological tool to better develop conversations with the public to obtain tips and information. The literature is grouped into the following categories: defining what constitutes social media, delineating the prevalence of its usage, demonstrating how government agencies can utilize social media tools, identifying derivative benefits and consequences, outlining potential obstacles to an agency's implementation of a social media strategy, and recommended policy considerations.

1.   Web 2.0 Technology Generally

A number of business-related news articles provide insight about what constitutes Web 2.0 technology, also referred to as social media, and how it can be utilized to provide benefit to a business or organization. Tim O'Reilly, whose company O'Reilly Radar coined the term Web 2.0, cites the web of connections that grow organically from the collective activity of Internet users and a company's role as enabler as central principles behind the success of business giants who have embraced social media.[5] O'Reilly defines eight core components that comprise Web 2.0:

---

[5] Tim O'Reilly, "What is Web 2.0? Design Patterns and Business Models for the Next Generation of Software," O'Reilly Network (September 30, 2005), p.6.

- Harnessing collective intelligence through architectures of user participation;

- Data is as or more important than software;

- Innovation through assembly of the massive amounts of data scattered across the Internet;

- Rich user experiences;

- Software above the level of a single device;

- Perpetual beta, meaning continuous change of software;

- Leveraging the long tail through customer self-service;

- Lightweight software and business models with cost effective scalability.

Musser, at O'Reilly Radar, describes Web 2.0 as thriving on network effects. Data gets richer the more people interact, and software applications become smarter the more people use them.[6] Social media technologies meet the expectations of Internet-era users because they are readily available, and versions easily improve over time, without any need for installations or upgrades.[7]

Figure 1.   Facebook Logo. [8]

Lowensohn describes Facebook as a free social-networking service that lets users connect with friends, co-workers, or others who share similar backgrounds or interests.[9] A user builds a profile and accumulates "friends," others with whom to communicate, by searching for them and creating a link between the user profiles. Text, photographs, video, and URL (i.e., a uniform or universal resource locator, an address on the World

---

6 John Musser, "Web 2.0 Principles and Best Practices," O'Reilly Radar, http://oreilly.com/ (Fall 2006), p. 2.

7 Ibid., p.5.

8 Google Images, retrieved June 16, 2012, from http://www.google.com/search?q=facebook+images&hl=en&prmd=imvns&tbm=isch&tbo=u&source=univ&sa=X&ei=zwPmT9etEuT40gG11uHkCQ&ved=0CE4QsAQ&biw=1366&bih=599.

9 Josh Lowensohn, "Newbie's Guide to Facebook," CNET, http://news.cnet.com/newbies-guide-to-facebook/ (August 1, 2007).

Wide Web) links can be posted and are shared with others depending on the privacy settings the user has selected, and updated information is automatically shared as soon as it is posted. In turn, recipients of posted information can send comments or indicate they "like" something by clicking on a provided link. Facebook is considered the largest of the social networking sites.[10]

Figure 2.   Twitter Logo.[11]

Strickland describes Twitter as a free social networking and micro-blogging service that enables a user to post and receive messages to a network of contacts.[12] Osimo explains that, rather than sending multiple emails or text messages, a user sends a single message to a Twitter account, and the service provider in turn distributes it to all of the user's followers.[13] Lagoudakis notes each message, referred to as a "tweet," is limited to 140 characters, and, when initially launched the provider did not allow the transmission of pictures.[14] That has since changed. Twitter can be used to facilitate a gathering, carry on a group conversation, or as with Facebook, send a status update to let others know what is happening at the moment. Users can search for others by using a search box, or they can browse and opt to follow the "tweets" of others.[15]

---

[10] WiseGEEK, "What is Facebook?" http://www.wisegeek.com/what-is-facebook.htm.

[11] Google Images, retrieved June 16, 2012, from http://www.google.com/search?q=twitter+images&hl=en&prmd=imvns&tbm=isch&tbo=u&source=univ&sa=X&ei=sgPmT-XTK4eC2wWp14zaCQ&sqi=2&ved=0CE0QsAQ&biw=1366&bih=599.

[12] Jonathan Strickland, "How Twitter Works," http://computer.howstuffworks.com/internet/social-networking/networks/twitter.htm; Gnoted Tech Blog, "What is Twitter and How Does it Work – Beginners Guide," http://gnoted.com/what-is-twitter-and-how-does-it-work-beginners-guide/ (February 8, 2009), .

[13] David Osimo, "Web 2.0 in Government: Why and How?," JRC Scientific and Technical Reports, European Communities (2008), p. 17.

[14] John Lagoudakis, "How Does Twitter Work?" http://johnlagoudakis.com/how-does-twitter-work/ (April 6, 2011).

[15] Gnoted Tech Blog, "What is Twitter."

Rettberg defines a blog, a contraction of the words "Web" and "log," or blogging as a cumulative process through which one or more individuals frequently writes brief posts on a topic of personal interest.[17] Postings chronicle the author's subjective view of and involvement with a particular topic, including the author's life experiences more generally.[18] The writing form is done in the first person, and most blogs encourage readers to leave comments, thus allowing an exchange of dialogue. Additionally, most blogs include links to other blogs regarding the same subject matter as well as other sources on the topic. The most dramatic growth of blogs occurred between 2003 and 2004 when the number of blogs tracked by search engine Technorati.com grew from 100,000 to 3 million.[19]

Figure 3.　　　Figure 3.　Depiction of a Hashtag.[20]

According to Golder and Huberman, tagging is the marking of content by its creator with descriptive terms or keywords and is a common method of organizing social

---

[16] Google Images, retrieved July 22, 2012, from http://www.google.com/search?q=images+for+blogs&start=10&hl=en&sa=N&prmd=imvns&tbm=isch&tbo=u&source=univ&ei=l0wMUI-mIYLpqgH6z_i8Cg&ved=0CFQQsAQ4Cg&biw=1366&bih=599.

[17] Jill Rettberg, *Blogging*, Cambridge: Polity Press (2009), pp. 4, 21.

[18] Ibid., p. 21.

[19] Ibid., p. 29.

[20] Google Images, retrieved June 16, 2012, from http://www.google.com/search?q=hashtag+images&hl=en&prmd=imvns&tbm=isch&tbo=u&source=univ&sa=X&ei=VgPmT9KcPIHl0QH80oXXCQ&ved=0CEYQsAQ&biw=1366&bih=599.

media content for ease of filtering, search, and navigation.[21] Collaborative tagging is the practice of allowing anyone, whether creator or reader, to freely insert keywords or tags. Twitter and more recently Facebook enable tagging of content by the insertion of a symbol such as a hash mark (#), also known as a hashtag. A simple search on the Internet provides information for users about how to apply a hashtag and how hashtags can be used to track content.[22] Golder and Huberman caution that information tagged by others will only be useful to the extent "the users in question make sense of the content in the same way, so as to overlap their classification choices" with those of the author.[23] Hotz reported that data-mining, marketing, and financial services companies also see the value of social media content, and they are willing to pay a premium for access to Twitter information.[24]

a.   *Social Media Usage*

Recent survey reports reveal the prevalence of social media usage in the United States. According to the Nielsen Company (Nielsen), across a snapshot of 10 major global markets, including the United States, social media sites reach over three-quarters of active Internet users and account for nearly one-quarter of the total time people spend on the Internet.[25] Nielsen found people most typically access social media through their computers (97%) and/or mobile phones (37%).[26] Madden and Zickuhr, through the Pew Research Center, determined the percentage of all adult Internet users who utilize social media has risen dramatically in the last six years, from 8% in 2005 to 65% in 2011.[27]

---

[21] Scott Golder and Bernardo Huberman, "The Structure of Collaborative Tagging Systems," Cornell University Library, http://www.hpl.hp.com/research/idl/papers/tags/tags.pdf (2005), p. 1.

[22] Twitter Fan Wiki, http://twitter.pbworks.com/w/page/1779812/Hashtags.

[23] Golder and Huberman, "Collaborative Tagging Systems," p. 7.

[24] Robert Hotz, "Decoding our Chatter," *Wall Street Journal* (October 1, 2011).

[25] Nielsen, "State of the Media: The Social Media Report, Third Quarter," http://www.nielsen.com/ (2011), p.1.

[26] Ibid., p. 6.

[27] Madden and Zickuhr, "Online Adults," p. 3; J. Brenner, "Pew Internet: Social Networking (Full Detail)," Pew Research Center's Internet & American Life Project http://www.pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx (March 29, 2012).

Hutton and Fosdick, through a Universal McCann global media study, determined social networking sites surpass all other means of keeping in touch with people, including face-to-face contact.[28] The study concluded people are more likely to use social networking sites to read and discuss personal topics than blogs and forums. In contrast, blogs have become sources of specialized and expert information, and even news.[29]

The Pew Research Center's Project for Excellence in Journalism, determined that people under the age of 40 are more likely to obtain local news and community information from the Internet than from television or a newspaper.[30] In contrast, people over the age of 40 are more likely to obtain this type of information from a newspaper. In terms of social networking sites, Hampton, et al., through the Pew Research Center, found that 92% of people use Facebook, followed by MySpace (29%), LinkedIn (18%) and Twitter (13%).[31] Facebook and Twitter are used much more frequently, however, than LinkedIn or MySpace. Approximately one-half of Facebook users (52%) and one-third of Twitter users (33%) engage with those sites daily.

Business author Qualman deems messaging through social media to be more easily managed than through email because messaging through social media more closely approximates a real conversation among friends.[32] Social media functions in a fluid manner in contrast to email:

> Open conversations within social media have an easier flow to them and replicate normal conversation. Also, the conversational content is broken down into bite-size chunks and is associated into more easily recognized compartments rather than just a long and daunting slew of 45 emails that you need to wade through systemically.

---

[28] Graeme Hutton and Maggie Fosdick, "The Globalization of Social Media," *Journal of Advertising Research* (December 2011), p. 567.

[29] Ibid.; Dictionary.com, www.dictionary.reference.com/browse/blog, retrieved July 9, 2012.

[30] Pew Research Center, "How People Learn About Their Local Community," Project for Excellence in Journalism, Pew Internet & American Life Project, Knight Foundation (September 2011), pp. 6-7.

[31] Keith Hampton et al., "Social Networking Sites and Our Lives," Pew Research Center, Pew Internet & American Life Project, http://pewinternet.org (June 2011), p. 13.

[32] Eric Qualman, *Socialnomic, How Social Media Transforms the Way We Live and Do Business*, Hoboken, NJ: John Wiley & Sons (2011), p. 51.

Boston College's decision to not distribute email accounts to incoming freshman for the class of 2013, for example, is a clear sign of the times.[33]

One explanation for the prevalent usage of social media may be its participatory nature. Collin et al. term social media a "participatory media environment" because it enables users to creatively produce content and empowers them to begin and sustain connections with other people.[34] Drapeau and Wells describe Web 2.0 as "dynamic and participatory" because it represents the zone where software interacts with many users and across many devices, and people are able to shift effortlessly between author and audience status.[35] Rettberg observes, "We have moved from a culture dominated by mass media, using one-to-many communication, to one where participatory media, using many-to-many communication, is becoming the norm."[36]

Henry Jenkins, author of *Convergence Culture*, suggests social media can be used to circulate data across different pop-culture media systems, such as by allowing users to post comments as they view television programs and online news reports.[37] Jenkins terms this recent development "convergence thinking" and concludes social media is impacting the very nature of relationships between media producers, audiences and content, thereby changing the way media is both created and consumed.[38] In this context, convergence is defined as:

---

[33] Ibid., pp. 51–52.

[34] Philippa Collin et al., "The Benefits of Social Networking Services," Cooperation Research Centre for Young People, Technology and Wellbeing, Inspire Foundation, Australia, https://docs.google.com/viewer?a=v&q=cache:2TNJ3Ghyn2kJ:www.interactivemediarelease.com/download.php?f%3D0neo1k_FINAL_The_Benefits_of_Social_Networking_Services_Lit_Review.pdf+The+Benefits+of+Social+Networking+Services&hl=en&gl=us&pid=bl&srcid=ADGEESiI9SyXCv7mh-efCI0yRw1KzWjhJx3Y5EqZL4gobc0OiGKb29MDUyVnOq-LZUU6Dn6K47Br8aj8BRZvRrmAMCnFoLkdJeRQHeHnSVarTdGi4K7mOh37IjW5VKdG5nJt0KAHJLMp&sig=AHIEtbSHpRqPc5Y1xtKXsIqiBAwQKOLQhQ, p. 9.

[35] Mark Drapeau and Linton Wells, "Social Software and National Security: An Initial Net Assessment," Center for Technology and National Security Policy, National Defense University (April 2009), p. 1.

[36] Rettberg, *Blogging*, p. 31.

[37] Henry Jenkins, *Convergence Culture, Where Old and New Media Collide*, New York University Press, (2006), p. 3.

[38] Ibid., pp. 12, 16.

both a top-down corporate driven process and a bottom-up consumer driven process. Corporate convergence coexists with grassroots convergence. Media companies are learning how to accelerate the flow of media content across delivery channels to expand revenue opportunities, broaden markets, and reinforce view commitments. Consumers are learning how to use these different media technologies to bring the flow of media more fully under their control and to interact with other consumers. The promises of this new media environment raise expectations of a freer flow of ideas and content. Inspired by those ideals, consumers are fighting for the right to participate more fully in their culture.[39]

Jenkins concludes the very nature of social media, which enables participation and collaboration, as well as the fact convergence is changing the ways in which television and news outlets operate means companies are at a critical juncture and may be forced to renegotiate their relationship with consumers.[40]

b. *Derivative Benefits and Consequences*

A recent Pew Research Center survey report demonstrates a number of benefits are derived from using social media. Hampton et al. conducted a national survey of 2,255 American adults, which included 1,785 Internet users and 975 social media users. Regression analysis was utilized to control for demographic factors. The report concludes those who use social networking sites derive a range of benefits. For example, users are found to have more close relationships, to receive more social support, to be more likely to be open to opposing points of view, and to be more politically engaged than most people.[41] Americans who use social networking sites through the Internet (46%) are more trusting of people than non-Internet users (27%).[42] And 74% of Americans belong to at least one community group or neighborhood association that focuses on issues or problems in their community, up from 65% in 2008.[43]

---

[39] Ibid., p. 18.

[40] Ibid., p. 243.

[41] Hampton et al., "Social Networking Sites," pp. 4–5.

[42] Ibid., p. 32.

[43] Ibid., p. 37.

Collin et al. conducted an extensive literature review for the Cooperative Research Centre for Young People, Technology and Wellbeing in Australia. The report summarizes findings on the topic of social networking services, defined as social media that enable young people to construct an online profile, select users with whom to share content, and view content created by others.[44] The literature includes international articles and reports written by academics, industry, and both government and non-government researchers, with a focus on Australian users. The literature covers disciplines ranging from education, sociology, and political science to cultural studies and health.

The broad range of benefits youth derive from engaging through social networking includes:

- Achievement of social media literacy;
- Obtaining an education that supplements school-based learning;
- Encouragement of creativity;
- Promotion of self-identity and self-expression;
- Strengthening of interpersonal relationships;
- Creation of a sense of belonging and collective identity;
- Civic engagement and political participation.[45]

Social networking technologies are perceived to dramatically transform the relationships young people have with one another, their families, and their communities.[46]

Youth use the Internet and social media not just for information and entertainment but, increasingly, as a means of communication with one another.[47] Risks from release of personal information, invasion of privacy, predation, and cyberbullying certainly present challenges for youth as well as their parents.[48] Research indicates, however, that "online risks are not radically different in nature or scope than the risks

---

[44] Collin et al., "Benefits of Social Networking."

[45] Ibid., pp. 12–20.

[46] Ibid., p. 3.

[47] Ibid., p. 8.

[48] Ibid., p. 11.

minors have long faced offline, and minors who are most at risk in the offline world continue to be most at risk online."[49] The authors conclude that the rise of social networking usage has fostered new communication and social connection patterns between young people that are not seen in older groups. As such, they recommend action be taken to enhance intergenerational communication to prevent a digital divide between youth, their parents, and older members of society.[50]

Qualman includes the erosion of written skills and an increasing fear of public speaking as direct consequences experienced from using social media as a means of communication.[51] Social media users may need additional guidance in business communications, project planning, and overall management skills. The social media-using generation is less likely to understand business-hour versus personal-life boundaries because, to them, "it's not a 9-to-5 world, it's a 24/7 world, and it's up to the individual to properly balance the hours in the day."[52] Despite these downsides, social media users reap benefits, including an understanding of one's place within the global community, possession of more creative and collaborative tendencies than non-users, expectation of a better work-life balance, and an enhanced ability to prioritize and multitask.[53]

2. Government Usage of Web 2.0 Technology

Adoption of Web 2.0 platforms and tools to help improve citizen engagement with government and collaboration between the two entities is the essence of Government 2.0. A research paper by Drapeau and Wells defines the four usages of social media by government as the sharing of information within one or more units of an agency (i.e., inward sharing), the sharing of internal information by an agency with other federal, state, local, or tribal agencies (i.e., outward sharing), the ability for government to obtain

---

[49] Ibid.

[50] Ibid., p. 21.

[51] Qualman, *Socialnomic*, p. 58.

[52] Ibid., p. 59.

[53] Ibid., p. 58.

input from citizens and other persons outside government (i.e., inbound sharing), and the ability of government to share information with and/or empower the public (i.e., outbound sharing). [54] The usages are depicted in Figure 4.
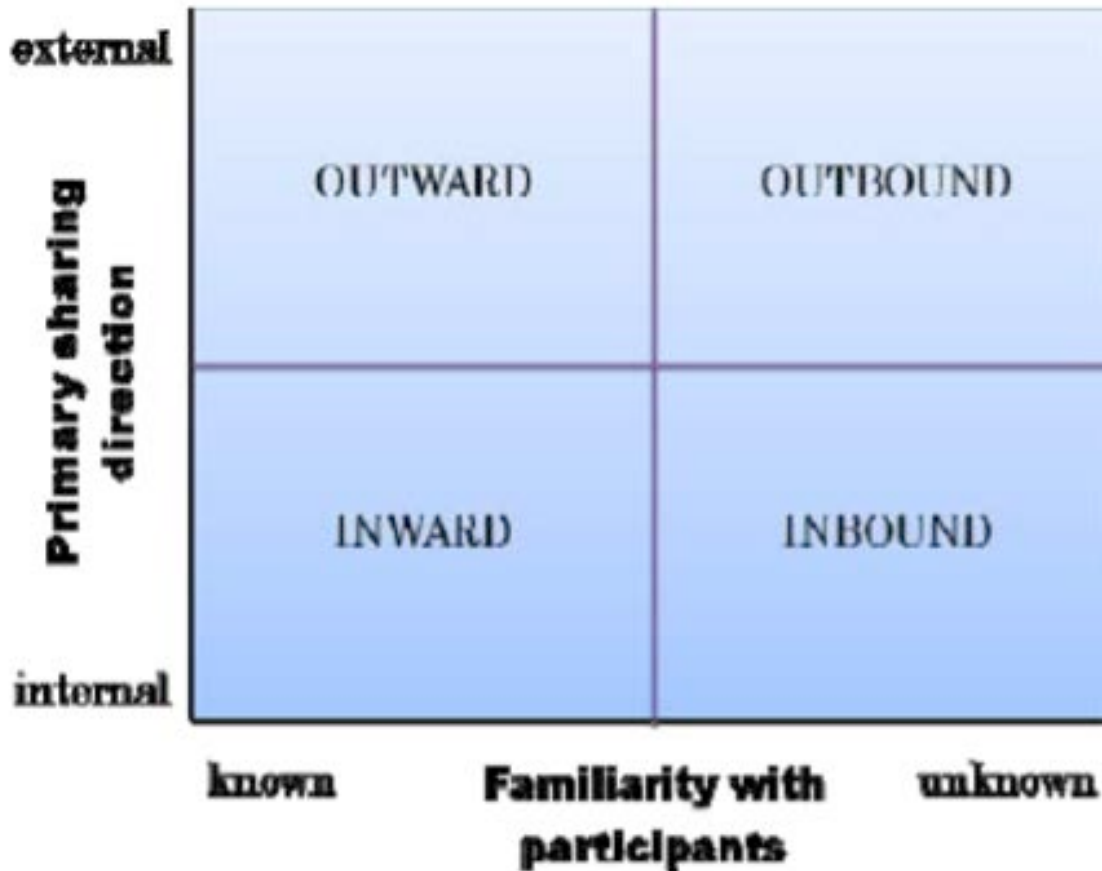
Figure 4.   Four-Quadrant Government Social Software Framework.

NASCIO, the National Association of Chief Information Officers, conducted a survey in July and August of 2010 to learn more about social media adoption by state governments across the country.[55] The survey included questions about adoption trends

---

[54] Drapeau and Wells, "Social Software," p.6; CIO Counsel, "Guidelines for Secure Use of Social Media by Federal Departments and Agencies," http://www.cio.gov (September 2009), pp. 7–8.

[55] National Association of Chief Information Officers [NASCIO], "Friends, Followers, and Feeds: A National Survey of Social Media Use in State Government," www.nascio.org/publications/documents/nascio-socialmedia.pdf, p. 2.

and current application usage. Individuals from 43 states and territories representing approximately 79% of the U.S. population responded. Key survey findings include the following:

- Social media tools are being actively adopted and used throughout state governments;

- The most common reasons for adoption are the enhancement of communication, citizen engagement, and outreach efforts, along with the low cost associated with social-media tools (e.g., 98% of the technology is free);

- Challenges with implementing social-media tools involve security, terms-of-service legal issues, privacy concerns, records management constraints, and the determination of what constitutes acceptable use.[56]

While many state governments got involved with social media simply to stay current with available technology, NASCIO determined the "migration of social media tools onto mobile platforms and the sheer ubiquity of the latter increasingly make social media tools a critical communications channel that states can take advantage of to extend their reach across all demographics through very cost-effective means."[57]

Drapeau and Wells believe social media activities involve important behavioral constructs which enable, inspire, engage and influence users.[58] Advantages for government include the promotion of networking and collaboration capabilities for agencies with groups and individuals outside government, improved speed in decision-making by agency personnel, increased agency adaptability and agility, and the ability to provide a platform for people who are already having conversations.[59]

Osimo conducted several case studies to provide customer-driven support to European Union policy makers assessing whether and to what extent Web 2.0 technologies can integrate into government operations. The research attempted to address whether the technologies are relevant in the government context, in what way they are likely to have an impact, the significance of the impact, and how technology use can be

---

[56] Ibid., p. 5.

[57] Ibid., p. 3.

[58] Ibid., p. 3.

[59] Ibid., pp. vi, 11.

implemented.[60] The study found specific benefits occur when citizen-users take a proactive role with government, such as enabling a governmental entity to better understand the public's needs through feedback and rating systems, enabling citizen awareness and monitoring of government activities (i.e., transparency), and involving the public in certain decision-making processes.[61] Additionally, social media technologies allow better collaboration within and across agencies, thereby reducing silo effects.[62]

In addition to benefits, Osimo determined Web 2.0 initiatives carry certain risks. The primary challenge with any collaborative effort is to ensure people participate and contribute.[63] Social media technologies, like the Internet more generally, are typically used by a certain group of individuals. Thus, government needs to be cautious about providing a greater voice to those who already have one. Agencies also need to monitor feedback on rating sites to intercede when citizens launch personal attacks against employees so comments do not have a negative impact on trust and collaboration efforts.[64] Government needs to educate citizen users on potential privacy issues and the consequences of publishing information on government-sponsored social media sites. Finally, the low quality of citizen contributions may impede the hunt for useful information, and government needs to militate against ceding too much control through excessive transparency.

The CIO Council recently created guidelines for federal agencies intending to use social media tools to collaborate and communicate among employees, partners, other agencies, and the public. The guidelines focus on secure implementation of social media technologies, and they caution that blogs, social networking sites, and Wikis (i.e., "What I Know Is" Web sites that allow anyone to add, delete, or edit content) are vulnerable to several cyber-attack methods thus necessitating the secure enabling of resources.[65]

---

[60] Osimo, "Web 2.0 in Government," p. 7.

[61] Ibid., pp. 9, 42.

[62] Ibid., p. 9.

[63] Ibid., p. 42.

[64] Ibid., p. 43.

[65] CIO Council, "Secure Use," pp. 9, 17.

a.   Law Enforcement and Social Media

Cohen reported six ways law enforcement agencies can use social media to fight crime. Social media can be used to disseminate an agency's police blotter, the chronicle of crime and arrest events, in real time as the medium enables officers to transmit information essential to the community about a crime as they respond.[66] News reporters, in turn, can obtain facts directly from this stream of online data. Use of social media for this purpose is a one-sided push of information out to the community.

Social media can also be used to upload digital wanted posters to the Internet with calls for help from the community in identifying unknown criminals.[67] The interactive nature of social media and networking sites and the fact they can be updated constantly offer the ability for residents to quickly and easily respond to requests for information by law enforcement. Social media acts as a force multiplier by enabling citizens to anonymously contribute leads and relevant information to law enforcement agencies through etips (i.e., electronic tips) mechanisms. For example, information sent via text, web chat, or another secure form of social media can enable a citizen to provide useful information without the fear of retribution. These types of calls to the community for help utilize social media in a two-sided exchange of information with law enforcement agencies.

Cohen next outlines two uses of social media that entail law enforcement data mining of information posted online by citizens. The "social media stakeout" involves searching social media sites using particular key words and phrases to obtain real-time information to develop strategic, tactical, and operational direction for officers.[68] Social media can also serve as a means for officers to infiltrate street gangs that engage one another through social networking sites such as Twitter and Facebook. The final way for law enforcement to use social media is as a mechanism to monitor

---

[66] Lori Cohen, "Six Ways Law Enforcement Uses Social Media to Fight Crime," http://mashable.com/2010/03/17/law-enforcement-social-media (March 17, 2010), p. 1.

[67] Ibid., p. 2.

[68] Ibid., p. 3.

crowd activity and provide real-time alerts, such as traffic safety messages, to the community as situations unfold.[69] This one-sided push of information by law enforcement can also be utilized to disseminate alerts about crime patterns.

Osimo determined social media enables citizens to take a more proactive role and thereby impact the way in which laws are enforced in their communities. Citizens, for example, can monitor other citizens and "publicly shame them" to influence compliance.[70] Citizens can focus efforts of local law enforcement by monitoring and highlighting problems that most concern the community.[71] Additionally, law enforcement agencies can co-opt citizen collaboration by disseminating video footage and seeking assistance in identifying criminals caught on surveillance cameras.

In 2010, the International Association of Chiefs of Police (IACP) Center for Social Media proposed law enforcement agencies incorporate social-media tools into policing efforts due to the exponential growth of Internet and social media usage by the public:

> The characteristics of community collaboration and interactive communication that are at the core of social media, lend directly to the core of democratic culture, and allow for positive community interaction and effective delivery of services. Community policing, investigations, and other strategic initiatives can all be enhanced with the effective use of social media.[72]

A 2011 IACP Mobile Fact Sheet deems social media and mobile technology the "next generation 911" because people present at the scene of an incident are able to take and share pictures and video that could contribute to suspicious activity reporting, crime reporting, and improved situational awareness for first responders.[73]

---

[69] Ibid., p. 4.

[70] Osimo, "Web 2.0 in Government," p. 36.

[71] Ibid., p. 37.

[72] International Association of Chiefs of Police [IACP], IACP National Law Enforcement Policy Center, "Social Media, Concepts and Issues Paper" (September 2010), p. 1.

[73] IACP, "Mobile Fact Sheet" (March 2011).

The IACP Center for Social Media conducted surveys in 2010 and 2011 that provide some insight into the current level of integration of social media tools by law enforcement agencies. The surveys were directed to federal, state, local, tribal, and academic law enforcement agencies. The 2011 IACP survey concluded 88% of the 800 responding law enforcement agencies use some form of social media to engage with the public, up from 81% of 728 agencies in 2010.[74] The 2011 IACP survey determined that law enforcement usage of social media falls within one or more of the following four categories: improving public perception of and community relationships with officers; pushing crime, emergency alert, and other information out to members of the public; soliciting crime and terrorism-related tips from the public to facilitate detection and prevention efforts; and developing intelligence through data mining.

The 2011 IACP survey results demonstrate nearly 43% of law enforcement agencies surveyed enlist social media for the specific purpose of reputation management.[75] In addition, a number of law enforcement agencies use social media as a recruitment tool (26%), to disseminate crime prevention advice (46%), to notify the public of emergency and disaster-related information (44%), and to broadcast crime problems within certain neighborhoods (50%). These forms of social media usage involve information flowing in a single direction—from the law enforcement agency to members of the public. Use of social media for this purpose is one-sided and does not allow for input from members of the public.

The 2011 IACP survey also demonstrates a number of law enforcement agencies use social media to solicit tips on crime (40%) and, most commonly, to assist active criminal investigations (71%). Use of social media for these purposes is two-sided as it allows for input from the public in response to messages posted by law enforcement. Further, nearly 56% of law enforcement agencies reported using social media to develop intelligence, and 32% specifically use it to monitor chatter between individuals. Such data mining activities encompass, by far, the fastest growing usage of social media by

---

[74] IACP, "2011 IACP Social Media Survey," IACP Center for Social Media, p. 1; IACP, "2010 IACP Social Media Survey," IACP Center for Social Media, p. 1.

[75] IACP, "2011 IACP Social Media Survey," p. 3.

law enforcement. While the 2010 IACP survey did not ask about data mining activities, only 4% of agencies indicated they used social media for a use not specified in the questionnaire.[76]

As noted above, 800 agencies participated in the 2011 IACP survey, and 728 participated in the 2010 survey. These numbers represent less than 5% of the approximately 17,000 law enforcement agencies operating today in the United States so the data does not present a complete picture of social media usage by all agencies in the country.[77] It is unknown to what extent the IACP findings are representative of social media usage by the greater number of law enforcement agencies. Additionally, the IACP surveys contain no analysis of the benefit derived by law enforcement agencies from utilizing social media for any of the enumerated purposes, including using the tool to develop crime and terrorism-related information by facilitating conversations with citizens.

b. *Homeland Security Efforts and Social Media*

Literature on the use of social media by government entities in the context of homeland security efforts is mostly confined to government documents. A paper recapping a July 2009 Center for Homeland Defense and Security (CHDS) Ogma workshop found the use of social media by federal, state, and local homeland security and public-safety agencies is "ad-hoc and relatively unorganized. A few agencies are using these tools in some manner; some agency's policies prohibit their use, while others appear not even aware of their existence."[78] CHDS Ogma Workshop participants acknowledged information control by agencies such as law enforcement is no longer possible since the advent of social media.[79] Participants concluded members of the public

---

[76] IACP, "2010 IACP Social Media Survey," p. 3.

[77] Federal Bureau of Investigation [FBI], Uniform Crime Reports, http://www.fbi.gov/about-us/cjis/ucr/ucr.

[78] "Ogma Workshop: Exploring the Policy & Strategy Implications of Web 2.0 on the Practice of Homeland Security: Summary," Center for Homeland Defense and Security, www.chds.us/ (July 7, 2009), p. 9.; see also J. Woodcock, "Leveraging Social Media to Engage the Public in Homeland Security," master's thesis, Naval Postgraduate School (September 2009).

[79] "Ogma Workshop," p. 10.

safety and law enforcement communities need to actively understand how to communicate with the general public using the same tools citizens are using to engage with one another.

Fresenko conducted three cases studies to evaluate the integration of social media by government agencies, such as fusion centers, engaged in homeland security efforts and determined some citizens are demanding local law enforcement capitalize on social media technologies to assist investigations.[80] Fresenko found it more practical and realistic for fusion centers to liaise with law enforcement agencies, however, and not to engage directly with the public.[81] Fusion centers that use social media to conduct two-way exchanges of information with the public could conceivably do more harm than good by cutting out direct communication between the public and first responders in law enforcement and emergency management agencies.[82] Findings from the case studies present limited utility in assessing the extent of social-media usage and the benefits derived therefrom in the homeland security context for the very reasons the author notes: the studies are not indicative of the policies and practices in use at all fusion centers, public safety departments, and law enforcement agencies across the country.[83]

c. *Social Media as an Open-Source Intelligence Tool*

Several government documents outline the use of social media as an Open Source intelligence tool (OSINT). In 2006, the Director of National Intelligence defined "open source information" through Intelligence Community Directive Number 301 to be information that is publically available and can be lawfully obtained by request, purchase, or observation.[84] The directive mandates all open-source information be made available across the Intelligence Community (IC) unless expressly prohibited by law. Open-source

---

[80] Victoria Fresenko, "Social Media Integration into State-Operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges," master's thesis, Naval Postgraduate School (December 2010), p. 39.

[81] Ibid., p. 40.

[82] Ibid., p. 41.

[83] Ibid., p. 50.

[84] Director of National Intelligence, "National Open Source Enterprise, Intelligence Community Directive Number 301," United States Office of the Director of National Intelligence (July 11, 2006).

information generally falls within one of four categories: (1) information widely available to anyone, (2) commercial data, (3) expert opinion data, and (4) limited-issue "gray" literature produced by the private sector, government agencies, and academia.[85] Social media is included in the first category due to its very nature.

The U.S. House of Representatives Committee on Homeland Security (CHS) considers social media to be an OSINT tool that federal, state, and local law enforcement agencies should use to develop timely, relevant, and actionable intelligence to secure the homeland against potential threats.[86] In particular, the CHS opined open source information should be used to supplement classified data as well as constituting a potential stand-alone source of valuable intelligence.[87] A 2008 CHS Open Source Survey determined 81% of state, local, and tribal survey respondents collect and utilize open-source information and intelligence as a tool to inform their community safety efforts.[88]

The CHS report concludes that, due to its nature as publicly available information, data mining from social media should be included along with information gleaned from periodicals, scientific and academic journals, news media, and the Internet generally as another potential source of OSINT. The CHS Open Source Survey does not include the use of social media as a mechanism for law enforcement agencies to directly engage the public for the purpose of obtaining crime and terrorism-related information.

In a Congressional Research Service (CRS) report for Congress, Best and Cumming similarly explore the increasing use of open-source information in light of technological advances and the relative ease of accessing volumes of information on the Internet.[89] Their report notes three prevailing views within the IC on the utility of open-

---

[85] United States Congress, Joint Economic Committee, Majority Staff, "Giving a Voice to Open Source Stakeholders: A Survey of State, Local and Tribal Law Enforcement," Washington, D.C.: U.S. House of Representatives, Committee on Homeland Security (September 2008), p. 4, citing A. Sands, "Integrating Open Sources into Transnational Threat Assessments," in J. Sims, and B. Gerber, *Transforming U.S. Intelligence*, Washington, D.C.: Georgetown University Press (2005), p. 65.

[86] Ibid., p. 1.

[87] Ibid., p. 6.

[88] Ibid., p. 4.

[89] Richard Best and Alfred Cumming, "CRS Report for Congress, Open Source Intelligence (OSINT): Issues for Congress," Congressional Research Service, Order Code RL 34270 (January 28, 2009), p. 1.

source information to develop intelligence products. First, some policymakers believe less value is derived through open-source collection methods because secrets and insight into an adversary's plans and intentions can only be obtained clandestinely.[90] A second viewpoint holds that open-source information provides not only an "important contextual supplement to classified data," but also a potential source of intelligence on its own.[91] The third viewpoint advocates a middle-ground position: open source information will never provide the ultimate evidence about a threat or law enforcement issue (i.e., the proverbial smoking gun), but it is instrumental in enabling analysts to better focus clandestine collection activities.

Best and Cumming present a somewhat broader definition of open-source information than the CHS Open Source Survey, as their definition specifically includes "computer-based information" within the types of widely available media.[92] In particular, their report notes the increasing value of information derived from Internet blogs.[93] According to some within the IC, blogs provide "a lot of rich information that are telling us a lot about social perspective and everything from what the general feeling is, to . . . people putting information on there that doesn't exist anywhere else."[94] This perception may be building due to an infusion of new employees in the IC workforce who are familiar, and therefore comfortable, with accessing Internet-based open-source information through their previous academic and/or professional endeavors. As with the CHS Open Source Survey, the Best and Cumming report advocates the mining of social media data to enhance open-source intelligence efforts, but it contains no mention of using social-media conversations to directly engage the public to encourage the provision of helpful tips for use by law enforcement agencies.

---

[90] Ibid., p. 2.

[91] Ibid., p. 3.

[92] Ibid., p. 6.

[93] Ibid., p. 7.

[94] Ibid., citing B. Gertz, "CIA Mines 'Rich' Content from Blogs," *Washington Times* (April 19, 2006), p. 4.

More recently, the news media has recounted efforts by the Central Intelligence Agency (CIA) to harness social media to obtain open-source information. Sullivan reported that the CIA bought stake in a company that was developing technology software to monitor social media conversations.[95] CIA interest was focused at that point, in October 2009, on the surreptitious monitoring of chat rooms, blogs, and social media outlets such as YouTube. Fitsanakis reported recently that CIA efforts continue to focus on mining publicly available information through its Open Source Center.[96] The CIA employs the center to "monitor up to five million tweets a day, and produces daily snapshots of global opinion assembled from tweets, Facebook updates and blog posts."[97] Vermeulen (2011) reports the Open Source Center accomplishes this effort through data mining software designed to automatically collect, search, and analyze words, sounds, and phrases.[98] These news articles reveal the CIA's utilization of social media continues to remain limited to the data mining realm.

d. Social Media as a Human Intelligence Tool

Government documents discussing the use of social media as a tool to garner human intelligence are very limited. In 2008, the Director of National Intelligence defined "human intelligence" (HUMINT) through Intelligence Community Directive Number 304 as a category of information obtained either clandestinely or overtly from human sources.[99] The definition, however, does not specify whether HUMINT necessitates personal contact with the human source in question or includes conversations

---

[95] James Sullivan, "Harnessing Open Source Intelligence: Social Media and the CIA," http://www.findingdulcinea.com/news/Americas/2009/October/Harnessing-Open-Source-Intelligence--Social-Media-and-the-CIA.html#0 (October 21, 2009).

[96] Joseph Fitsanakis, "Analysis: CIA Open Source Center Monitors Facebook, Twitter, Blogs," http://intelnews.org/2011/11/08/01-861/#more-7508 (November 8, 2011).

[97] Ibid.; see also Brian Fung, "The Intelligence Community Gets Social," Washington Post, http://www.washingtonpost.com/blogs/innovations/post/the-intelligence-community-gets-social/2011/09/13/gIQAvlrldK_blog.html (September 19, 2011); Associated Press, "CIA Analysts Comb Social Media for Trouble Spots," http://www.npr.org/2011/11/04/142029141/cia-analysts-comb-social-media-for-trouble-spots (November 4, 2011).

[98] Mathias Vermeulen, "Open Source Intelligence and Social Media Monitoring," *Privacy International*, https://www.privacyinternational.org/article/bbi-open-source-intelligence-and-social-media-monitoring (November 30, 2011).

[99] Director of National Intelligence, "National Open Source Enterprise, Intelligence Community Directive Number 304," United States Office of the Director of National Intelligence (July 9, 2009).

facilitated by technology, such as social media. The U.S. Army's definition of HUMINT is somewhat broader: "the collection of information by a trained human intelligence collector from people, and their associated documents and media sources."[100] Neither of these definitions, however, provides insight into how an agency can implement social-media tools to obtain information from citizens or what conditions must be present to foster such social-media exchanges.

Mumm argues in a journal article that the prevalence of cellular telephone and Internet technology necessitates the U.S. military strengthen its human intelligence gathering efforts through social media. Traditional HUMINT efforts are constricted by the fact an intelligence collector has a finite number of human sources and typically meets with them in person.[101] U.S. Army commanders should expand HUMINT efforts by creating a social-media network that broadcasts messages directly to the local community, enables locals to communicate information directly back, and circulates the results of operations, thereby providing immediate and positive feedback about the contributions.[102] Mumm's journal article is an isolated mention of social media as a mechanism to actively engage the public in providing information that benefits local intelligence gathering efforts. The article, however, contains no literature review or methodology and thus provides no academic support for the author's opinion.

e.   *Social Media Usage during Emergencies and Disasters*

Currie authored a report summarizing findings compiled through a survey of individuals and organizations and an expert roundtable including members of government and private business. Currie advises organizations that protect health and safety to remember social media use entails more than just pushing important alerts and notifications out to the public; it is also a conduit for receiving communication from and

---

[100] Nicholas Mumm, "Crowdsourcing: A New Perspective on Human Intelligence Collections in a Counterinsurgency," *Small Wars Journal*, http://smallwarsjournal.com/node/12036 (January 3, 2012).

[101] Ibid., p. 2.

[102] Ibid., pp. 7–8.

about citizens and conversing with them during an emergency situation.[103] The major challenges associated with two-way exchanges of information via social media include a lack of confidentiality regarding potential patient information and the danger associated with relying upon nonverified reports.[104] Nonetheless, Currie advocates for using social media as the speed of information spread through this mechanism not only enhances two-way communication, it also provides an edge for first responders by speeding up situational awareness.

In a CRS report for Congress, Lindsay termed current government agency use of social media during disasters and emergencies "passive," as it merely involves the dissemination of information to citizens and the receipt of user feedback from citizens, akin to customer service commentary.[105] In contrast, the author argues for a more systematic approach to incorporating and using social media technologies, such as to:

- Disseminate emergency communications and issue warnings;
- Receive victim requests for assistance;
- Monitor user activities and observations to gain situational awareness;
- Upload images to create damage estimates.

Current emergency communication systems typically engage in one-way messaging from an agency to the public. Social media could alter that relationship by allowing information to flow in multiple directions, thereby assisting officials tasked with compiling lists of dead and injured persons and contact information for the victim's family and friends.[106]

---

[103] Donya Currie, "Special Report: Expert Round Table on Social Media and Risk Communication During Times of Crisis: Strategic Challenges and Opportunities," American Public Health Association, http://www.apha.org/NR/rdonlyres/47910BED-3371-46B3-85C2-67EFB80D88F8/0/socialmedreport.pdf (2009), pp. 2–3.

[104] Ibid., p. 2.

[105] Bruce Lindsay, "Social Media and Disasters: Current Uses, Future Options, and Policy Considerations," Congressional Research Service, Order Code R41987 (September 6, 2011), p. 1.

[106] Ibid., p. 5.

f.   Citizen Journalism and Situational Awareness

Rettberg describes citizen journalism in her book *Blogging* as the reporting of events as they happen by the very people who experience them.[107] The real-time nature of the information being transmitted means even mainstream media use information on blog posts when reporting on events. A survey of blog readers conducted by the advertising company Blogads further demonstrates the utility of information provided through this mechanism: people visit blogs because they are viewed as more credible than reports generated by mainstream media.[108] A reader either trusts or distrusts what is read, based upon a perception about the author. Blog posts are perceived to be based upon personal authenticity, whereas traditional journalism is perceived to rely upon institutional credibility and reputation.[109] Rettberg notes that, although personal authenticity can be faked, the truth will eventually come out, and the backlash against a deceptive author will be powerful.[110]

Allan writes in a journal article that ordinary citizens appropriate social-media technologies in order to build their own networked communities and challenge the traditional dynamics of top-down, one-way message distribution associated with mass media.[111] Allan conducted a case study of citizen journalism in an effort to analyze the spontaneous actions of ordinary people who felt compelled to bear witness during the London bombings in July 2005. Their efforts are described as follows:

> Members of London's blogging community were mobilising to provide whatever news and information they possessed, in the form of typed statements, photographs or video clips, as well as via survivors' diaries, roll-calls of possible victims, emergency-response instructions, safety advice, travel tips, links to maps pinpointing the reported blast locations, and so forth. Many focused on perceived shortcomings in mainstream

---

[107] Rettberg, *Blogging*, p. 66.

[108] Ibid., p. 92.

[109] Ibid., pp. 92—93.

[110] Ibid., p. 93.

[111] Stuart Allan, "Citizen Journalism and the Rise of 'Mass Self-Communication': Reporting the London Bombings," *Global Media Journal*, Australian ed. 1, no. 1 (2007), p. 2, citing M. Castells, "Communication, Power and Counter-Power in the Network Society," *International Journal of Communication* 1, no. 1 (2007), pp. 238–66.

news reports, offering commentary and critique, while others dwelt on speculation or rumour, some openly conspiratorial in their claims.[112]

Citizens tagged individual photographs into groups using words such as "#explosions," "#bombs," and "#London" to facilitate efforts by readers to find relevant images.[113]

Allan notes that blogs are very different from the Internet or newspaper front pages. Blogs list the most recent things first, which is something a reader desires when following a story, as opposed to mass media, which lists first what is considered by the outlet as the most important thing.[114] Blogs also differ because they are quicker to update and allow people a place to connect on an emotional level with an event. Like Rettberg, Allan points out the risk readers and news organizations face when relying on "amateur" accounts and footage. Steps, therefore, should be taken to ensure the value of the posted information before relying upon it.[115]

3. Collective Efforts Enhance Information Accuracy

Osimo describes collective intelligence as the process by which "contributions are made more meaningful and rich through collaboration and networking between users, so that the total is more than the sum of the individual contributions."[116] Peer review supplies quality control and a filtering system to improve the end product. Hotz reports that a study on Twitter usage during the 2010 earthquake in Chile revealed that in a crisis, crowds reflexively sort facts from falsehoods, thereby exerting collective wisdom "on the fly."[117] The truth wins out over misinformation as the network provides a filter.

---

[112] Ibid., p. 10.

[113] Ibid., pp. 13–14.

[114] Ibid., p. 12.

[115] Ibid., p. 15.

[116] Osimo, "Web 2.0 in Government," p. 18.

[117] Hotz, "Decoding Our Chatter."

"Hundreds of social media, data-mining and financial services companies now are paying a base rate of up to $360,000 a year for Twitter's information," clear demonstration of the perceived value of information produced through this social media mechanism.[118]

Surowiecki argues the phenomenon of group intelligence is demonstrated through a number of studies conducted by American psychologists and sociologists between 1920 and the mid-1950s.[119] The studies suggest several key conditions must exist in order for a group to be smart: diversity of opinion among those weighing in; independence such that individual opinion is not determined by others; decentralization, which enables individuals to specialize and draw on local knowledge; and aggregation to transform private judgment into a collective decision.[120] Surowiecki concludes, "[U]nder the right circumstances, groups are remarkably intelligent, and are often smarter than the smartest people in them. Groups do not need to be dominated by exceptionally intelligent people in order to be smart. Even if most of the people within a group are not especially well-informed or rational, it can still reach a collectively wise decision."[121]

Palen and her research group at the University of Colorado, Boulder, analyzed social-media usage during the shootings at Virginia Tech on April 16, 2007.[122] The study involved reviewing official and unofficial news releases, conducting in-person interviews, and reading content posted on several social-networking sites. The study focused on group problem-solving efforts to identify victims preceding official announcements.[123] Compiled information from several online lists correctly identified all victims, and the lists were widely available before authorities confirmed the final death toll. Collaborative efforts through social media were found to demonstrate "the problem-solving efficiency and accuracy of large-scale, highly distributed online collaboration."

---

118 Ibid.

119 James Surowiecki, *The Wisdom of Crowds*, New York: Anchor Books (2005).

120 Ibid., pp. 32, 65, 69–72.

121 Ibid., pp. viii–ix.

122 Leysia Palen, "Online Social Media in Crisis Events," *Educause Quarterly*, no. 3 (2008).

123 Ibid., p. 77.

The results suggest "future emergency management needs to incorporate mechanisms within organizational processes for supporting and leveraging information generated and disseminated by the public."[124]

Stephenson and Bonabeau similarly posit in a journal article that terrorism and response strategies should capitalize on information generated through the combination of social-media communication technologies and the science of swarm intelligence.[125] Like the term "group intelligence," "swarm intelligence" connotes the ability of a group to create highly sophisticated structures and collaborative projects that exceed the capabilities of individual group members.[126] The authors argue formal homeland security planning needs to include citizen-generated information because "advances in networked communications, combined with human nature, make it almost inevitable that individuals during a disaster will automatically turn to the increasing array of electronics they use every day to reach out to others for comfort and mutual assistance."[127] Agencies such as the Federal Emergency Management Agency (FEMA), therefore, need to embrace collaborative social-media tools and treat the public as full partners in prevention and response activities by creating the conditions that directly foster group intelligence.[128] Failing to do so may result in people taking matters into their own hands and circumventing governmental efforts during disasters and attacks.

4. Potential Obstacles to Social Media Adoption

While the literature provides powerful incentive for incorporation of social media technologies by law enforcement agencies as a means of communication to receive crime and terrorism-related tips and information, a number of articles and government studies suggest challenges may exist to its adoption. The 2011 IACP survey inquired about specific barriers to adopting social media in law enforcement agencies, and the top two

---

[124] Ibid., p. 78.

[125] W. David Stephenson and Eric Bonabeau, "Expecting the Unexpected: The Need for a Networked Terrorism and Disaster Response Strategy," *Homeland Security Affairs* 3, no. 1 (February 2007), p. 1.

[126] Ibid., pp. 1–2.

[127] Ibid., p. 4.

[128] Ibid., p. 7.

barriers were identified as resource driven: time constraints and limited personnel.[129] Additional barriers include security, liability, and privacy concerns. The IACP's Law Enforcement Executives' Social Media Top Ten explains that, while social media tools are free to use, their implementation, monitoring, and maintenance require personnel time.[130]

Alexander notes several additional obstacles. Agencies may be concerned with the speed of social media and the fear that information shared through this mechanism can become widespread before officials are prepared to comment about an ongoing investigation.[131] Another concern may be due to the perceived volume of social-media-driven communication that will be sent to the agency and the fear the agency is not capable of handling it.[132] Additionally, individual officers may worry that they will face increased exposure to verbal attacks from the public should a system be created that allows citizens to send comments directly to an agency.

Stephenson and Bonabeau observe some agencies may find it difficult to deal with the ability of individuals to self-organize through social media as it can result in an inability for government to exercise top-down command and control over a situation.[133] Agencies do not want citizens to take matters into their own hands or to circumvent government efforts during natural disasters and terrorist attacks.

Lindsay identifies several practical considerations associated with implementing a social media program in the context of emergencies and disasters. Limited battery life for computers and mobile telephones means an overreliance on social media technologies during a prolonged power outage would be problematic.[134] The cost to launch, maintain,

---

[129] IACP, "2011 IACP Social Media Survey," p. 5.

[130] IACP, "IACP Law Enforcement Executives' Social Media Top Ten," Bureau of Justice Assistance, U.S. Department of Justice (January 2011).

[131] Dan Alexander, "Using Technology to Take Community Policing to the Next Level," *Police Chief Magazine* (July 2011), p. 2.

[132] Ibid., p. 3.

[133] Stephenson and Bonabeau, "Expecting the Unexpected," p. 7.

[134] Lindsay, "Social Media and Disasters," p. 7.

and staff such a program is unclear. And privacy concerns are implicated through the collection, retention, and data mining of personal information received by any government agency.

The 2009 CHDS Ogma Workshop participants identified three primary trust barriers that militate against the integration of social media tools into the homeland security arena. The most commonly identified concern is with the quality of data sent out to the public, as well as received by homeland security and public-safety agencies.[135] Other concerns include the reluctance of homeland security professionals to adopt and integrate Web 2.0 technologies, as well as a perceived lack of awareness about the tools that are available, how they can be utilized, and how internal policies can be adjusted accordingly.[136]

The greatest obstacle for law enforcement to the adoption of a social media strategy may be the very nature of the police organizational culture. Lawless reviewed management science literature and conducted a case study to determine the manner in which an innovative program could be implemented in a law enforcement agency.[137] Lawless concluded these agencies exhibit great resistance to innovation because, generally,

> the organizational culture in police departments tends to be insular. Officers see themselves as separate from the public, and even unpopular at times. Consequently, they value secrecy and control over information about the way they work. Innovations, like information systems or models, that open operations to scrutiny can therefore appear threatening. Police also value tradition highly. Innovations that disrupt traditional procedures are poorly received.[138]

Lawless notes agency structure is dependent upon rules and procedures. Several factors, therefore, can significantly influence implementation success, such as development of

---

[135] "Ogma Workshop," pp. 8–9.

[136] Ibid., p. 9.

[137] Michael Lawless, "Institutionalization of a Management Science Innovation in Police Departments," *Management Science* 33, no. 2 (February 1987).

[138] Ibid., p. 245.

formal operating procedures, training programs, job descriptions and specifications to set expectations, and budgeting time to incorporate running the new program.[139]

More recently, Williams conducted a literature review to examine the institutionalization of innovative change by law enforcement in the context of community policing. The review included a number of studies analyzing police reform efforts throughout the twentieth century. Williams describes agreement within the literature that "the endurance of community policing will depend upon the extent to which it becomes both philosophically and operationally integrated with routine police operations."[140] The success of implementing a change effort depends upon the extent to which an organization can alter the behavioral patterns of its employees, such as by altering the structural components that support the targeted behavior.[141]

5.   Policy Considerations and Implementation Strategies

In the business context, Byl et al. propose the essential elements of a social media policy be considered to include reminders that:

- The organization's broader ethical guidelines also apply to social media;
- Employees will be held responsible and liable;
- Employees must post disclaimers that they do not speak for the organization;
- Employees must disclose their affiliation with the organization when posting;
- Employees must respect copyright and fair use laws;
- Employees must honor the confidentiality of proprietary or internal information;
- Employees are prohibited from using hate speech, ethnic slurs, etc.;
- Employees should respect privacy and use discretion.[142]

The policy drafting team should comprise legal staff, human resources staff, information technology staff, and some of the employees who will use the tools.[143]

---

[139] Ibid., pp. 247–48.

[140] E. J. Williams, "Structuring in Community Policing: Institutionalizing Innovative Change," *Police Practice and Research* 4, no. 2 (2003), p. 120.

[141] Ibid., p. 121.

[142] Bart Byl, Amanda Nelson, and David Thomas, "Social Media Blueprint: A Step-by-Step Plan to Prepare Your Company," Radian 6, Community ebook (April 2012), p.16.

[143] Ibid., pp. 10, 12.

Johnson engaged in a comparative analysis through several case studies before concluding FEMA should improve its Web 2.0 strategy to better enable collaboration within the agency as well as with its partners, such as members of the community.[144] His research demonstrates several policy initiatives are necessary to foster the success of any new social-media strategy. First, agency leadership needs to create a culture of collaboration.[145] Second, the agency needs to invest time to learn more about the social-media technologies being used by the community it serves so it can determine which items employees should be trained on and use. Third, the agency must devote personnel resources sufficient to encourage engagement with and ensure timely response to information provided by the community. Fourth, employees must be empowered to experiment and innovate through social media. And, lastly, employees must be permitted to access social-media sites during work hours on government-issued equipment.

Ogma Workshop participants identified several initial solutions to overcoming trust-based concerns, including building awareness of social-media technologies and their potential benefits through targeted education for agency employees and implementing pilot projects to establish best practices.[146] Lindsay suggests agencies adopt methods and protocols to assist with the interpretation of incoming information to counter the fact that the very nature of social-media platforms and people's use of them can result in the inadvertent or intentional transmission of false and inaccurate information.[147]

Hrdinova et al. reviewed policy documents and interviewed professionals employed by 26 international, federal, state, and local government agencies. The research revealed eight essential elements for any government social-media policy:

- Outline employee access by delineating which social media sites can be accessed and by whom, and whether the access will be unrestricted or controlled;

---

[144] Samuel Johnson, "Improved Web 2.0 Strategy for FEMA to Enable Collaboration and a Shared Situational Awareness across the Whole of Community," master's thesis, Naval Postgraduate School (March 2012).

[145] Ibid., pp. 55–57.

[146] Ibid., pp. 10–12.

[147] Lindsay, "Social Media and Disasters," pp. 6–7.

- Designate at least one manager who is responsible for establishing, maintaining, and when appropriate, closing agency social media accounts;

- Outline how the agency expects employees to use social media tools and consequences for violating the policy;

- Include expectations for professional employee conduct, such as respecting the rules of the venue, striving for transparency, and being respectful in all online postings;

- Devise a content management strategy to ensure accuracy of posted information;

- Incorporate best practices for ensuring security of data and the agency's technical infrastructure;

- Reference applicable laws and regulations;

- Decide whether to keep interactions one-way (agency to citizen) or permit two-way conversations that solicit and enable citizen comments. If two-way interaction is permitted, develop and post expectations for acceptable citizen conduct.[148]

The research report contains sample language derived from policies in operation in the participating jurisdictions.

The IACP National Law Enforcement Policy Center's model policy for social media begins with language that sets a tone by clearly establishing the potential value this technology can bring to a law enforcement agency: "assisting the department and its personnel in meeting community outreach, problem-solving, investigative, crime prevention, and related objectives."[149] The model policy contains a detailed strategy for professional and personal use of social-media technologies, thereby providing guidance on how these tools can be used to communicate with and push alerts and information out to members of the public. (See Appendix A.)

Stevens delineates a number of steps, in addition to establishing a robust policy, that law enforcement agencies should utilize when implementing a social-media program to further its success:

---

[148] Jana Hrdinova, Natalie Helbig, and Catherine Peters, "Designing Social Media Policy for Government: Eight Essential Elements," Center for Technology in Government, University at Albany, Research Foundation of State University of New York (May 2010), p. 9.

[149] IACP, "Social Media."

- The agency must have a defined strategy that outlines the type of social media technology to be used, how it will be utilized, and the personnel who will be responsible for it;

- The assigned personnel must maintain the content and respond to incoming posts to keep the information flowing;

- An agency's inability to provide updates and content means the agency should not engage in social media;

- Personnel should abandon their fears about receiving too much or negative information because by seeing what people are saying, the agency has the opportunity to engage the community and rebut criticism;

- An agency will lose credibility with the community by creating, then walking away from, a social media presence;

- Because social media tools are designed to enhance communication between human beings, the agency needs to identify personnel who are responsible for its maintenance;

- Twitter needs to be used as a two-way communication tool, and not just to push out messages and alerts;

- Agencies should seek advice from other agencies already engaging the public through social media tools.[150]

All of the literature in this context establishes a government agency needs to clearly set expectations for all social media users, whether employees within or citizens external to the agency.

D.   CONCLUSION

The ubiquity of social media use through the Internet and mobile telephones (i.e., smart phones) in society today is undeniable. Pew Research Center, Universal McCann, and Nielsen survey data demonstrate the prevalence of usage by people throughout the country as a means of communication with one another. CHDS Ogma Workshop participants put it succinctly: public-safety and law enforcement agencies need to understand and embrace a communication mechanism the general public is already using to converse with one another. The data also reveals a preference for using social networking sites to communicate with one another.

---

[150] Lauri Stevens, "Social Media in Policing: Nine Steps for Success," *Police Chief Magazine* 77, no. 2 (February 2010).

The participatory nature of social media readily enables collaboration and the sharing of content, such as information, video, and photographs. The speed of Internet connections and the ability for social media to reach a broad audience combine to attract great interest in these technologies. The trend continues to rise each year and, on its own, presents a compelling reason for law enforcement agencies to include this technology among the tools they use to engage and communicate with the communities they serve.

The literature demonstrates social media use results in a number of benefits to individual users, including the creation of a sense of belonging and a collective identity, as well as fostering the ability to engage civically. It also demonstrates that adoption of social-media technologies by government promotes networking and collaboration among a diverse group of individuals, both within and outside of the agency setting. Public-safety and law enforcement agencies, in particular, can enhance situational awareness and thereby improve decision making and targeted-response efforts. Social-media tools have the capacity to innovate traditional police work by reaching a broad audience through digital wanted posters and online calls for assistance with solving open investigations. The tools can also facilitate prevention efforts via the transmission of crime and terrorism-related tips and information from the public. Designing a process that fosters group intelligence and group problem solving can improve an agency's confidence in the quality of received information.

A number of agencies may elect to start using social media tools primarily in an effort to remain current. The simple logic of that reasoning, however, ignores what the literature demonstrates—a tremendous number of people use social media to converse with one another and participate in one or more groups focused on community issues. Many private companies embrace social media as a mechanism to stay in touch with their target audiences and enhance the customer service experience. Just as with the advent of the telephone, law enforcement agencies must adapt to incorporate this increasingly popular information exchange mechanism.

Studies regarding the institutionalization of innovative change in the context of police organizations indicate the need to develop formalized operating procedures and training programs, among other things, to make a new social media program successful.

Additionally, agencies must dedicate the personnel necessary to monitor received information, vet it to address quality and accuracy concerns, and provide feedback to encourage further public engagement efforts. Passive information acquisition through surreptitious data mining and the dissemination of community alerts may prove beneficial. Law enforcement agencies should also strive to engage in two-way conversations with the public, a more collaborative application of social media, to provide an avenue for the transmission of valuable crime and terrorism-related tips and information.

This thesis continues by analyzing the community's role in the law enforcement enterprise (Chapter II), explaining distinctions between various social media mechanisms (Chapter III), and demonstrating the manner in which available social media mechanisms can be utilized to facilitate citizen involvement in the protection of the homeland through an analytical case study methodology (Chapter IV). Chapter V will present suggestions for implementation, including legally mandated budget considerations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE PUBLIC'S ROLE IN THE EVOLVING HOMELAND SECURITY AND POLICING PARADIGMS

> *Individual citizens and cohesive communities are key partners in the homeland security enterprise and have an essential role to play in countering terrorism. Mechanisms for identifying and reporting suspicious activities must be made clear and accessible.*
>
> Quadrennial Homeland Security Review Report

A. NATIONAL HOMELAND SECURITY STRATEGY

The nation has grappled since World War II with creating a mission for homeland security that is sufficient to protect the country against terrorist threats as well as man-made and natural disasters. The events of 9/11 demonstrated that, as recently as a decade ago, the U.S. government still did not have in place a comprehensive vision of how best to achieve this goal. Since that time, the Department of Homeland Security (DHS) was created, and a philosophy of shared responsibility for our nation's security has evolved. Nonetheless, defining specific strategic objectives has been a work in progress during which the roles to be played by all levels of government, including law enforcement, and civilians have likewise evolved.

The 2002 National Strategy for Homeland Security (the 2002 Strategy) outlines a fairly limited role to be played by members of the public in homeland security efforts.[151] The Citizen Corps, launched that same year by President Bush, was designed to train volunteers to support first responders by providing assistance to victims and at disaster sites. Additionally, the Citizen Corps planned to expand the crime prevention mission of the Neighborhood Watch Program to incorporate terrorism prevention by having citizens report suspicious behavior to law enforcement (e.g., "See Something, Say Something"). Citizen volunteers were also to be utilized through the Medical Reserve Corps, for provision of medical services, and the Police Services, for provision of assistance to resource-constrained local law enforcement agencies.

---

[151] United States Office of Homeland Security, "National Strategy for Homeland Security" (July 2002), p. 12.

The 2007 National Strategy for Homeland Security is similarly limited in terms of the role to be played by members of the public. For example, the 2007 Strategy calls for training for citizens on what to do in the event of an attack or natural disaster, thereby reducing the impact of a threat on the community and easing the burden on emergency managers and first responders.[152] In addition, it calls for citizens to continue playing a role in terrorism prevention by reporting suspicious behavior to law enforcement agencies.

It was not until the Quadrennial Homeland Security Review Report was released in 2010 that the expected role of the public was more expansively and clearly defined. A philosophical change occurred: the DHS recognized that the 2002 definition of homeland security (i.e., a concerted national government-centric effort to prevent terrorist attacks, reduce the country's vulnerability to terrorism, and minimize damage and recovery from attacks that do occur) was too narrow. Homeland security, under the 2010 definition, "is not simply about government action alone, but rather upon the collective strength of this entire country" and is to be achieved through collaboration between government, businesses, individuals, families, and communities.[153] The new definition was influenced by the recognition that homeland security is not solely about government action, but rather about the collective strength of the entire country. In July 2010, the DHS launched a national public awareness campaign to further solidify the "See Something, Say Something" campaign and to encourage citizen reporting of suspicious activity to law enforcement agencies.

The view of empowering Americans to contribute to the country's security and embrace a unity of effort stems from the realization the federal government "cannot be everywhere, nor can it alone ensure resilience or thwart every threat, despite best efforts. Private individuals, communities and other nongovernmental actors must be empowered

---

[152] United States Department of Homeland Security [USDHS], Homeland Security Council, "National Strategy for Homeland Security" (October 2007), pp.4–5.

[153] USDHS, "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland," Washginton, D.C.: United States Department of Homeland Security (February 2010), p. 3.

to take action."[154] A similar realization backed the movement in law enforcement toward the utilization of the public as a partner in community-oriented policing several decades ago.

B.   COMMUNITY POLICING STRATEGY

Figure 5.   Community Policing Word Cloud.[155]

By the 1990s, government and community leaders began to recognize that citizens must accept some responsibility for keeping their neighborhoods safe and secure. The community policing strategy was developed to get citizens involved with crime

---

[154] Ibid.

[155] Google Images for Community Policing, retrieved July 18, 2012, from http://www.google.com/imgres?q=images+for+community+policing&start=76&hl=en&sa=X&biw=1366&bih=599&tbm=isch&prmd=imvns&tbnid=IjVi327_-5zUiM:&imgrefurl=http://oaklandnorth.net/2010/01/21/after-five-years-of-measure-y-oakland-asks-%25E2%2580%259Cis-community-policing-the-answer%25E2%2580%259D/&docid=63k-pbuz4VyOMM&imgurl=http://oaklandnorth.net/wp-content/themes/calpress/library/extensions/timthumb.php%253Fsrc%253Dhttp://oaklandnorth.net/wp-content/uploads/2010/01/wordle_title.png%2526w%253D620&w=620&h=406&ei=ZgwHUIK2NunO2gW7sPjiDw&zoom=1&iact=hc&vpx=572&vpy=19&dur=2861&hovh=182&hovw=278&tx=147&ty=89&sig=112656406066592759659&page=4&tbnh=128&tbnw=171&ndsp=28&ved=1t:429,r:3,s:76,i:15

prevention, intervention, and the proactive development of solutions to address the immediate underlying conditions that contribute to public-safety problems.[156] Community partnerships incorporating these ideals can provide an additional resource to law enforcement agencies beyond the after-the-fact response officers traditionally take to address crime.[157]

Community policing is made up of three primary elements: problem solving to reduce crime and disorder by addressing its immediate underlying conditions; implementing associated organizational changes within law enforcement agencies to ensure the philosophy is both successfully implemented and institutionalized; and forming partnerships between agencies and the communities they serve.[158] The philosophy of community policing is thus neighborhood-based:

> The local community (or at any rate the law-abiding side of it) identifies the problems, interprets them in terms of neighborhood malfunctions or malpractices, works through a strategy to address those problems, and either implements them directly or applies pressure on those competent to act. The police are partly catalysts to this process, partly collaborators, and partly advisors.[159]

Community policing is believed to erode barriers that separate officers and the citizens they serve while imbuing officers with a greater sense of a community's problems and the conditions that create them.[160] The relationship enables the community to participate

---

[156]United States Department of Justice [USDOJ], "Understanding Community Policing, A Framework for Action," Office of Justice Programs, Bureau of Justice Assistance (August 1994), p. 4; USDOJ, Office of Community Oriented Policing Services, "Community Policing Defined," Washington, D.C., p. 12; Y. Xu, M. Fiedler, and K. Flaming, "Discovering the Impact of Community Policing: The Broken Windows Thesis, Collective Efficacy, and Citizens' Judgment," *Journal of Research in Crime and Delinquency* 42 (2005), p. 150.

[157] USDOJ, Understanding Community Policing," p. 4.

[158] USDOJ, COPS Office, "Community Partnerships: A Key Ingredient in an Effective Homeland Security Approach," *Community Policing Dispatch* 1, no. 2 (February 2008).

[159] Nick Tilley, "Community Policing and Problem Solving," in *Community Policing (Can it Work)*, Belmont, CA: Wadsworth (2004), p. 167.

[160] Jack Greene, "Community Policing in America: Changing the Nature, Structure, and Function of the Police," *Criminal Justice* 3 (2000), p. 301.

in shaping and evaluating police objectives.[161] Partnerships may also result in the revelation to officers of otherwise inaccessible information that is pertinent to crime solving, deterrence, and prevention.

Relationship building that actively engages citizens in frank discussions about community life and the role of law enforcement is integral to the community policing strategy.[162] Communication between officers and citizens must allow for the exchange of information in both directions. It must be "horizontal" in nature, not the traditional top-down relationship law enforcement agencies typically enjoy when disseminating information to the public or taking reports from individual crime victims. This includes allowing community members to provide regular feedback about neighborhood conditions, as well as the effectiveness of police intervention activities designed to address them.

C.   INTELLIGENCE-LED POLICING STRATEGY

Following the events of 9/11, the U.S. Department of Justice issued several documents calling for the incorporation of more robust intelligence generating activities by law enforcement agencies. Borrowing from a concept employed in the United Kingdom, agencies throughout the United States were encouraged to migrate to a philosophy of intelligence-led policing (ILP) to address all crimes and all threats. There are many definitions of ILP, but at its core the philosophy envisions a collaborative law enforcement approach that combines community and problem solving policing with enhanced intelligence operations.[163] ILP is not just a process that adds another layer to policing. ILP requires "strategic integration of intelligence into the overall mission of the organization."[164] Agencies that collect, examine, and vet large quantities of information to develop intelligence are considered better able to engage in proactive decision making

---

[161] Ibid., p. 312.

[162] Ibid., p. 313.

[163] USDOJ, Global Justice Information Sharing Initiative, "Navigating Your Agency's Path to Intelligence-Led Policing" (April 2009), p. 4.; D. Carter, "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies," U.S. Department of Justice, Office of Community Oriented Policing Services (January 2009), p. 80.

[164] Carter, "Law Enforcement Intelligence," pp. 79, 87.

for resource allocation, crime prevention and reduction efforts, and identification and prevention of terrorist threats, as represented in Figure 6 below. ILP can enable operational planning to "either prevent a threat from maturing or mitigate the threat should it occur."[165]
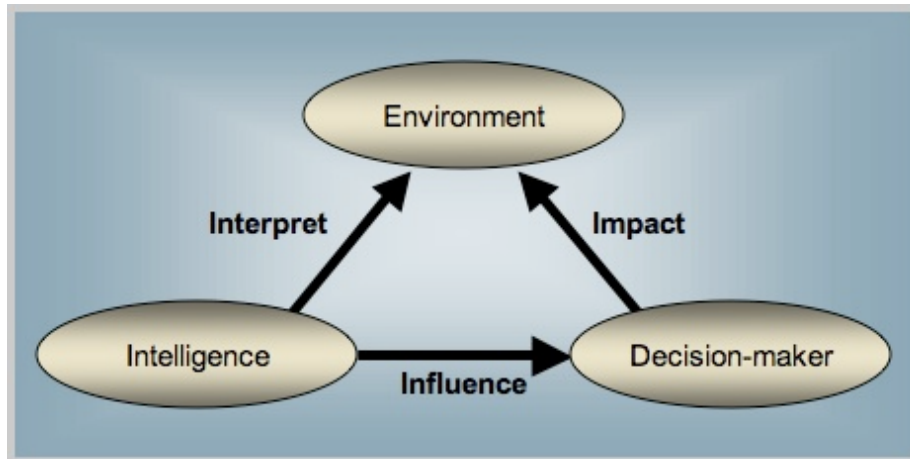

Figure 6.   ILP and Crime Reduction Process[166]

Like community policing, ILP requires law enforcement agencies to engage in coordination, cooperation, and collaboration with non-law enforcement agency partners, such as citizens. Additionally, like community policing, ILP focuses on threats and prevention efforts, as opposed to traditional after-the-fact investigations and crime solving. Law enforcement agencies must therefore build stronger police-community partnerships so threat information can be developed through Suspicious Activity Reports filed by officers, tips from community members, and other indicators suggestive of the presence or emergence of serious multijurisdictional problems.[167]

---

[165] Ibid., p. 82.

[166] Jerry Ratcliffe, "Intelligence-led Policing," *Trends and Issues in Crime and Criminal Justice*, no. 248, Australian Institute of Criminology, Canberra (2003).

[167] Ibid., p. 89; Marilyns Peterson, "Intelligence-Led Policing: The New Intelligence Architecture," U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, NCJ 210681 (September 2005), p. 15.

D.   SUSPICIOUS ACTIVITY REPORTING STRATEGY

The 2007 National Strategy for Information Sharing holds as a guiding principle that those responsible for combating terrorism must have access to timely and accurate information concerning individuals who want to attack the United States, their plans and activities, and their intended targets.[168] Information is needed for all levels of law enforcement to rapidly identify immediate and long-term threats, identify persons involved in terrorism-related activity, and implement intelligence-led counter-terrorism response efforts.[169] The long-term goal of the NSI is for law enforcement agencies across the country to participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information that is potentially terrorism-related.[170]

The acquisition process begins when a citizen, private-sector partner, government official, or law enforcement officer observes suspicious activity, defined as "observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention."[171] The observation is reported to either a local law enforcement or federal agency officer. An investigator documents the suspicious activity in a written document (i.e., a SAR) after completing an initial investigation. The information is vetted within the investigating agency in light of other known suspicious and criminal activity information, although the level of review will depend upon the size of the agency and its available resources. The vetting process also serves to ensure the SAR information was gathered legally.

---

[168] The White House. "National Strategy for Information Sharing, Successes and Challenges In Improving Terrorism-Related Information Sharing" (October 2007), p. 2.

[169] Criminal Intelligence Coordinating Council. "Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project," Global Information Sharing Toolkit, http://www.it.ojp.gov/ (October 2008), p. 8.

[170] Program Manager, "Concept of Operations," p. 3.

[171] USDHS, Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR), Version 1.5, ISE-FS-200 (November 17, 2010), p. 9; Program Manager, "Concept of Operations," pp. 7–13.

SARs having a potential terrorism nexus are forwarded to the area fusion center or Joint Terrorism Task Force (JTTF) for possible further dissemination. Operational feedback should be provided to source agencies to relay the validity and utility of transmitted SAR reports. Additionally, SARs containing personal information later determined to have no criminal or terrorism nexus should be removed from the Intelligence Sharing Environment to protect the privacy interests of involved individuals. This flow of activity is depicted below in Figure 7.

As with community policing and ILP, collaboration with the community is a critical component to the success of the SAR strategy.[172] Agencies should offer education programs to instruct citizens on how to make observations, how to discern activity that is suspicious in nature, how to report observations, what to report, and what will occur next (i.e., what feedback to expect).[173] In particular, training should emphasize that "SAR reporting is based on observable/articulable behaviors and <u>not</u> individual characteristics such as race, culture, religion, or political associations" and include guidance for protecting the right to privacy and other civil liberties.[174] (Emphasis in original.) A well-developed process for documenting SARs and integrating the resultant intelligence into police strategies can improve law enforcement efforts in the all-crimes context as well as the counterterrorism one.[175]

---

[172] Criminal Intelligence Coordinating Council, "Findings and Recommendations," p. 3.

[173] Carter, "Law Enforcement Intelligence," p. 93; Criminal Intelligence Coordinating Council, "Findings and Recommendations," p. 20.

[174] Criminal Intelligence Coordinating Council, "Findings and Recommendations," p. 21. See also USDOJ, Global Justice Information Sharing Initiative, "Final Report: Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR), Evaluation Environment" (January 2010), pp. 49–50.

[175] Jerome Bjelopera, "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress," Congressional Research Services, N. R40901 (June 10, 2011), p. 14.
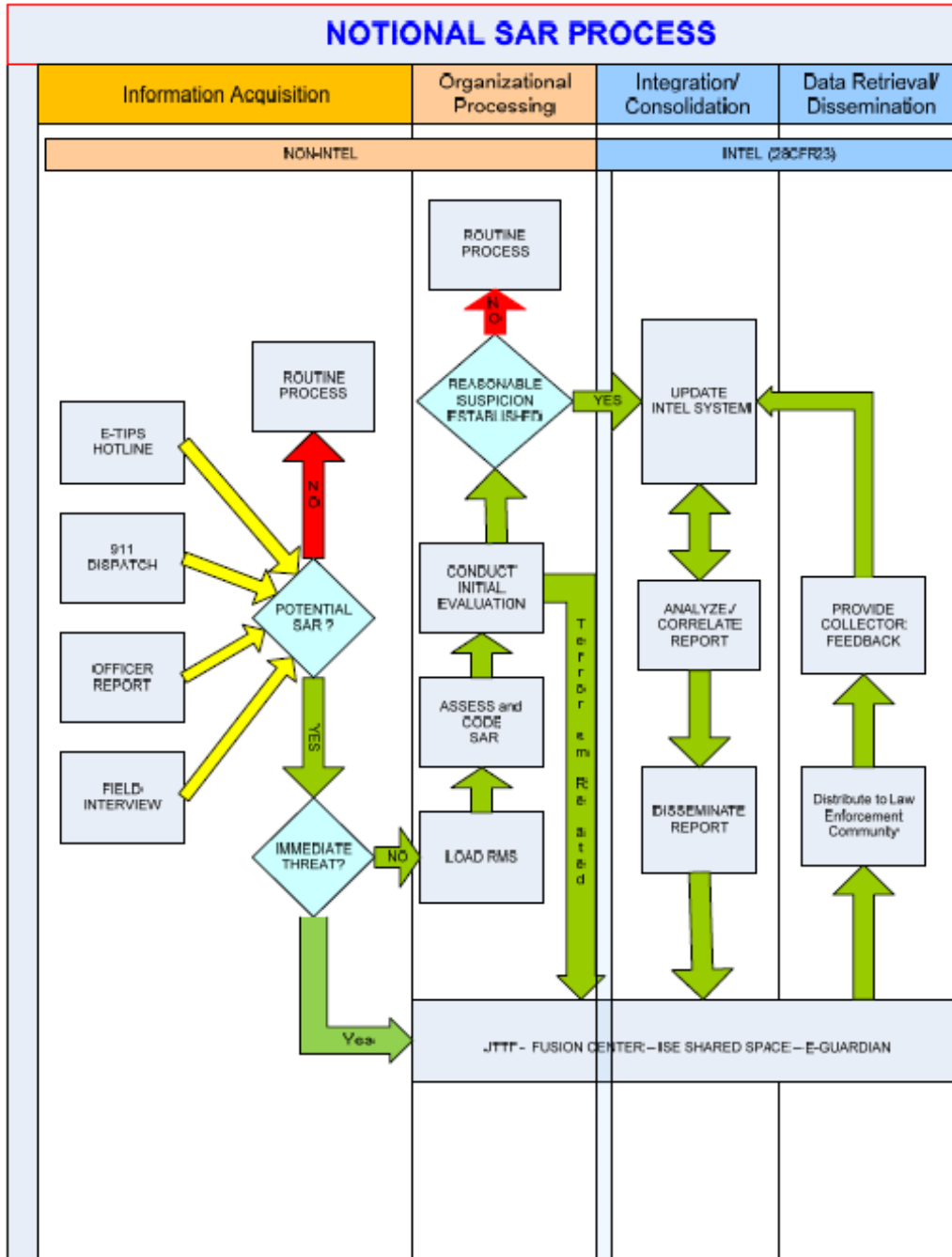
NOTIONAL SAR PROCESS

Figure 7.   Notional SARS Process.[176]

---

176 Criminal Intelligence Coordinating Council, "Findings and Recommendations," p. 31.

E.   BUILDING TRUST IN THE COMMUNITY-LAW ENFORCEMENT RELATIONSHIP

The National Homeland Security strategy documents and policing paradigms described in this chapter presuppose the existence of a working relationship between law enforcement officers and the citizens they serve. Developing successful relationships, however, can present challenges. The element of common sense may be lacking in the context of government–public relations due to fundamental misunderstandings and feelings of distrust between the two entities. Feelings of distrust may derive from an agency's poor transparency track record or problems with its past privacy, civil rights, and civil liberties protection efforts.[177] For example, accusations of racial profiling and the existence of police strategies that focus on one segment of a community to the exclusion of others can inhibit the public's trust of law enforcement officers.

The U.S. Department of Justice recently created an initiative entitled *Building Communities of Trust* to establish the foundation for improved community-law enforcement communication.[178] The goal of the initiative is

> to bring about a better understanding by communities of how law enforcement is using information to protect neighborhoods and citizens, while at the same time educating law enforcement on the priorities and needs of residents and how various community members view law enforcement efforts.[179]

The initiative advocates for full disclosure of the SAR process, its purpose, and the policies and operating methods for its implementation.[180] In addition to such transparency efforts, agencies are encouraged to provide a feedback component that allows community members to express relevant concerns about the SAR process and requires officers to listen.[181] Law enforcement personnel need to be encouraged to use community relationships as a tool for better understanding crime, disorder, and terrorism

---

[177] See generally Robert Bach and David Kaufman, "A Social Infrastructure for Hometown Security, Evolving the Homeland Security Paradigm," *CNA Analysis & Solutions* (January 23, 2009).

[178] Robert Wasserman, "Guidance for Building Communities of Trust," U.S. Department of Justice, Office of Community Oriented Policing Services (July 2010).

[179] Ibid., p. 8.

[180] Ibid., p. 14.

[181] Ibid., pp. 14, 27–28.

from the neighborhood resident's perspective.[182] Officers also need to understand the derivative benefits from developing and nurturing relationships with diverse segments of the community and through regularly reaching out to community leaders.

F.   CONCLUSION

The National Homeland Security strategy documents and the community policing and ILP paradigms necessitate interaction between law enforcement officers and community residents. Interaction in the form of partnerships can better position officers to detect, prevent, and address crime and terrorism-related issues specific to the neighborhoods they are assigned to protect. Successful interaction requires several critical components to foster the exchange of information and ideas between both sides of the partnership. In the context of SARs, citizens need to contribute observations of suspicious behavior, and law enforcement agencies need to provide encouragement through feedback to let citizens know the utility of reported information. Agencies need to work with their community partners through regular outreach to provide direction and training to cultivate suspicious activity reporting. They also need to enable citizens to shape and evaluate police objectives, performance, and procedure through feedback channels.

Law enforcement agencies are tasked through the NSI with developing and instituting a SAR process for gathering timely and accurate information. The Universal McCann, Nielsen, and Pew Research Center survey reports described above demonstrate that people today are more likely to converse with one another through a social media mechanism than through face-to-face contact. Additionally, two-thirds of the general public communicate with one another through social media. In its present form, the NSI SAR process does not incorporate social media tools as a mechanism to obtain information from citizens. The very nature and design of community-law enforcement partnerships argue for their inclusion. The first people to know about a terrorist attack or criminal act committed within a community will be those who reside there. Engaging citizens in homeland security efforts via social media and networking sites is a logical

---

182 Ibid., p. 29.

progression in the relationship between law enforcement and the citizens they serve. It is imperative to capitalize on the public's knowledge and use it to strengthen the homeland security mission.[183]

---

[183] See Fresenko, "Social Media Integration," p. 13, citing Woodcock, "Leveraging Social Media," pp. 2–3.

III. LEVERAGING SOCIAL MEDIA FUNCTIONALITY TO ENHANCE THE FLOW OF INFORMATION FROM CITIZENS

> *A lot of us have jobs where we need to give people structure but that is different from controlling.*

> Keith Miller, author

The literature demonstrates the pervasive usage of social media in society today. Corporate America co-opts customer participation to drive innovation and improve delivery of service. The majority of people use social media to communicate daily with one another—and more often than through in-person contact. According to the 2011 IACP survey, the vast majority of law enforcement agencies already utilize some form of social media to engage with the public for some purpose. Less than half, however, utilize social-media tools to solicit tips, clearly demonstrating a missed opportunity in the realm of gathering SARs to protect communities. This chapter will provide examples to illustrate the distinction between types of social media to demonstrate the manner particular media mechanisms may facilitate communication between law enforcement agencies and the public.

A. EXCHANGING INFORMATION THROUGH STRUCTURED AND UNSTRUCTURED SOCIAL-MEDIA TOOLS

At its most basic, social media is an instrument of communication.[184] Traditional media allows for the unidirectional transfer of information. Social media enables a two-way transfer: a user can both view content created by another and contribute thoughts and comments about it. Social-media mechanisms vary in terms of the level of integration between users. Some, like text messaging, only allow communication between two individuals—sender and recipient. Others, like social networking sites, enable communication between groups of people who follow the same site. The type of social-media mechanism an agency employs to develop SARs, therefore, may influence the level of citizen acceptance and usage of the tool.

---

[184] Daniel Nations, "What is Social Media?" About.com, http://webtrends.about.com/od/web20/a/social-media.htm.

1.   Structured Tip Mechanisms

Structured mechanisms that permit the transmission of crime- and terrorism-related information include online etips forms. Etips forms require the entry of specific types of information into set data fields found on one or more screens on the Internet. This type of reporting mechanism is designed to enhance the accuracy of the information being relayed. Law enforcement guides the flow of information by predetermining the types of data that can be submitted on the form. While having the potential to elicit relevant and detailed information regarding incidents and offenders, the very design of the exchange process may deter some people from using it.

Several law enforcement agencies, like the New York Police Department (NYPD), allow citizen reporting through an online etips form found on its department Web site. The NYPD form consists of multiple sections, each containing a series of pre-set data fields.[185] None of the data fields is required, meaning failure to fill out one or more fields will not prevent submission of the form. The design, however, is cumbersome. The form contains space for information about a suspect (30 data fields), vehicle (seven data fields), and notes describing the offense (eight data fields). The form also provides the ability to attach photographs. The form enables, but does not require, contact information from the citizen submitting the report (four data fields). A copy of the NYPD online tip form is attached as Appendix B.

This type of information exchange design does not allow citizens to relay the information in a natural, conversational style. It does not enable a citizen to control the information exchange process, in contrast to text messaging, where the sender is in complete control of the format of the message content. It does not incorporate the look and feel of popular social networking services such as Facebook and Twitter, described further below, which are presently used by the vast majority of Americans. In addition, a form that solicits particulars through dozens of data fields may connote a detailed interview by a law enforcement officer, the very type of interaction some citizens seek to

---

[185] New York Police Department Crime Stoppers, https://a056-crimestoppers.nyc.gov/crimestoppers/public/tipForm.cfm?pgLang=english&mwID=0; see also Chicago Police Department Community Policing e-Tip, https://portal.chicagopolice.org/xdb/cpdportal/f?p=712:110:2695960673384871.

avoid. Further, an etips form may be perceived by some as too arduous or time-consuming to complete. All of these characteristics call for law enforcement agencies that provide this type of citizen tip mechanism to consider also including other more user-friendly alternatives to reach a broader audience, such as through unstructured social media tools.

2. Unstructured Tip Mechanisms

An unstructured social-media mechanism for citizens to transmit crime- and terrorism-related information permits citizens to exert more control over the content and format of messages they transmit to law enforcement. Several agencies, such as the NYPD and Chicago Police Department, enable citizens to text tips and information via mobile phone.[186] Another alternative is to provide on the department Web site a truncated etips form that contains very few data fields.[187]

Other agencies have developed free apps (i.e., applications) for mobile smart phones (i.e., telephones that enable greater connectivity through the Internet). One example is available through NIC, Inc., a national provider of government Web sites and online services. NIC offers a free Suspicious Activity Reporting app through iTunes that enables citizens to document information about people and vehicles and mark the location of the citizen's observations.[188] This particular app is compatible with iPhone, iPod touch, and iPad products and allows simultaneous reporting to multiple West Virginia and federal law enforcement agencies with a single click. In contrast to an online etips form, the NIC Suspicious Activity Reporting app provides more flexibility and ease of use.

---

[186] New York Police Department TIP577, http://a056-crimestoppers.nyc.gov/crimestoppers/public/index.cfm; Chicago Police Department TXT2TIP, https://portal.chicagopolice.org/portal/page/portal/ClearPath/Communities/Crime%20Prevention/TXT2TIP.

[187] See, e.g., Burlington City, New Jersey, Police Department eTips, http://burlingtonpolicenj.com/eservices/etips; Laguna Vista, Texas, Police Department ETips Submission, retrieved on June 30, 2012, from http://www.lvtexas.com/etips.html.

[188] NIC Suspicious Activity Reporting App, http://itunes.apple.com/us/app/suspicious-activity-reporting/id501164126?mt=8.
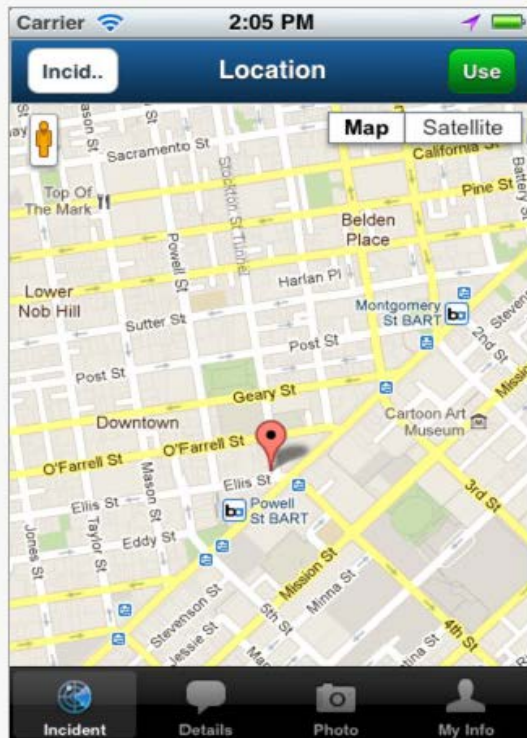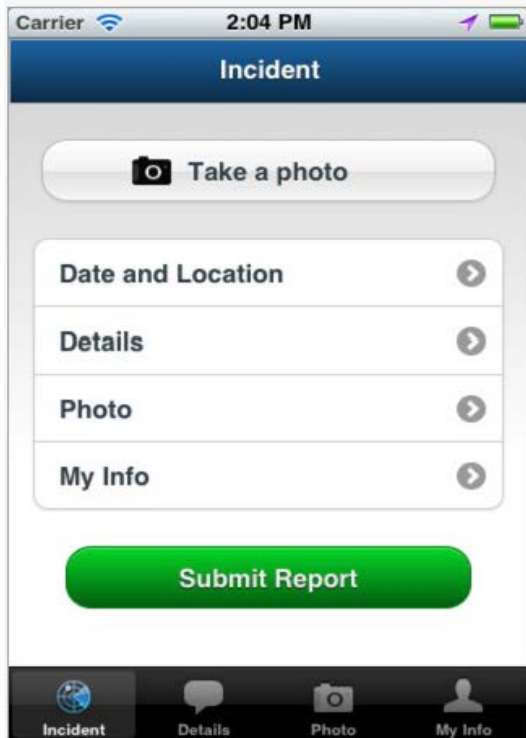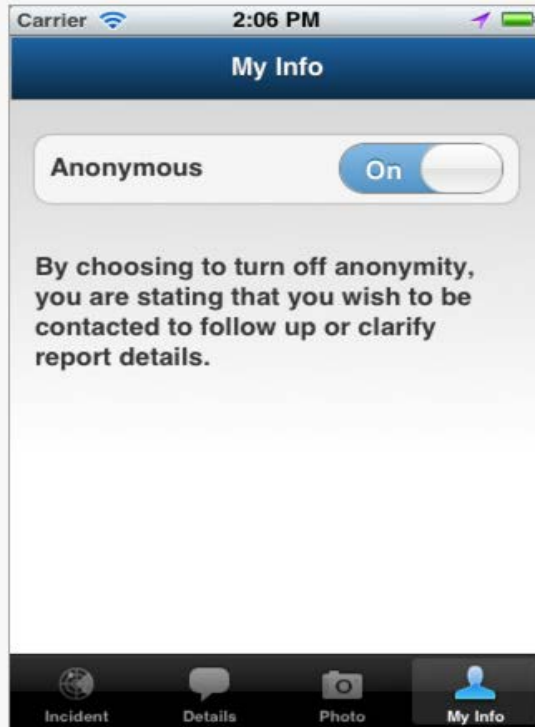
Figure 8.   NIC Suspicious Activity Reporting App.

As depicted above, the app consists of four screens and requires very little typing by the person submitting the report. There is no need to wade through dozens of pre-formatted data fields. Additionally, the app replicates the look and feel of other social media tools, such as the social-networking services Facebook and Twitter, by enabling the posting of text as well as photographs. In contrast to social-networking sites, however, the app allows the information to be shared only with designated recipient law enforcement agencies. No other citizen can view the transmitted information, build on it, or amend it. Thus, there is no opportunity for group intelligence efforts to improve the accuracy and completeness of the information end product.

B. EXCHANGING INFORMATION THROUGH SOCIAL NETWORKING SITES

As recounted above, the Pew Research Center determined that 92% of people use Facebook to communicate with others, and the two most frequently used social-networking sites are Facebook and Twitter. The global total of Facebook subscribers was more than 835,000 in March 2012, up 170,000 from the same time frame one year earlier.[189] At the same time, Twitter had 140 million active users viewing 340 million tweets of information daily.[190] This number of daily Twitter views is more than double the number from one year ago.

Facebook enables account holders to post text, photographs, video, and URL links, which can be viewed by other Facebook users and the public, depending on privacy settings selected by the account holder. Communication begins with one person's post and continues through comments and additional information provided by others, which are appended in sequential order. The entire chain of posts appears on the Facebook pages of the people who contribute and is visible to others with whom those people are connected through friendship links on the site. Facebook's popularity derives from the

---

[189] Internet World Stats, "Usage and Population Statistics, Facebook Users in the World, Facebook Growth Stats for 2011–2012," http://www.internetworldstats.com/facebook.htm.

[190] Leena Rao, "Active Users Sending 340M Tweets Per Day," TechCrunch.com, http://techcrunch.com/2012/03/21/six-year-old-twitter-now-has-140m-active-users-sending-340m-tweets-per-day/ (March 21, 2012).

opportunity it presents for people to easily remain connected with others, the options it affords for uploading and sharing media content, and the ability it fosters to instantly respond when others share comments and/or media.

Twitter operates in a similar fashion yet restricts comments to 140 characters in length. Twitter also allows the transmission of photographs taken by the poster as well as the forwarding of a page from the Internet (e.g., a news article, Web site, photograph, or video) when the item contains a link to the Twitter service. Perhaps the popularity of social media is due to the easy flow of information it allows between users, much like an in-person conversation. Social media users are also able to remain linked around the clock since the advent of high-speed wireless Internet connections.

The literature demonstrates collective intelligence develops through collaboration and networking. Truth wins out over misinformation because the collaboration process allows for peer review and the ability to correct errors. Social-networking sites provide a ready forum for individuals to asynchronously aggregate information. The sites link people with varying degrees of relationship to one another due to family, personal, and professional connections or merely a common interest found through the Internet. Social-networking sites thus foster the key conditions for group intelligence: diversity of opinion, independence, decentralization, and aggregation.

The sample Facebook exchange depicted below illustrates the potential social-networking sites hold for producing valuable SARs through the collective intelligence of citizens. The initial post encourages comments about streams. In response, information about how streams can be used (to skip stones) and the proximity some people have to them (they can be found both in residential and academic neighborhoods) was quickly provided. The sample also demonstrates the broad audience Facebook can reach in response to a request for information or assistance. Here, 15 people weighed in and 59 people indicated they liked the conversation within a few days of its creation. In addition, any Facebook user could easily and instantly find all publicly available comments on this thread had the initial post requested comments include a hashtag such as "#mystream."

Figure 9.   Sample Facebook Communication Exchange.[191]

C.   CONCLUSION

The type of information solicitation tool employed by a law enforcement agency may influence the extent to which it is utilized by the public. Structured mechanisms, such as online etips forms, may not be fully utilized due to a perception they are not considered to be user-friendly. Consequently, such tools may provide few usable SARs. Conversely, unstructured mechanisms, such as texting and social-networking sites, may prove more conducive to community acceptance and utilization. Social-networking sites

[191] Sierra Club, http://connect.sierraclub.org/app/render/go.aspx?g=1ed575e9-25e4-4776-9929-80fffe1cf3ca&xsl=tp_SocialObjects_ObjectType_SIERRA_CLUB_ONLINE_COMMUNITIES_PROJECT_PUBLIC.xslt&id=1ED575E9-25E4-4776-9929-80FFFE1CF3CA&cons_id=&ts=1340664426&signature=82bdd8fdbd5a3a012a0405e116290e46.

may even hold the greatest potential for actionable SARs. The mechanism reaches a broad and diverse audience. It fosters conditions that enable a group to work collectively to improve the reliability of the end product produced through the online discussion. The self-correcting nature of the group information exchange process holds promise for providing accurate and usable SARs.

Law enforcement should capitalize on society's enthusiasm for social media by fully and formally integrating one or more social-media tools into agency operations. Social media can be used to forge community partnerships and holds the potential to develop crime- and terrorism-related tips that can be used to protect communities.

IV.   METHODOLOGY

Research is formalized curiosity. It is poking and prying with a purpose.

Zora Neale Hurston, author

This chapter will proceed utilizing a case study analysis to investigate a contemporary phenomenon, namely government usage of social media, within its real life context.[192] The research outlined below will describe and analyze three different social media implementations in an effort to produce conditional generalizations to address the research questions raised in Chapter I:

- How can social media be utilized to engage members of the community and provide a conduit for citizens to disclose information that may develop into an intelligence product that can assist local law enforcement with the detection and prevention of terrorist acts?

- How does utilizing a structured mechanism for social-media communication, vis-à-vis a one-way push of information, compare to utilizing an unstructured social-media mechanism that enables a two-sided conversation between citizens and law enforcement?

- What conditions must exist within a law enforcement agency for social media to provide a conduit for crime-related and terrorism-related information to flow from citizens?

The methodology will examine not just how social media can present an efficacious mechanism for information exchange in each of the three case studies but also the conditions that need to exist to maximize its effectiveness. Accordingly, each case study will be analyzed in the context of the intended audience of users, the type of information solicited, efforts to market and court participation, education efforts about using the medium, encouragement to participants, efforts to filter erroneous information, and built-

---

[192] Jennifer Rowley, "Using Case Studies in Research," *Management Research News* 25, no. 1 (2002), p. 18, citing R. K. Yin, *Case Study Research: Design and Methods*, 2nd ed., Thousand Oaks, CA: Sage (1994), p. 13.

in metrics to measure success of the venture.[193] The case studies were selected using a diverse strategy intended to achieve maximum variance along relative dimensions of social-media usage by government, as revealed through the literature review.[194]

A.   PEER TO PATENT

1.   Description

Seven years ago Professor Beth Noveck at New York Law School proposed engaging citizens to assist the U.S. Patent and Trademark Office (USPTO) address a problem with the issuance of low-quality patents. Poor patents not only impact the related industry by creating a two-decade monopoly, they also can result in costly litigation for other patent holders.[195] Severe information access restrictions meant USPTO examiners were unable to consult the public, talk to experts, or even use the Internet before granting a patent.[196] Instead, examiners were faced with relying upon information supplied by the applicant and whatever antecedents directly related to the patent—referred to as "prior art"—the examiner could locate to assess the merits of the proposed invention.

Peer to Patent (P2P) was created as a mechanism to improve the scientific portion of the patent review analysis. The P2P process:

> separates scientific from legal decision-making. By means of an online network, the scientific community provides what it knows best—scientific information relevant to determining the novelty and non-obviousness of a patent application. With her deep knowledge of the pertinent statutory standards, the patent examiner then uses that input to make a legal determination of patentability. In this model, the patent examiner remains the ultimate arbiter.

---

[193] A matrix containing a side-by-side comparison of the three case studies utilizing the above-described variables is attached as Appendix D.

[194] Jason Seawright and John Gerring, "Case Selection Techniques in Case Study Research," *Political Research Quarterly* 61, no. 2 (June 2008), p. 300.

[195] Beth Noveck, "Peer to Patent: Collective Intelligence, Open Review, and Patent Reform," *Harvard Journal of Law & Technology* 20, no. 1 (Fall 2006), p. 127.

[196] Ibid., p. 124.

P2P incorporates the extraordinary knowledge and enthusiasm available through online collaboration.[197] Allowing ordinary people to contribute through an open model of scientific review leverages the wisdom of the crowds and ultimately enables a better informed legal decision on the merits of an application.

P2P began as a one-year pilot from June 2007 to April 2008 and was run by students and faculty from New York Law School, not the USPTO. Once an applicant consented to participation, the USPTO Web site enabled self-selected experts to form a review team. The team

- discussed the application;
- submitted prior art;
- critiqued the submissions;
- voted on the relevance of the submissions to the patent application.[198]

Only the ten prior-art references deemed most relevant were forwarded for consideration, along with explanatory annotations. Each team was provided a shared discussion space for assignment of research tasks, posting results and deliberation. The USPTO Web site was optimized to enable the collaborative tagging of applications with additional labels. Patents are officially classified by the USPTO, but this kind of supplemental community self-tagging using terminology common in the field via "folksonomy" is believed to make it easier for all experts to find applications of interest.[199] A depiction of the overall P2P review process appears below in Figure 10.

The USPTO and New York Law School engaged in several efforts to encourage participation in P2P. The decision was made early on to allow consenting applicants to jump to the head of the patent review line, approximately one million in number. This created heavy incentive for applicants to participate. The lack of a budget for outreach or marketing to reach potential peer reviewers resulted in the strategy of enlisting the help of charismatic community leaders to advertise the project through their blogs, online

---

[197] Ibid., p. 144.

[198] Naomi Allen et al., "Peer to Patent First Anniversary Report," Center for Patent Innovations, New York Law School (June 2008), p. 5.

[199] Noveck, "Peer to Patent," p. 146.

newsletters, and organizations' meetings.[200] The P2P Web site, accessible through the USPTO Web site, included a written explanation about the project and how people could contribute to the effort.[201] Future iterations of the project included online videos containing tutorial instructions and other perspectives about the project.
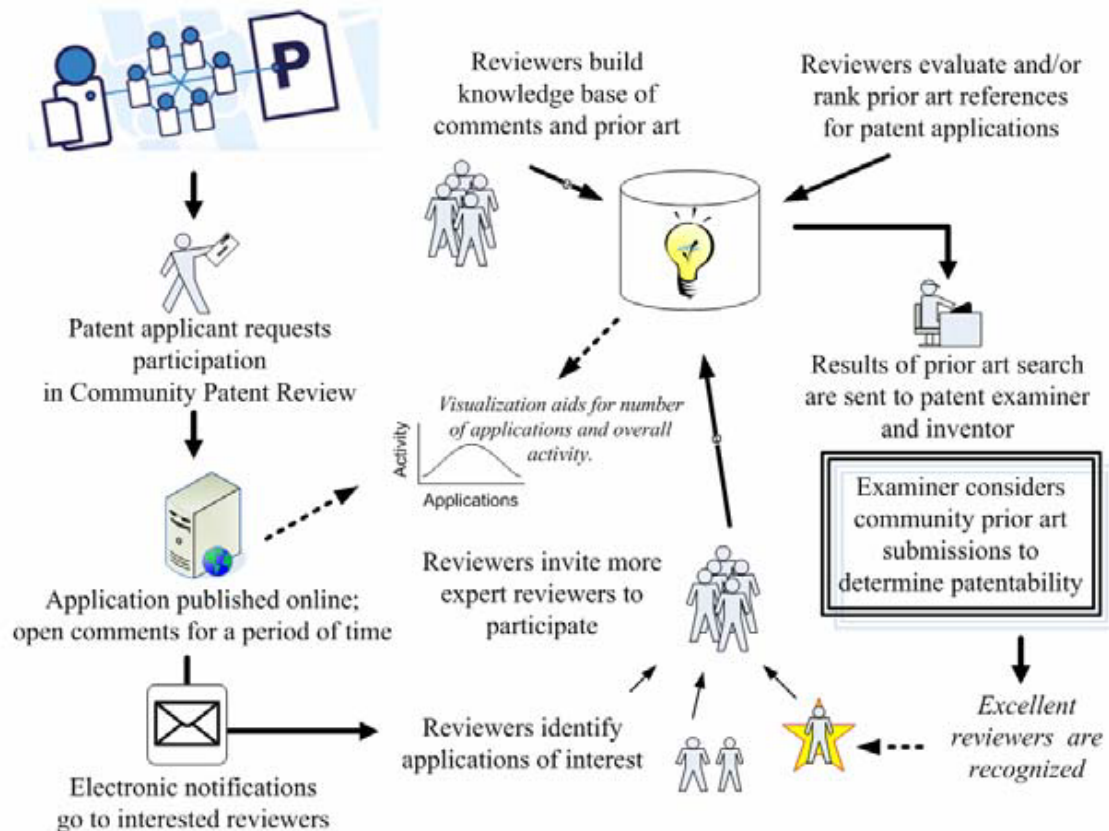

Figure 10.   Peer to Patent Application Review Process.[202]

The success of the project was thought to stem "from having well-thought out practices that allow participants to clearly see the community of which they are a part, to understand their role within the group, to participate simply and easily in the process, and

---

[200] Allen et al., "First Anniversary Report," p. 16.

[201] Peer to Patent, "Getting Started," http://peertopatent.org/getting_started.

[202] Allen et al., "First Anniversary Report," p. 4.

to see the outcome."[203] The P2P software was designed to issue "reputation points" to reward worthy contributions (depicted in Figure 10 as a gold star) like those issued on eBay to signal who is a trustworthy seller or purchaser.[204] The Web site even encouraged healthy competition between review teams through a "most active teams" feature on the Web site's home page, depicted with an arrow in Figure 11.

Figure 11.   P2P Web Site Home Page.

Several qualitative and quantitative methodologies were utilized to measure the impact of public expert contributions on government examiner decision making, the level of expertise of the peer reviewers, the impact of the online group-based process in shaping the peer reviewers' expertise, and ultimately the resultant quality of issued patents.[205] Data culled from the software and surveys reveals the P2P Web site attracted over 40,000 visitors from 140 different countries, 2,000 registered users, and 173

---

[203] Noveck, "Peer to Patent," p. 160.

[204] Ibid., pp. 149–50.

[205] Allen et al., "First Anniversary Report, p. 11.

submissions of prior art on 40 applications during its first year of operation.[206] By the end of the second year, P2P Web site visits rose to more than 74,000 people from 161 countries.[207] The number of registered users at that point exceeded 2,600, and the number of participating applicants increased by 329%. The most current year of operation ran from October 2010 through September 2011. Analysis of that data is not yet available.

P2P ran as a pilot during each year it was offered, though the type of eligible patent applications increased with each iteration. Each year, nearly 70% of patent examiners responded in the survey they believed P2P, if formally adopted by the USPTO, would be helpful in doing their job.[208]

2.   Analysis

The P2P project involved a public-private partnership between a federal agency and a nongovernmental academic team. The project leveraged social media to create a collaborative online work space for self-selected citizen experts to contribute to the core mission of the USPTO. The development team devoted a great deal of advance work toward defining the specific problem the project sought to address as well as several hypotheses about the project's impact to assess its outcomes. As a result, the P2P software and a survey tool were specifically designed to enable the capture and assessment of the types of data necessary to conduct the assessment analysis.

Budgetary constraints led to creative no-cost efforts to target market the P2P project. Community leaders were leveraged to perform outreach to the type of individuals the project sought to entice as participants. Once individuals learned about P2P, the Web site provided the instruction necessary to enable meaningful participation. Instruction included a written explanation, visual depiction of the participants' role in the patent review work flow, and during future iterations, video tutorials.

---

[206] Ibid., p. 6.

[207] Naomi Allen et al., "Peer to Patent Second Anniversary Report," Center for Patent Innovations, New York Law School (June 2009), p. 5.

[208] Ibid.; Allen et al., "First Anniversary Report," p. 6.

The very nature of the P2P work environment enabled the two-sided exchange of information. The Web site and project design ensured the existence of the key conditions necessary for group intelligence—diversity of opinion, independence, decentralization, and aggregation—to transform private judgment into collective decision. Peer reviewers were provided a discrete task to perform: obtain, vet, vote on, annotate, and transmit to a patent examiner the most relevant prior art pertaining to an assigned pending application. Participants were also afforded the opportunity to provide additional labels to patents in the USPTO library through collaborative tagging to promote ease in searching, much like social-networking site users are allowed to denote commentary with hashtags. Participants were provided feedback via a reward system for making valuable contributions. Contributions were also recognized in the annual review documents generated by the academic team. The annual reviews clearly demonstrate the benefit derived from the P2P project.

B. DID YOU FEEL IT?

1. Description

The U.S. Geological Survey (USGS) has been tracking macroseismic intensity (i.e., the strength of shaking from an earthquake at a particular location) since 1931.[209] Information is tracked both through instrumentation to measure ground movement, such as strong-motion seismographs, and personal observations from the people who actually experience earthquakes.[210] Early observational data was collected through questionnaires mailed to post offices in impacted regions. The process to send and receive surveys, manually analyze the returned information, and use it to create a synthesized intensity map took several months. Since the late 1990s, the USGS has been using a Web page

---

[209] David Wald and James Dewey, "Did You Feel It? Citizens Contribute to Earthquake Science," U.S. Department of the Interior, U.S. Geological Survey, Fact Sheet 2005-3016 (March 2005), p. 1.

[210] United States Geological Society [USGS], http://earthquake.usgs.gov/research/dyfi/.

known as "Did You Feel It?" (DYFI) to perform these tasks. The result is the ability to more quickly obtain larger quantities of more comprehensive data than ever before, at minimal cost.[211]

The DYFI Web page contains a brief Internet questionnaire that can be accessed by any individual who selects from a list of recent earthquakes in a region or chooses the "new or unknown earthquake" option. The questionnaire solicits uniform information about what a person experienced through descriptions of the earthquake's effects, such as damage caused and strength of shaking. A depiction of the questionnaire is contained in Figure 12. Response options are preformatted; the contributor can select from simple dropdown values and check-the-box options to relay information. Data is then aggregated to create Community Internet Intensity Maps (CIIMs), which become publicly available on the USGS Web site almost instantly.

The USGS creates a CIIM automatically after each widely felt earthquake in the United States. CIIMs use an algorithm to depict the intensity values assigned by each community, defined as discrete zip code regions in the impacted area.[212] CIIMs can also be created through geocoding the addresses voluntarily provided on questionnaires. Each CIIM is updated every few minutes following a significant event and less frequently as the volume of received data diminishes.[213] The CIIM is overlaid on intensity data gathered through ground-motion instrumentation.[214] Both sets of information typically track one another, indicating the high reliability of citizen observations.

---

[211] Gail Atkinson and David Wald, "Did You Feel it? Intensity Data: A Surprisingly Good Measure of Ground Motion," *Seismological Research Letters* 78, no. 3 (May/June 2007), p. 1.

[212] USGS.

[213] David Wald et al., "'Did You Feel It?' Internet-based Macroseismic Intensity Maps," *Annals of Geophysics* 54, no. 6 (2011), p. 692.

[214] Atkinson and Wald, "Did You Feel It?" p. 2.

Figure 12.   DYFI Questionnaire.[215]

To date, more than one and a half million people have completed a DYFI questionnaire, either during or after an earthquake event.[216] Consequently, the USGS has received volumes of mostly instantaneous data. This includes data from areas without seismic instruments and for smaller earthquakes the USGS does not normally record. The USGS uses the data both qualitatively and quantitatively. Resultant CIIMs provide a unique tool for understanding earthquakes as the potential number of Internet responders

---

[215] Wald and Dewey, "Did You Feel It?" p. 2.

[216] Wald et al., "Did You Feel It?" p. 692.

far exceeds the number of available seismic instruments, and the received details exceed what can be garnered solely through instrumentation.[217] In addition to CIIMs, the USGS provides the DYFI data online in several searchable formats.[218]

The USGS touts a number of benefits to users of the DYFI Web site.[219] Individuals can garner an education and understanding about earthquakes. In addition, the process is believed to afford emotional support to citizens who have just lived through a traumatic experience by allowing them to share their experiences. Citizens are also able to contribute to the public interest by alerting and educating others about an earthquake in the region.

One limitation with the received information is its utility for emergency responders. Internet and power outages caused by high intensity damage will delay the receipt of earthquake information. In addition, the USGS has determined that poor quality and intentionally erroneous information is occasionally transmitted through the DYFI Web site. Automatic filters have been created to screen out data outliers, such as a single report from a region, by removing and flagging them but not deleting them.[220] Nonetheless, the USGS considers data received from DYFI questionnaires to be highly accurate.

2.   Analysis

The DYFI project represents the leveraging of social media by a government agency as a means to improve upon a long-standing effort to solicit a certain type of data from citizens. The development team devoted advance work toward defining what constitutes valuable data for use by the USGS. The DYFI questionnaire was designed to easily solicit relevant information. The structured form contains preformatted responses

---

[217] Wald and Dewey, "Did You Feel It?" p. 1.

[218] Wald et al., "Did You Feel It?" p. 702.

[219] Ibid., pp. 699–700.

[220] Ibid., p. 701; USGS.

that enable the transmission of uniform, and therefore easy-to-compare, data. Additionally, the team created filters as an integrity system to identify, flag, and quarantine incomplete forms and outlier information.

The DYFI project builds upon a decades-long practice, so marketing efforts have been somewhat limited. The agency disseminates a written fact sheet and has partnered with educational institutions to incorporate the Web site and use of it as a learning tool. Once individuals learn about the DYFI project, the Web site provides the instruction necessary to enable meaningful contribution. Participation involves performing a single task, the filling out of an online form. The design of the form is simple and short, leaving little room for interpretation.

The nature of the DYFI Web site transforms the one-sided push of information from citizens into a two-way exchange of information. In addition to sending in a questionnaire, a person can view citizen-generated earthquake data at any time on the Web site. The data is available in several different formats, CIIMs and searchable tables. Participant contributions are recognized through inclusion in the official maps and data tables displayed online by the USGS. Assessments demonstrate the ongoing benefit to government derived from the DYFI project.

C.   THE 2010 HAITI EARTHQUAKE

1.   Description

A 7.0 earthquake struck Haiti on January 12, 2010, impacting nearly 3.5 million people.[221] More than 300,000 were injured, and an estimated 220,000 died. Roughly 300,000 homes and 60% of government and administrative buildings were damaged or destroyed. Infrastructure was decimated, including many communications systems and gas and water mains.[222] Emergency response and relief efforts were provided by a number of governmental agencies, including several from the United States and various

---

[221] "Haiti Earthquake Facts and Figures," Disasters Emergency Committee, http://www.dec.org.uk/haiti-earthquake-facts-and-figures.

[222] Anne Nelson and Ivan Sigal, "Media, Information Systems and Communities: Lessons from Haiti," Knight Foundation, http://www.hightfoundation.org/ (January 11, 2011), p. 5.

international volunteer organizations. This resulted in the need for a mechanism to enable coordination among the various relief workers as well as communication between those workers and people in need of assistance.

An unsolicited global groundswell of individuals leveraged social-media technologies to create a number of tools to facilitate response efforts:

> A largely volunteer band of new media and information technology experts converged to apply their innovations in support of the rescue effort. They worked energetically across a range of platforms, from FM radio to Internet mapping, to test everything from SMS [text] messaging systems to new digital people-finder programs. These services, in partnership with local media, helped people find emergency food and shelter, locate missing friends and family, direct calls for help and recruit support to rebuild the country.[223]

All social media efforts were enabled through crowdsourcing and group intelligence, which produced solutions from the aggregated knowledge of those involved.

Figure 13.   Map of Global Volunteers on the Text Messaging Effort.[224]

---

[223] Ibid., p. 6; see also Jason Palmer, "Social Networks and the Web Offer a Lifeline in Haiti," BBC (January 15, 2010), http://news.bbc.co.uk/2/hi/technology/8461240.stm; Larisa Epatko, "Haiti Quake Propels Use of Twitter as Disaster-Relief Tool," PBS (February 16, 2010), http://www.pbs.org/newshour/rundown/2010/02/haiti-quake-propels-twitter-community-mapping-efforts.html; Jessica Heinzelman and Carol Waters, "Crowdsourcing Crisis Information in Disaster Affected Haiti, Special Report 252," United States Institute of Peace (October 2010), pp. 6–8.

[224] Nelson and Sigal, "Media, Information Systems," p. 16.

Typical earthquake response efforts are driven by large military and international humanitarian organizations that manage information within closed systems.[225] This differs dramatically from the open and democratic approach to information sharing fueled through crowdsourcing, though more recently emergency responders "have been increasing their support for innovative information technology."[226] The Haiti earthquake demonstrates the extraordinary level of cooperation that can occur between local media, residents, local Internet and mobile-phone service providers, diaspora networks in other countries, and responding agencies and organizations.[227] For example, local service providers agreed to furnish free connectivity so residents in need could use their mobile phones to receive announcements and communicate with others via text and calls. Devices were created to recharge mobile phones using alternative energy sources. Haitian immigrants in the United States volunteered to translate text messages sent in Creole, a language used by a portion of the local population. FEMA, the U.S. Marines and the U.S. Coast Guard worked with social-media mapping tools created by volunteers to better target response efforts.

These examples of collaboration and the integration of volunteer-driven social-media solutions were not without problems.[228] There were no preexisting connections between military or humanitarian organizations and the social media activists. Consequently, interaction occurred on an ad hoc basis through friend, relative, and professional networks somehow found to exist between individual members of each group. Additionally, technical problems resulted in periodic cell network shutdowns that caused volunteers to receive backlogs of information in floods. Locals received text announcements about rescue efforts but many times did not know whether their text requests for help had been received.

The extent to which the crowdsourced social-media efforts proved useful to emergency-response efforts is still unknown. "The Haitian earthquake may have provided

---

[225] Ibid., p. 9; Heinzelman and Waters, "Crowdsourcing Crisis Information," p. 3.

[226] Nelson and Sigal, "Media, Information Systems," p. 16.

[227] Ibid., pp. 9–13, 16–17.

[228] Ibid., p. 14.

a laboratory for innovation in emergency media response, but it is still difficult to provide a comprehensive assessment of the results."[229] Nonetheless, individuals like FEMA Director Craig Fugate recognize the potential social media holds for emergency responders. "We can adjust much quicker if we can figure out how to have this two-way conversation and if we can look at the public as a resource. The public is putting out better situational awareness than many of our own agencies can."[230]

2. Analysis

The use of social media following the Haiti earthquake represents an organically developed public-private collaboration between emergency responders and tech-savvy volunteers. Social media was leveraged to create a communication solution to allow those in need to receive announcements as well as to transmit requests for aid. Internet-based mapping tools were engaged, and improved upon, to provide more robust delineation of damage zones and to pinpoint requests for assistance. No advance work was done to establish connections between social-media volunteers and the emergency responders to whom they sought to provide technological assistance. Connections between the groups, like the social-media solutions created by the volunteers, were merely crafted on the fly.

Efforts to market the tools to emergency responders were designed as they were created. Preexisting social networks were the primary reason someone from outside of government (i.e., a volunteer) was able to connect with someone within an agency. The key conditions necessary for group intelligence—diversity of opinion, independence, decentralization, and aggregation—were created when the global network of volunteers joined together.

Volunteers worked due to altruistic motivation. Feedback came through a sense their efforts were making a valuable contribution to rescue and relief efforts. More formal recognition came when their contributions were immediately and frequently recounted in the mainstream media. There is no empirical data to assess the usefulness of social media

---

[229] Ibid., p. 15.

[230] J. Nicholas Hoover, "FEMA to Use Social Media for Emergency Response," *InformationWeek* (January 19, 2011), http://www.informationweek.com/news/government/info-management/229000918.

to emergency-response activity in Haiti. There is, however, a great deal of anecdotal evidence to support the conclusion social media has the potential to be a valuable tool for communicating with affected communities and focusing humanitarian efforts.

D.   CONCLUSION

The case studies described in this chapter suggest several generalizations about how social media can be utilized to engage members of the community and provide a conduit for citizens to disclose information beneficial to the performance of a government function. The very nature of social media promotes engagement. Tools such as interactive Web sites and texting are intuitive to many, so minimal instruction may be necessary to court participation. Co-opting devices already used by the greater population reduces the need for guidance about how they can be used to enable citizen-government collaboration.

Each example in this chapter involves citizen participants performing one or more tasks that contribute to an effort already being handled by a government agency. The case studies demonstrate citizens motivated by the unselfish desire to contribute will do just that, whether or not solicited to do so. Government agencies can target contribution through the assignment of a discrete task for volunteers to perform. Both the P2P and DYFI projects incorporated this type of framework. The Haiti earthquake suggests that volunteers can also rapidly accommodate multiple simultaneous tasks, even when the tasks have been identified solely by the coalition's members instead of government.

The case studies provide several generalizations about how utilizing structured social-media mechanisms to guide information exchange can impact the value of citizen contributions. The P2P project team developed a virtual collaborative environment to facilitate group efforts to obtain relevant prior art for use by patent examiners. The DYFI project team developed a short, preformatted questionnaire to ensure the information received is both advantageous to the USGS and easy to compare so CIIMs can be created. In both situations, the nature of the implemented social-media tool was heavily

influenced by advance work. The advance work involved delineating the precise agency effort to be addressed, the task(s) for citizens to perform, the nature of contributions citizens could make and what the agency was going to do with the received information.

A secondary manner in which structured mechanisms can impact citizen contributions is by enabling the performance of a value assessment of the received information. Preformatted and check-the-box responses, like those appearing in the short DYFI questionnaire, promote scientific data analysis since received information is uniform and consistent. They also enable the identification of outlier responses, such as when only one person in a region reports an earthquake, so the problem data can be filtered and isolated.

Both the P2P and DYFI projects created assessment tools before data was collected. It is unclear, however, whether the nature of the social media mechanism(s) being employed dictates the design of an assessment tool or, conversely, to what extent the design of an assessment tool will influence the nature of the data exchange process being implemented. The absence of an assessment tool appears to hamper the ability to perform an empirical evaluation of the contributions. Anecdotal evidence from the Haiti case study suggests social media was beneficial to emergency responders. Anecdotal evidence alone, however, is not reliable enough to draw broad-based conclusions about the utility of social media during all types of disasters. "The primary weakness of anecdotes as evidence is that they are not controlled. This opens them up to many hidden variables that could potentially affect the results."[231]

The only case study to include both the one-way push of information as well as two-sided conversations through social media, thereby allowing a comparison between the two avenues of information exchange, is the Haiti earthquake. Anecdotal evidence suggests people receiving pushes of information (e.g., announcements and alerts) derive some benefit. For example, locals in Haiti were advised of the location and type of relief activities that were underway. Anecdotal evidence also suggests people transmitting

---

[231] Steven Novella, "The Role of Anecdotes in Science-Based Medicine," *Science-Based Medicine*, http://www.sciencebasedmedicine.org/index.php/the-role-of-anecdotes-in-science-based-medicine/ (January 30, 2008).

information for use by a government entity who get no response indicating the transmission was received (i.e., feedback) feel frustration and question the utility of their activity. These conclusions are intuitive but of limited utility since they are not based upon scientifically accepted data analysis principles.

The case studies provide several generalizations about what conditions must exist within a government agency for social media to provide a conduit for information to flow from citizens. The studies suggest:

- an agency needs to be willing to receive information sent by members of the public;
- an agency needs to recognize the value such information holds;
- an agency needs to devote resources sufficient to respond to received transmissions, recognize valuable contributions, and encourage further participation.

The prevalence of social media usage in society today is demonstrated by the literature. The altruistic desire of citizens to contribute to the performance of government is suggested by the case studies. Together, they indicate the potential utility of integrating social media as a mechanism to foster citizen collaboration and enable the exchange of information to further government efforts.

THIS PAGE INTENTIONALLY LEFT BLANK

V. IMPLEMENTATION RECOMMENDATIONS FOR INTEGRATING SOCIAL MEDIA INTO THE NSI

You don't make progress by standing on the sidelines, whimpering and complaining. You make progress by implementing ideas.

Shirley Hufstedler, former U.S. Secretary of Education

The literature and case studies suggest a number of preliminary tasks should be addressed before social media mechanisms are incorporated by law enforcement agencies as a tool to develop crime- and terrorism-related tips. The tasks fall into several categories: advance work, policy design, training, and budgeting.

A. ADVANCE WORK

The primary precursor to adoption of social media as a mechanism to develop SARs is for agency leadership to set the tone by:

- creating a culture of collaboration;
- communicating within the agency the acceptance of incorporating social media technology to engage with the public;
- dedicating resources and staff sufficient to monitor and respond to information as it is received.

Radian6, a company that provides advice, support, and services to organizations heading down the social-media path, recommends assembling a core group to handle design and implementation functions for the project.[232] The group should be comprised of legal, technical, and human-resources staff and at least one employee who will be utilizing social media to connect with the public. The group should be headed by a senior person who handles public relations for the organization. In addition, at least one high-ranking agency manager should be associated with the group to encourage attendance and participation by members.

---

[232] Byl, Nelson, and Thomas, "Social Media Blueprint," pp. 10, 12.

The core group's advance work should entail the following activities:

- discerning what devices community members are already using to communicate with one another (to decrease the learning process for citizens the agency seeks to engage);

- defining the type(s) of information citizens can transmit to the agency (e.g., text, photographs, video);

- determining steps to market the social-media mechanism to promote citizen use of it;

- developing a feedback process that confirms receipt of submissions and encourages further citizen participation;

- defining what constitutes "success" in the social-media venture and how it can be measured;

- determining what, if any, results will be shared publicly as further feedback with the community (e.g., $\underline{X}$ number of tips were received, which resulted in $\underline{X}$ number of arrests/interdictions);

- learning from the smart practices of other agencies by discussing what has and has not worked and understanding the pitfalls that may be encountered.

The more steps a law enforcement agency takes before rolling out a social-media mechanism that enables the flow of crime- and terrorism-related tips and information, the greater the likelihood the agency can exert control over and assess the value of the effort.

B.   POLICY AND TRAINING RECOMMENDATIONS

The literature suggests a variety of components for inclusion in a law enforcement agency's social-media policy. Each component sets expectations for agency personnel while empowering them to innovate through the technology. For example:

- Personnel devoted to developing SARs should be afforded access to social media and social-networking sites tools during regular work hours.

- The policy should delineate whether social-media usage will be permitted for all agency personnel or just those in the intelligence unit dedicated to developing SARs.

- The policy should contain language from or at least reference applicable laws and regulations, such as restrictions upon broad dissemination of personal identifying information.

- The policy should outline what constitutes professional conduct and respectful communication.

78

- The policy should also describe the agency's efforts to afford contributors anonymity, should they request it, whether and how information will be kept confidential, and steps the agency will take to protect individuals' privacy.

Training provides the opportunity for employees to become familiar with using social-media tools while reinforcing agency expectations about how they are to be utilized. "[P]ersonal social media use is quite different from social media use for business purposes, and as you integrate more teams into your larger social strategy, it's your responsibility to get everyone involved on the same page."[233] The literature suggests agency transparency can be furthered by disseminating a copy of the social-media policy to the public, along with a parallel policy delineating acceptable citizen conduct.

C.   BUDGETING TO ADDRESS LEGAL MANDATES

Legal mandates can increase the lifetime budget of a law enforcement technology-related program, such as the creation of online conversations and content exchange through social media, because storage of the created images is required for several distinct reasons.

1.   Record Retention and Production Laws

The first requirement, and one that impacts all states in the country, is open-records laws.[234] These laws are patterned after the federal Freedom of Information Act (FOIA). Illinois's FOIA statute, for example, mandates with few exceptions that "all records in the custody or possession of a public body are presumed to be open to inspection or copying."[235] The definition of "public record" is very broad and covers all materials "pertaining to the transaction of public business, regardless of physical form or characteristics, having been prepared by or for, or having been or being used by, received by, in the possession of, or under the control of any public body."[236] The language of the Illinois statute includes social-media text and images in the possession of a law enforcement agency as public records.

---

[233] Radian6, "Training Your Company for Social Media," Community Ebook (April 2011), p. 2.

[234] Open Government Guide, http://www.rcfp.org/ogg/index.php, retrieved July 3, 2011.

[235] 5 ILCS 140/1.2.

[236] 5 ILCS 140/2(c).

The purpose behind FOIA laws is grounded in public policy. For example, the legislature in Illinois decreed:

> Pursuant to the fundamental philosophy of the American constitutional form of government, it is declared to be the public policy of the State of Illinois that all persons are entitled to full and complete information regarding the affairs of government and the official acts and policies of those who represent them as public officials and public employees consistent with the terms of this Act.[237]

The conclusion reached by the Illinois legislature is similar to that reached by other state legislatures: access to public records promotes the transparency and accountability of government.

Record retention laws impose an additional legal requirement on many state and local units of government, further necessitating the expenditure of monies to retain electronic records. Not every state has a record retention requirement based in statute. It may exist through policy.[238] Illinois is one state that has a statutory requirement, and a review of the law's language is helpful to understanding the concept of record retention. The Illinois Local Records Act decrees that all "public records made or received by, or under the authority of, or coming into the custody, control or possession of any officer or agency shall not be mutilated, destroyed, transferred, removed or otherwise damaged or disposed of, in whole or in part, except as provided by law."[239]

The definition of a public record in this statute, similar to the one found in open-records FOIA laws, is very broad and includes those things "made, produced, executed or received by any agency or officer pursuant to law or in connection with the transaction of public business and preserved or appropriate for preservation . . . as evidence of the organization, function, policies, decisions, procedures, or other activities thereof, or because of the informational data contained therein."[240]

---

[237] 5 ILCS 140/1.

[238] NASCIO, " Electronic Records Management and Digital Preservation: Protecting the Knowledge Assets of the State Government Enterprise." NASCIO. http://www.nascio.org/ (October, 2007), p. 3.

[239] 50 ILCS 205/4.

[240] 50 ILCS 205/3.

The obligation to preserve electronic records under Illinois's Local Records Act is absolute. The statute provides that no public record can be disposed of except pursuant to a formal retention policy that has received prior written approval of the appropriate Local Records Commission.[241] The absence of a retention policy imposes a lifetime retention requirement for the item in question.

The third legal requirement that imposes a burden upon state and local units of government for the retention of electronic records is known as preservation of evidence. A duty to preserve evidence, such as electronic records, is owed if a reasonable person should have foreseen that the item is material to a potential civil action.[242] "Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.[243]

The duty to preserve evidence applies not just to parties to litigation. The duty applies to anyone, including an employee of a state or local unit of government who is in possession of or exerts control over an item that a party may want to use in litigation. The duty to preserve has even been extended to cover the scenario where a party to litigation cannot fulfill the duty to preserve because he or she does not own or control the evidence (e.g., it is under the control of a third party): "the party still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence."[244]

The consequence of failure to abide by the legal duty to preserve includes a wide range of penalties. When the person who or entity that failed to preserve an item of evidence is a party to the litigation, the penalty can result in or increase the likelihood of a finding of liability and, in turn, the award of monetary damages.[245] Alternatively, the

---

[241] 50 ILCS 205/7.

[242] *Boyd v. Travelers Insurance Company*, 166 Ill.2d 188, 652 N.E.2d 267, 271 (1995).

[243] *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2nd Cir. 1999), quoting generally from Black's Law Dictionary.

[244] *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001).

[245] *Hirsch v. General Motors Corp.*, 266 N.J. Super. 222, 260 (1993).

penalty can include dismissal of the case, an order by the court restricting the defenses that can be claimed during litigation, or an order by the court restricting the evidence and testimony that can be presented during trial.

The penalty can also include an instruction to the jury that a party's destruction of evidence relevant to an issue at trial supports an inference that the evidence "would have been unfavorable to the party responsible for its destruction."[246] Such an instruction can be devastating to the fact trier's decision. Finally, whether or not the person who or entity that failed to preserve an item of evidence is a party to the litigation, a monetary penalty can be imposed, including a fine, attorney's fees, and court costs associated with bringing the issue to the court's attention.[247]

2.   Budgeting Recommendations

Procuring the capital investment for a law enforcement technology-related venture occurs at the start of the program, not throughout its duration. Budgeted expenditures usually include the initial purchase, installation and maintenance of computer software and hardware, as well as upgrades to existing technology equipment. They also usually include a salary component to cover the cost of one or more employees to interact through the technology, such as by disseminating updated information to the public and monitoring the text and photographic images received in return. Costs associated with electronic-records management, including retention, preservation, and production pursuant to the aforementioned legal requirements, are not typically factored into the initial budget equation for a social-media program, though they should be.

NASCIO, the National Association of State Chief Information Officers, recommends also including electronic-records management costs in the overall budget for any technology project:

> The better approach is to examine requirements for digital preservation at the time a business need is identified, management initiatives are planned, and systems for supporting those initiatives are designed and developed.

---

[246] *Kronisch v. United States*, 150 F.3d 112, 126 (2nd Cir. 1998).

[247] *Mosaid Technologies, Inc. v. Samsung Electronics Co.*, 348 F.Supp.2d 332, 339 (2004).

> In other words, digital preservation as well as electronic records management issues need to be planned and budgeted part and parcel with any initiative that will create data, information or knowledge. When information will be created by an enterprise, the lifecycle of that information must be determined. Further, it must be valued at each phase of that lifecycle. Those economics along with regulatory requirements determine how long information will be retained by the enterprise.[248]

Budgeting for electronic-records management efforts needs to include hardware (e.g., server(s) for storage), software (i.e., a system for retrieval and production of items), and personnel to timely respond to preservation and production requests. Obtaining additional funding during the course of a new technology-related program, as opposed to at its onset, is often very difficult to achieve.[249] An agency that seeks to obtain more funding midstream to cover a cost that should have been included at the outset could face significant opposition and criticism.

a. Strategic Implementation

Legal retention and production mandates are well established but only known to attorneys whose practice area includes FOIA law and litigation. For example, social media "presents unique challenges during litigation, because data changes fast, content often resides on third-party servers, and getting access may require knowledge of passwords or other privacy settings."[250] Information technology (IT) personnel and agency decision makers likely are not aware of these requirements. Attorneys employed by or who regularly represent an agency embarking on a social-media program should conduct training for involved staff and managers to acquaint them with both the legal requirements and the need to include monetary and personnel resources in the initial budget to address them. Familiarity and understanding can promote intelligent budgeting decisions.

---

[248] NASCIO, "Electronic Records," p.2.

[249] Ibid.

[250] Michael Collyard, "E-Discovery: Riding Herd on Social Media ESI," *InsideCounsel*, http://www.insidecounsel.com/2011/10/03/e-discovery-riding-herd-on-social-media-esi (October 3, 2011).

Additionally, support of this budgeting strategy from the head of the agency implementing the social-media program is vital. Law enforcement entities are paramilitary-style operations. Orders and direction are disseminated from the top and expected to be incorporated and acted upon by all employees. It is vital to educate the agency's leader about legal retention and production mandates so necessary electronic-records management infrastructure costs are included in the budgeting process engaged in by those tasked with bringing the program to life.

Education efforts must emphasize that hefty monetary penalties imposed upon an agency due to the failure to abide by and budget for these legal requirements will end up negatively impacting the agency in several ways. Court-imposed damage awards, fines, fees, and costs will be footed by taxpayers through the agency's corporate budget. When this occurs, there may be significant backlash from the agency's funding body due to negative press coverage and outrage expressed to elected officials by constituents. In addition, midstream increases to the lifetime budget of the technology program may be perceived as "cost overruns." This, too, can lead to a diminishment in both public and political support for the project.

b.   *Potential Hurdles*

Opposition to the budgeting strategy of including infrastructure costs to cover the retention and retrieval of electronic records will occur during the project's planning stage. That is the stage when monetary calculations and funding streams are being evaluated—before a final decision has been made about defining the project's scope. Opposition will likely be encountered from the law enforcement agency's finance division or grant program manager, depending upon the source of the project's funding. The argument proffered will be that money spent on servers, software, and personnel for electronic-records management infrastructure is less money available for other law enforcement projects. The problem with such a viewpoint is it presumes electronic-records management infrastructure costs are an optional component to a social-media program. In actuality, such infrastructure costs are an integral component and must be reflected in the initial project budget.

84

In addition, some decision makers involved with the social-media project's design and implementation may view the investment in electronic-records management infrastructure as akin to purchasing insurance: it is something you are required to obtain but may never need or use. Such a viewpoint, however, is ill advised. The legal mandates are clear, and the monetary consequences from failing to preserve and/or produce public records are potentially dire. Gambling with taxpayer money is indefensible and can poorly position an agency come the next general budget season.

Finally, some decision makers may not see a derivative benefit for the agency from retaining electronic records created through a social-media program. The education efforts referenced above should include examples of captured content, both text and images, that can work to the law enforcement agency's advantage in defense of lawsuits claiming false arrest or illegal search. Being able to present a time-stamped copy of information transmitted to the agency, along with demonstrating steps taken to vet the information before taking action upon it, can go a long way to defending the agency's conduct in court.

Despite best efforts, government attorneys may be faced with defending an agency that failed to provide the infrastructure necessary to retain and produce electronic records generated through a social-media program. The reality of any law practice is clients may not follow legal advice, regardless of how sound and well reasoned it is. In this context, however, courts will reject arguments that a lack of monetary and/or personnel resources prevented the agency from fulfilling its obligations under the law. Penalties will be imposed when the failure to retain and produce issues reach the courtroom. Unfortunately, such an outcome may be needed to convince an agency head to strategically budget for electronic-records management infrastructure.

D.   CONCLUSION

The literature and case studies suggest a number of preliminary tasks should be addressed before social-media mechanisms are incorporated as a tool to develop crime- and terrorism-related tips. The agency head needs to set the tone by communicating the acceptance of social media as a tool for developing SARs and dedicating monetary and

staff resources to fully support the effort. A team needs to be assembled to craft policy and conduct training for impacted agency personnel. Marketing efforts are needed to court citizen interest and encourage participation. Each of these steps can enable an agency to exert control over the collaborative effort, assess its value, and make necessary adjustments along the way.

VI. CONCLUSION

We have the duty of formulating, of summarizing, and of communicating our conclusions, in intelligible form, in recognition of the right of other free minds to utilize them in making their own decisions.

Ronald Fisher, mathematician

A. DISCUSSION AND RECOMMENDATIONS

The NSI envisions law enforcement agencies will develop crime- and terrorism-related tips from citizens and synthesize those with information obtained from other sources to create SARs. The NSI process delineates front-line personnel can solicit relevant behaviors observed by the public through in-person or telephonic interviews or online etips forms. It does not, in its current form, include the use of less formal social-media tools such as text messaging, mobile-phone apps and social-networking sites like Facebook and Twitter, though some agencies are doing just that. The literature demonstrates the majority of people in America use social-media and social-networking sites to communicate every day. In addition, more than three-quarters of people already use this technology to participate in at least one group that is focused on issues impacting the community in which they live.

Citizens will vary in terms of their willingness to proactively provide information to law enforcement, no matter how timely, relevant, or actionable it may be. Nonetheless, some will be willing to collaborate with officers on developing SARs that can protect their families and communities. Including social media technologies as an option for communicating a tip provides another and likely familiar means by which interested individuals can provide information about their observations.

Recommendation #1: The NSI model and the Notional SAR Process (Figure 7) should be amended to include social media as an additional avenue for transmission of tips from the public.

Citizens may also vary in terms of the types of social-media mechanisms they feel comfortable using. For example, etips, text, and social-networking sites offer a variety of structure to the information exchange process. The literature and case studies strongly suggest an etips form or mobile-phone app that seeks to impose structure on the

87

information being relayed should be short and user friendly. Preformatted drop-down values or check-the-box options enable the transmission of uniform and consistent data. A social-media tool incorporating this type of structure may be perceived as onerous if the individual has too many data fields to wade through. In contrast, text messaging and social-networking sites offer the ability to transfer information in a more natural and conversational way.

> Social-networking sites may also offer a collaborative environment that enables multiple community members to work in tandem to produce a piece of information. The very nature of sites like Facebook and Twitter enable group intelligence by allowing a diverse group of individuals to asynchronously improve the end product of their discussion. Social-media mechanisms that merely allow the transmission of information from a single citizen to an agency, such as text messaging and smart-phone apps, do not create the environment for group intelligence to function.

Recommendation #2: An agency should adopt a variety of social media tools to appeal to the largest number of individuals in the community.

The decision to include social media as another mechanism to accept the transmission of crime- and terrorism-related tips must be made at the uppermost level of the agency to set the tone for all involved employees. Social-media software typically carries a low cost, but the overhead to maintain mechanisms designed to elicit tips, update requests for contributions sent to the public, and review submitted material will entail designating one or more agency employees, ideally operating around the clock. In addition, legal mandates require government agencies retain and produce the electronic records they receive in the ordinary course of business for a variety of reasons. Budgeting to cover the costs of retention and production should be included when the resource calculations are initially conducted. Another cost will be incurred should an agency decide to create metrics to measure the amount and usefulness of citizen contributions through social media. An absence of metrics will prevent meaningful assessment of using this mechanism to develop SARs.

Recommendation #3: The decision to include social media, like the decision to participate in the NSI, will require commitment of the agency head as well as the dedication of personnel and monetary resources.

An agency should do some groundwork to determine what social media technologies are most commonly used by community members to communicate with one another. Work should be done to market the effort in simple terms, such as by describing it as a virtual 911 for relaying crime- and terrorism-related text, photographs, and video.

Using social media for a law enforcement purpose differs from using it to engage in informal conversation with friends. For that reason, training is needed both for agency personnel and citizens to set expectations about the type of information considered relevant to the NSI. To protect against retribution, an agency should include the ability for tips to be relayed anonymously. In addition, officers should meet with community members to both promote the social-media avenues for relaying tips and provide encouragement. Community meetings of this nature can build a foundation of trust for citizen-agency collaboration. While regular outreach efforts can court citizen participation, an agency leveraging social-media tools to develop SARs should also consider providing feedback to reward past and encourage further contributions.

Recommendation #4: Courting citizen participation in the NSI through social media will encompass ongoing efforts to build trust between the agency and the community.

Policies should be established to guide both agency personnel and community members using social media to develop SARs. The IACP has already developed a robust social-media policy (see Appendix A) that can serve as a prototype for any agency. The sample policy can be tailored based on the specific social-media tool(s) being implemented and contributions garnered through smart-practice discussions with other agencies who already utilize one or more of the tools. A policy for citizen usage of social media to send tips need not be as complex. Instead, it should set the tone for acceptable language and constructive messages.

Agency social media and SARs policies should be shared with the public to further agency transparency, demystify the SARs process, and allay fears about how transmitted information will be utilized by the agency. The NSI already includes

designating an officer to handle privacy and civil liberties issues that arise with SARs.[251] That same officer should be involved with or handle similar issues that arise with citizen use of social media to transmit tips.

Agencies may also fear the perceived volume of social media–driven communication that will be sent to the agency due to worries the agency is not capable of handling it. The literature suggests, however, that social media is utilized by a number of individuals to facilitate conversations that are already occurring. Social media does not appeal to everyone. It may, however, appeal to some, and having the option to provide suspicious observations reports through a social-media mechanism may influence a certain segment of society to contribute to the NSI that otherwise may not have had the interest in relaying a tip. In addition, the NSI framework already incorporates a component for reviewing and vetting received information before the SAR is passed along to a fusion center or JTTF.[252] This vetting process will also apply to tips relayed via social media and work to allay apprehension about receiving unverified reports.

> ***Recommendation #5: Agencies should develop policies and conduct training to set expectations for both agency personnel and the community about the use of social media as a mechanism to develop SARs.***

Including social media as another mechanism by which citizens can transmit crime- and terrorism-related tips and information to their local law enforcement agencies provides an exciting next step for the NSI.

B.   SUGGESTIONS FOR FURTHER RESEARCH

A review of the relevant literature did not reveal any studies conducted to assess the usefulness of social media as a law enforcement tool to solicit tips for SARs. Ideas for future study therefore include:

- Research to compare the accuracy and usefulness of information relayed via a social-media mechanism versus in-person, on the telephone, and through etips forms. A side-by-side comparison could reveal the avenue(s) law enforcement

---

[251] "Fact Sheet, Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations Report for the Nationwide Suspicious Activity Reporting Initiative (NSI)." Washington, D.C.: Nationwide SAR Initiative, http://nsi.ncirc.gov/.

[252] Ibid.

agencies should most rely upon to develop SARs. This would be most valuable to agencies with limited monetary and personnel resources. It could also determine whether the ultimate utility of transmitted tips is in any way impacted by the vehicle used for transmission. If so, further revision may be needed to the Notional SAR process information flow.

- Research to determine whether the prevalent usage of social media in society means formally including the technology in the NSI dramatically increases the volume of crime- and terrorism-related information received by local agencies. The research could attempt to determine whether the popularity of the transmission mechanism (e.g., social media versus land-line telephones) impacts the number of tips and volume of citizen participation.

- Research to compare the volume of false information transmitted through social-media mechanisms versus through each of the established transmission mechanisms (i.e., in-person interview, telephonic questioning, etips form).

Each of these studies is beyond the scope of this thesis and would likely entail a combination of raw data, surveys, and interviews.

C.   CONCLUSION

Social media is presented here as another tool for law enforcement to incorporate in its efforts to engage and collaborate with the public. The NSI involves obtaining tips and information to both detect and prevent events, thereby protecting communities from crime- and terrorism-related incidents. Formally including social media in the Notional SAR Process would be a national policy pronouncement designed to cultivate consistent application of such tools to develop SARs.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alexander, Dan. "Using Technology to Take Community Policing to the Next Level." *Police Chief Magazine* (July 2011).

Allan, Stuart. "Citizen Journalism and the Rise of 'Mass Self-Communication': Reporting the London Bombings." *Global Media Journal*, Australian ed., 1, no. 1 (2007).

Allen, Naomi, Joanne Ingham, Bridgette Johnson, Joseph Merante, Beth Noveck, William Stock, Yeen Tham, Mark Webbink, and Christopher Wong. "Peer to Patent First Anniversary Report." Center for Patent Innovations, New York Law School (June 2008).

Allen, Naomi, Andrea Casillas, Jason Deveau-Rosen, Jason Kreps, Thomas Lemmo, Joseph Merante, Michael Murphy, Kaydi Osowski, Christopher Wong, and Mark Webbink. "Peer to Patent Second Anniversary Report." Center for Patent Innovations, New York Law School (June 2009).

Associated Press. "CIA Analysts Comb Social Media for Trouble Spots." National Public Radio. http://www.npr.org/2011/11/04/142029141/cia-analysts-comb-social-media-for-trouble-spots (November 4, 2011) (last retrieved January 9, 2012).

Atkinson, Gail, and David Wald. "Did You Feel It? Intensity Data: A Surprisingly Good Measure of Ground Motion." *Seismological Research Letters* 78, no. 3 (May/June 2007).

Bach, Robert, and David Kaufman. "A Social Infrastructure for Hometown Security, Evolving the Homeland Security Paradigm." *CNA Analysis & Solutions* (January 23, 2009).

Best, Richard, and Alfred Cumming. "CRS Report for Congress, Open Source Intelligence (OSINT): Issues for Congress." Congressional Research Service, Order Code RL 34270 (January 28, 2009).

Bjelopera, Jerome. "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress." Congressional Research Services, N. R40901 (June 10, 2011).

Boyd v. Travelers Insurance Company, 166 Ill. 2d 188, 652 N.E.2d 267 (1995).

Brenner, Joanna. "Pew Internet: Social Networking (Full Detail)." Pew Research Center's Internet & American Life Project. http://www.pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx (March 29, 2012) (last retrieved August 4, 2012).

Burlington City, New Jersey, Police Department. http://burlingtonpolicenj.com/ (last retrieved June 30, 2012).

Burlington City, New Jersey, Police Department eTips. http://burlingtonpolicenj.com/eservices/etips (last retrieved June 30, 2012).

Byl, Bart, Amanda Nelson, and David Thomas. "Social Media Blueprint: A Step-by-Step Plan to Prepare Your Company." Radian6, Community ebook (April 2012).

Carter, David. "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies." U.S. Department of Justice, Office of Community Oriented Policing Services (January 2009).

Chicago Police Department. http://www.chicagopolice.org.

Chicago Police Department Community Policing e-Tip. https://portal.chicagopolice.org/xdb/cpdportal/f?p=712:110:2695960673384871 (last retrieved June 30, 2012).

Chicago Police Department TXT2TIP. https://portal.chicagopolice.org/portal/page/portal/ClearPath/Communities/Crime%20Prevention/TXT2TIP (last retrieved June 25, 2012) (last retrieved June 30, 2012).

CIO Counsel. "Guidelines for Secure Use of Social Media by Federal Departments and Agencies." http://www.cio.gov (September 2009) (last retrieved August 17, 2012).

Cohen, Lori. "Six Ways Law Enforcement Uses Social Media to Fight Crime." http://mashable.com/2010/03/17/law-enforcement-social-media (March 17, 2010) (last retrieved August 4, 2012).

Collin, Philippa, Kitty Rahilly, Ingrid Richardson, and Amanda Third. "The Benefits of Social Networking Services." Cooperative Research Centre for Young People, Technology and Wellbeing. Inspire Foundation, Australia. https://docs.google.com/viewer?a=v&q=cache:2TNJ3Ghyn2kJ:www.interactivemediarelease.com/download.php?f%3D0neo1k_FINAL_The_Benefits_of_Social_Networking_Services_Lit_Review.pdf+The+Benefits+of+Social+Networking+Services&hl=en&gl=us&pid=bl&srcid=ADGEESiI9SyXCv7mh-efCI0yRw1KzWjhJx3Y5EqZL4gobc0OiGKb29MDUyVnOq-LZUU6Dn6K47Br8aj8BRZvRrmAMCnFoLkdJeRQHeHnSVarTdGi4K7mOh37IjW5VKdG5nJt0KAHJLMp&sig=AHIEtbSHpRqPc5Y1xtKXsIqiBAwQKOLQhQ (April 5, 2011) (last retrieved August 4, 2012).

Collyard, Michael. "E-Discovery: Riding Herd on Social Media ESI." *InsideCounsel*. http://www.insidecounsel.com/2011/10/03/e-discovery-riding-herd-on-social-media-esi (October 3, 2011) (last retrieved July 14, 2012).

Criminal Intelligence Coordinating Council. "Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project." Global Information Sharing Toolkit. http://www.it.ojp.gov/ (October 2008) (last retrieved August 17, 2012).

Currie, Donya. "Special Report: Expert Round Table on Social Media and Risk Communication During Times of Crisis: Strategic Challenges and Opportunities." American Public Health Association. http://www.apha.org/NR/rdonlyres/47910BED-3371-46B3-85C2-67EFB80D88F8/0/socialmedreport.pdf (2009) (last retrieved August 4, 2012).

Director of National Intelligence. "National Open Source Enterprise, Intelligence Community Directive Number 301." United States Office of the Director of National Intelligence (July 11, 2006).

Director of National Intelligence. "National Open Source Enterprise, Intelligence Community Directive Number 304." United States Office of the Director of National Intelligence (July 9, 2009).

Drapeau, Mark, and Linton Wells. "Social Software and National Security: An Initial Net Assessment." Center for Technology and National Security Policy, National Defense University (April 2009).

Epatko, Larisa. "Haiti Quake Propels Use of Twitter as Disaster-Relief Tool." PBS. http://www.pbs.org/newshour/rundown/2010/02/haiti-quake-propels-twitter-community-mapping-efforts.html (February 16, 2010) (last retrieved July 16, 2012)..

"Fact Sheet, Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations Report for the Nationwide Suspicious Activity Reporting Initiative (NSI)." Washington, DC: Nationwide SAR Initiative. http://nsi.ncirc.gov/ (last retrieved August 17, 2012).

Federal Bureau of Investigation. Uniform Crime Reports. http://www.fbi.gov/about-us/cjis/ucr/ucr (last retrieved August 17, 2012).

Fitsanakis, Joseph. "Analysis: CIA Open Source Center Monitors Facebook, Twitter, Blogs." IntelNews. http://intelnews.org/2011/11/08/01-861/#more-7508 (November 8, 2011) (last retrieved August 4, 2012).

Fresenko, Victoria. "Social Media Integration into State-Operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges." Master's thesis, Naval Postgraduate School (December 2010).

Fung, Brian. "The Intelligence Community Gets Social." *Washington Post*. http://www.washingtonpost.com/blogs/innovations/post/the-intelligence-community-gets-social/2011/09/13/gIQAvlrldK_blog.html (September 19, 2011) (last retrieved April 22, 2012).

Gnoted Tech Blog. "What is Twitter and How Does it Work—Beginners Guide." http://gnoted.com/what-is-twitter-and-how-does-it-work-beginners-guide/ (February 8, 2009) (last retrieved October 22, 2011).

Golder, Scott, and Bernardo Huberman. "The Structure of Collaborative Tagging Systems." Cornell University Library. http://www.hpl.hp.com/research/idl/papers/tags/tags.pdf (2005) (last retrieved October 18, 2011).

Greene, Jack. "Community Policing in America: Changing the Nature, Structure, and Function of the Police." *Criminal Justice 2000* (July 2000).

"Haiti Earthquake Facts and Figures." Disasters Emergency Committee. http://www.dec.org.uk/haiti-earthquake-facts-and-figures (last retrieved July 18, 2012).

Hampton, Keith, Lauren Goulet, Lee Rainie, and Kristen Purcell. "Social Networking Sites and Our Lives." Pew Research Center, Pew Internet & American Life Project. http://pewinternet.org/ (June 2011) (last retrieved August 4, 2012).

Heinzelman, Jessica, and Carol Waters. "Crowdsourcing Crisis Information in Disaster Affected Haiti, Special Report 252." United States Institute of Peace (October 2010).

Henrikson, Jenise. "The Growth of Social Media: An Infographic." *Search Engine Journal.* http://www.searchenginejournal.com/the-growth-of-social-media-an-infographic/32788/ (August 30, 2011) (last retrieved October 27, 2011.

Hirsch v. General Motors Corp., 266 N.J. Super. 222 (1993).

Hoover, J. Nicholas. "FEMA to Use Social Media for Emergency Response." *InformationWeek* http://www.informationweek.com/news/government/info-management/229000918 (January 19, 2011) (last retrieved July 18, 2012).

Hotz, Robert. "Decoding Our Chatter." *Wall Street Journal* (October 1, 2011).

Hrdinova, Jana, Natalie Helbig, and Catherine Peters. "Designing Social Media Policy for Government: Eight Essential Elements." Center for Technology in Government, University at Albany, Research Foundation of State University of New York (May 2010).

Hutton, Graeme, and Maggie Fosdick. "The Globalization of Social Media." *Journal of Advertising Research* (December 2011).

Illinois Freedom of Information Act, 5 ILCS 140/1, et seq.

Illinois Local Records Act, 50 ILCS 205/1, et seq.

International Association of Chiefs of Police. "2010 IACP Social Media Survey." IACP Center for Social Media (2010).

———. "2011 IACP Social Media Survey." IACP Center for Social Media (2011).

———. "IACP Law Enforcement Executives' Social Media Top Ten." Bureau of Justice Assistance, U.S. Department of Justice (January 2011).

International Association of Chiefs of Police. "Mobile Fact Sheet." (March 2011).

International Association of Chiefs of Police, IACP National Law Enforcement Policy Center. "Social Media, Concepts and Issues Paper." (September 2010).

Internet World Stats. "Usage and Population Statistics, Facebook Users in the World, Facebook Growth Stats for 2011–2012." http://www.internetworldstats.com/facebook.htm (last retrieved July 14, 2012).

Jenkins, Henry. *Convergence Culture, Where Old and New Media Collide*. New York University Press (2006).

Johnson, Samuel. "Improved Web 2.0 Strategy for FEMA to Enable Collaboration and a Shared Situational Awareness across the Whole of Community." Master's thesis, Naval Postgraduate School (March 2012).

Kronisch v. United States of America, 150 F.3d 112 (2nd Cir. 1998).

Lagoudakis, John. "How Does Twitter Work?" http://johnlagoudakis.com/how-does-twitter-work/ (April 6, 2011) (last retrieved October 22, 2011).

Laguna Vista, Texas, Police Department. http://www.lvtexas.com/ (last retrieved June 30, 2012).

Laguna Vista, Texas, Police Department ETips Submission. http://www.lvtexas.com/etips.html (last retrieved June 30, 2012).

Lawless, Michael. "Institutionalization of a Management Science Innovation in Police Departments." *Management Science* 33, no. 2 (February 1987).

Lindsay, Bruce. "Social Media and Disasters: Current Uses, Future Options, and Policy Considerations." Congressional Research Service, Order Code R41987 (September 6, 2011).

Lowensohn, Josh. "Newbie's Guide to Facebook." CNET. http://news.cnet.com/newbies-guide-to-facebook/ (August 1, 2007), (last retrieved October 22, 2011).

Madden, Mary, and Kathryn Zickuhr. "Sixty-five Percent of Online Adults Use Social Networking Sites." Pew Research Center, Internet & American Life Project, http://pewinternet.org/ (August 2011) (last retrieved August 4, 2012).

Mosaid Technologies v. Samsung Electronics Co., 348 F.Supp.2d 332 (D.N.J. 2004).

Mumm, Nicholas. "Crowdsourcing: A New Perspective on Human Intelligence Collections in a Counterinsurgency." *Small Wars Journal.* http://smallwarsjournal.com/node/12036 (January 3, 2012).

Musser, John. "Web 2.0 Principles and Best Practices." O'Reilly Radar. http://oreilly.com/ (Fall 2006) (last retrieved August 17, 2012).

National Association of Chief Information Officers. "Friends, Followers, and Feeds: A National Survey of Social Media Use in State Government." NASCIO. http://www.nascio.org/ (September 2010) (last retrieved April 24, 2012).

National Association of Chief Information Officers. "Electronic Records Management and Digital Preservation: Protecting the Knowledge Assets of the State Government Enterprise." www.nascio.org/publications/documents/nascio-socialmedia.pdf (October 2007) (last retrieved April 24, 2012).

Nations, Daniel. "What is Social Media?" About.com. http://webtrends.about.com/od/web20/a/social-media.htm (last retrieved June 30, 2012).

Nelson, Anne, and Ivan Sigal. "Media, Information Systems and Communities: Lessons from Haiti." Knight Foundation. http://www.knightfoundation.org/ (January 11, 2011).

New York Police Department. www.nyc.gov/nypd/ (last retrieved June 30, 2012).

New York Police Department Crime Stoppers. https://a056-crimestoppers.nyc.gov/crimestoppers/public/tipForm.cfm?pgLang=english&mwID=0 (last retrieved June 25, 2012).

New York Police Department TIP577. http://a056-crimestoppers.nyc.gov/crimestoppers/public/index.cfm (last retrieved June 30, 2012).

NIC Suspicious Activity Reporting App. http://itunes.apple.com/us/app/suspicious-activity-reporting/id501164126?mt=8 (last retrieved June 25, 2012).

Nielsen. "State of the Media: The Social Media Report, Third Quarter." http://www.nielsen.com/ (2011) (last retrieved August 4, 2012).

Noveck, Beth. "Peer to Patent: Collective Intelligence, Open Review, and Patent Reform." *Harvard Journal of Law & Technology* 20, no. 1 (Fall 2006).

Novella, Steven. "The Role of Anecdotes in Science-Based Medicine." *Science-Based Medicine*. http://www.sciencebasedmedicine.org/index.php/the-role-of-anecdotes-in-science-based-medicine/ (January 30, 2008) (last retrieved July 19, 2012).

"Ogma Workshop: Exploring the Policy & Strategy Implications of Web 2.0 on the Practice of Homeland Security: Summary." Center for Homeland Defense and Security. www.chds.us/ (July 7, 2009).

Open Government Guide. http://www.rcfp.org/ogg/index.php (last retrieved July 3, 2011).

O'Reilly, Tim. "What is Web 2.0? Design Patterns and Business Models for the Next Generation of Software." O'Reilly Network (September 30, 2005).

Osimo, David. "Web 2.0 in Government: Why and How?" JRC Scientific and Technical Reports, European Communities (2008).

Palen, Leysia. "Online Social Media in Crisis Events." *Educause Quarterly*, no. 3 (2008).

Palmer, Jason. "Social Networks and the Web Offer a Lifeline in Haiti." BBC. http://news.bbc.co.uk/2/hi/technology/8461240.stm (January 15, 2010) (last retrieved July 16, 2012).

Peer to Patent. "Getting started." http://peertopatent.org/getting_started (last retrieved July 15, 2012).

Peterson, Marilyn. "Intelligence-Led Policing: The New Intelligence Architecture." U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, NCJ 210681 (September 2005).

Pew Research Center. "Global Digital Communication: Texting, Social Networking Popular Worldwide." Pew Global Attitudes Project. http://www.pewglobal.org/2011/12/20/global-digital-communication-texting-social-networking-popular-worldwide/ (December 20, 2011) (last retrieved April 24, 2012).

Pew Research Center. "How People Learn About Their Local Community." Project for Excellence in Journalism, Pew Internet & American Life Project, Knight Foundation (September 2011).

Program Manager, Information Sharing Environment, "Nationwide Suspicious Activity Reporting Initiative Concept of Operations." Version 1. Nationwide SAR Initiative. http://nsi.ncirc.gov/ (December 2008) (last retrieved August 17, 2012).

Qualman, Eric. *Socialnomic: How Social Media Transforms the Way We Live and Do Business*. Hoboken, NJ: John Wiley & Sons (2011).

Radian6. "Training Your Company for Social Media." Community Ebook (April 2011).

Rao, Leena, "Active Users Sending 340M Tweets Per Day." TechCrunch.com. http://techcrunch.com/2012/03/21/six-year-old-twitter-now-has-140m-active-users-sending-340m-tweets-per-day/ (March 21, 2012) (last retrieved July 14, 2012).

Ratcliffe, Jerry. "Intelligence-led Policing." Trends and Issues in Crime and Criminal Justice, no. 248, Australian Institute of Criminology, Canberra (2003).

Reporters Committee for Freedom of the Press. http://www.rcfp.org/ (last retrieved August 17, 2012).

Rettberg, Jill. *Blogging*. Cambridge: Polity Press (2009).

Rowley, Jennifer. "Using Case Studies in Research." *Management Research News* 25, no. 1 (2002).

Seawright, Jason, and John Gerring. "Case Selection Techniques in Case Study Research." *Political Research Quarterly* 61, no. 2 (June 2008).

Sierra Club. http://connect.sierraclub.org/app/render/go.aspx?g=1ed575e9-25e4-4776-9929-80fffe1cf3ca&xsl=tp_SocialObjects_ObjectType_SIERRA_CLUB_ONLINE_COMMUNITIES_PROJECT_PUBLIC.xslt&id=1ED575E9-25E4-4776-9929-80FFFE1CF3CA&cons_id=&ts=1340664426&signature=82bdd8fdbd5a3a012a0405e116290e46 (last retrieved June 25, 2012).

Silvestri v. General Motors Corp., 271 F.3d 583 (4th Cir. 2001).

Stephenson, W. David, and Eric Bonabeau. "Expecting the Unexpected: The Need for a Networked Terrorism and Disaster Response Strategy." *Homeland Security Affairs* 3, no. 1 (February 2007).

Stevens, Lauri. "Social Media in Policing: Nine Steps for Success." *Police Chief Magazine* 77, no. 2 (February 2010).

Strickland, Jonathan. "How Twitter Works." HowStuffWorks. http://computer.howstuffworks.com/internet/social-networking/networks/twitter.htm (last retrieved October 22, 2011).

Sullivan, James. "Harnessing Open Source Intelligence: Social Media and the CIA." Finding Dulcinea. http://www.findingdulcinea.com/news/Americas/2009/October/Harnessing-Open-Source-Intelligence--Social-Media-and-the-CIA.html#0 (October 21, 2009) (last retrieved April 22, 2012).

Surowiecki, James. *The Wisdom of Crowds*. New York: Anchor Books (2005).

Tilley, Nick. "Community Policing and Problem Solving." Ch. 7 in Wesley Skogan, *Community Policing (Can It Work)*. Belmont, CA: Wadsworth (2004).

Twitter Fan Wiki. http://twitter.pbworks.com/w/page/1779812/Hashtags (last retrieved July 9, 2012).

United States Bureau of Justice Assistance, Community Policing Consortium. "Understanding Community Policing, A Framework for Action." Washington, D.C.: Bureau of Justice Assistance (August 1994).

United States Congress, Joint Economic Committee, Majority Staff. "Giving a Voice to Open Source Stakeholders: A Survey of State, Local and Tribal Law Enforcement." Washington, D.C.: House of Representatives, Committee on Homeland Security (September 2008).

United States Department of Homeland Security. "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland." Washington, D.C.: United States Department of Homeland Security (February 2010).

United States Department of Homeland Security. "Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)." Version 1.5, ISE-FS-200. http://www.dhs.gov (November 17, 2010) (last retrieved August 4, 2012).

United States Department of Homeland Security, Homeland Security Council. "National Strategy for Homeland Security." http://www.dhs.gov (October 2007) (last retrieved August 4, 2012).

United States Department of Justice, "Understanding Community Policing, A Framework for Action," Office of Justice Programs, Bureau of Justice Assistance (August 1994).

United States Department of Justice, Office of Community Oriented Policing Services. "Community Policing Defined." Washington, D.C. (April 3, 2009).

United States Department of Justice, COPS Office. "Community Partnerships: A Key Ingredient in an Effective Homeland Security Approach." *Community Policing Dispatch* 1, no. 2 (February 2008).

United States Department of Justice, Global Justice Information Sharing Initiative. "Navigating Your Agency's Path to Intelligence-Led Policing." Washington, D.C. (April 2009).

United States Department of Justice, Global Justice Information Sharing Initiative. "Final Report: Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR), Evaluation Environment." Washington, D.C.: United States Department of Justice's Global Justice Information Sharing Initiative (January 2010).

United States Geological Society Website. http://earthquake.usgs.gov/research/dyfi/ (last retrieved July 15, 2012).

United States Geological Survey. http://www.usgs.gov/ (last retrieved August 4, 2012).

United States Office of Homeland Security. "National Strategy for Homeland Security." http://www.ncs.gov (July 2002) (last retrieved August 4, 2012).

Vermeulen, Mathias. "Open Source Intelligence and Social Media Monitoring." *Privacy International*. https://www.privacyinternational.org/article/bbi-open-source-intelligence-and-social-media-monitoring (November 30, 2011).

Wald, David, and James Dewey. "Did You Feel It? Citizens Contribute to Earthquake Science." U.S. Department of the Interior, U.S. Geological Survey, Fact Sheet 2005-3016 (March 2005).

Wald, David, Vincent Quitoriano, Charles Worden, Margaret Hopper, and James Dewey. "'Did You Feel It?' Internet-based Macroseismic Intensity Maps." *Annals of Geophysics* 54, no. 6 (2011).

Wasserman, Robert. "Guidance for Building Communities of Trust." U.S. Department of Justice, Office of Community Oriented Policing Services (July 2010).

West v. Goodyear Tire & Rubber Co., 167 F.3d 776 (2nd Cir. 1999).

The White House. "National Strategy for Information Sharing, Successes and Challenges In Improving Terrorism-Related Information Sharing." http://www.fas.org (October 2007) (last retrieved August 4, 2012).

Williams, E. J. "Structuring in Community Policing: Institutionalizing Innovative Change." *Police Practice and Research* 4, no. 2 (2003).

WiseGEEK. "What is Facebook?" http://www.wisegeek.com/what-is-facebook.htm (last retrieved October 22, 2011).

Woodcock, Jody. "Leveraging Social Media to Engage the Public in Homeland Security." Master's thesis, Naval Postgraduate School (September 2009).

Xu, Yili, Mora Fiedler, and Karl Flaming. "Discovering the Impact of Community Policing: The Broken Windows Thesis, Collective Efficacy, and Citizens' Judgment." *Journal of Research in Crime and Delinquency* 42 (2005).

THIS PAGE INTENTIONALLY LEFT BLANK

IACP National Law Enforcement Policy Center
SOCIAL MEDIA
Model Policy
August 2010

I. PURPOSE

The department endorses the secure use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. This policy establishes this department's position on the utility and management of social media and provides guidance on its management, administration, and oversight. This policy is not meant to address one particular form of social media, rather social media in general, as advances in technology will occur and new tools will emerge.

II. POLICY

Social media provides a new and potentially valuable means of assisting the department and its personnel in meeting community outreach, problem-solving, investigative, crime prevention, and related objectives. This policy identifies potential uses that may be explored or expanded upon as deemed reasonable by administrative and supervisory personnel. The department also recognizes the role that these tools play in the personal lives of some department personnel. The personal use of social media can have bearing on departmental personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by department personnel.

III.   DEFINITIONS

Blog: A self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments. The term is short for "Web log."

Page: The specific portion of a social media website where content is displayed, and managed by an individual or individuals with administrator rights.

Post: Content an individual shares on a social media site or the act of publishing content on a site.

Profile: Information that a user provides about himself or herself on a social networking site.

Social Media: A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

Speech: Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

Web 2.0: The second generation of the World Wide Web focused on shareable, user-generated content, rather than static web pages. Some use this term interchangeably with social media.

Wiki: Web page(s) that can be edited collaboratively.

IV. ON-THE-JOB USE

A. Department-Sanctioned Presence
1. Determine strategy
   a. Where possible, each social media page shall include an introductory statement that clearly specifies the purpose and scope of the agency's presence on the website.
   b. Where possible, the page(s) should link to the department's official website.
   c. Social media page(s) shall be designed for the target audience(s) such as youth or potential police recruits.
2. Procedures
   a. All department social media sites or pages shall be approved by the chief executive or his or her designee and shall be administered by the departmental information services section or as otherwise determined.
   b. Where possible, social media pages shall clearly indicate they are maintained by the department and shall have department contact information prominently displayed.
   c. Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies.
       (1) Content is subject to public records laws. Relevant records retention schedules apply to social media content.
       (2) Content must be managed, stored, and retrieved to comply with open records laws and e-discovery laws and policies.
   d. Where possible, social media pages should state that the opinions expressed by visitors to the page(s) do not reflect the opinions of the department.
       (1) Pages shall clearly indicate that posted comments will be monitored and that the department reserves the right to remove obscenities, off-topic comments, and personal attacks.
       (2) Pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure.
3. Department-Sanctioned Use

106

a. Department personnel representing the department via social media outlets shall do the following:
    (1) Conduct themselves at all times as representatives of the department and, accordingly, shall adhere to all department standards of conduct and observe conventionally accepted protocols and proper decorum.
    (2) Identify themselves as a member of the department.
    (3) Not make statements about the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions, nor post, transmit, or otherwise disseminate confidential information, including photographs or videos, related to department training, activities, or work-related assignments without express written permission.
    (4) Not conduct political activities or private business.
b. The use of department computers by department personnel to access social media is prohibited without authorization.
c. Department personnel use of personally owned devices to manage the department's social media activities or in the course of official duties is prohibited without express written permission.
d. Employees shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

B. Potential Uses
  1. Social media is a valuable investigative tool when seeking evidence or information about
     a. missing persons;
     b. wanted persons;
     c. gang participation;
     d. crimes perpetrated online (i.e., cyberbullying, cyberstalking); and
     e. photos or videos of a crime posted by a participant or observer.
  2. Social media can be used for community outreach and engagement by
     a. providing crime prevention tips;
     b. offering online-reporting opportunities;
     c. sharing crime maps and data; and
     d. soliciting tips about unsolved crimes (i.e., Crimestoppers, text-a-tip).
  3. Social media can be used to make time-sensitive notifications related to
     a. road closures,
     b. special events,
     c. weather emergencies, and
     d. missing or endangered persons.
  4. Persons seeking employment and volunteer positions use the Internet to search for opportunities, and social media can be a valuable recruitment mechanism.

5. This department has an obligation to include Internet-based content when conducting background investigations of job candidates.
6. Searches should be conducted by a nondecision maker. Information pertaining to protected classes shall be filtered out prior to sharing any information found online with decision makers.
7. Persons authorized to search Internet-based content should be deemed as holding a sensitive position.
8. Search methods shall not involve techniques that are a violation of existing law.
9. Vetting techniques shall be applied uniformly to all candidates.
10. Every effort must be made to validate Internet-based information considered during the hiring process.

II. PERSONAL USE
A. Precautions and Prohibitions
Barring state law or binding employment contracts to the contrary, department personnel shall abide by the following when using social media.
1. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of this department for which loyalty and confidentiality are important, impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the department.
2. As public employees, department personnel are cautioned that speech on- or off-duty, made pursuant to their official duties—that is, that owes its existence to the employee's professional duties and responsibilities—is not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the department. Department personnel should assume that their speech and related activity on social media sites will reflect upon their office and this department.
3. Department personnel shall not post, transmit, or otherwise disseminate any information to which they have access as a result of their employment without written permission from the chief executive or his or her designee.
4. For safety and security reasons, department personnel are cautioned not to disclose their employment with this department nor shall they post information pertaining to any other member of the department without their permission. As such, department personnel are cautioned not to do the following:
   a. Display department logos, uniforms, or similar identifying items on personal web pages.
   b. Post personal photographs or provide similar means of personal recognition that may cause them to be identified as a police officer of this department. Officers who are, or who may reasonably be expected to work in undercover operations, shall not post any form of visual or personal identification.

5. When using social media, department personnel should be mindful that their speech becomes part of the worldwide electronic domain. Therefore, adherence to the department's code of conduct is required in the personal use of social media. In particular, department personnel are prohibited from the following:
    a. Speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.
    b. Speech involving themselves or other department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.
6. Engaging in prohibited speech noted herein, may provide grounds for undermining or impeaching an officer's testimony in criminal proceedings. Department personnel thus sanctioned are subject to discipline up to and including termination of office.
7. Department personnel may not divulge information gained by reason of their authority; make any statements, speeches, appearances, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this department without express authorization.
8. Department personnel should be aware that they may be subject to civil litigation for
    a. publishing or posting false information that harms the reputation of another person, group, or organization (defamation);
    b. publishing or posting private facts and personal information about someone without their permission that has not been previously revealed to the public, is not of legitimate public concern, and would be offensive to a reasonable person;
    c. using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose; or
    d. publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.
9. Department personnel should be aware that privacy settings and social media sites are constantly in flux, and they should never assume that personal information posted on such sites is protected.
10. Department personnel should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the department at any time without prior notice.
11. Reporting violations—Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provision of this policy shall notify his or her supervisor immediately for follow-up action.

Acknowledgment

This *Model Policy* was developed by the IACP Center for Social Media in conjunction with the IACP National Law Enforcement Policy Center. We are appreciative of the many police agencies across the country who shared their existing policies.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.

APPENDIX B.   CRIME STOPPERS TIP FORM

Crime Stoppers | Tip Form

**Fill out as much information as possible and click "Submit Tip" below.
Please be sure to include all information that you know regarding the suspect.
For instance, in addition to a name, we need to know where to find this person.**

Last Name:

First name:

Middle:

Alias(es):

Race:

Sex:

\---

Ht-Feet:

\---

Ht-Inches:

\---

Weight (pounds):

Age:

Eye Description:

Hair Description:

Address of suspect:

City:

State:

Zip code:

Country:

Scars, Marks, Tattoos:

Suspect's Clothing:

Type of animals owned:

Weapons:

Hangouts:

Known Associates:

Gang Affiliation:

Name of suspect's employer:

Address of Employer:

Employer City:

Employer State:

Employer Zip code:

Employer Country:

V E H I C L E   I N F O R M A T I O N

Make:

Model:

Color:

Year:

License:

State:

Other Vehicle Notes:

C R I M E N O T E S

Type of Offense:

Warrant Number: (if known):

Offense City:

Case Number: (if known):

Where did you last see this suspect? :

Victim's Information:

Crime Description (Including - Who, What, When, Where and Why?):

Please limit to 1000 characters. You have `1000` characters remaining

Is this additional information on an existing tip?:

● No: ● Yes, my previous report number was (tipId):

P I C T U R E U P L O A D

Hit 'Browse' to select a GIF, PNG, JPG or Video files to send with this tip:

⚠ **For security purposes we recommend that you DO NOT print this tip submission form or save it to your computer. Be sure that you did not give your name above.**

Contact Information

Please enter the code shown below:

This helps the NYPD prevent automated input:

Click here to refresh image if image is not clear

Submit Tip

APPENDIX C.   SUSPICIOUS ACTIVITY REPORTING

Suspicious Activity Reporting
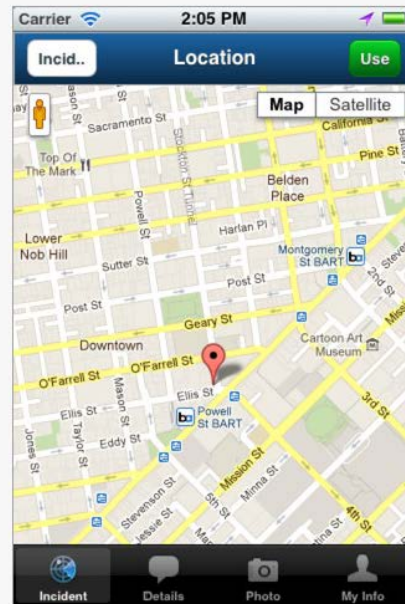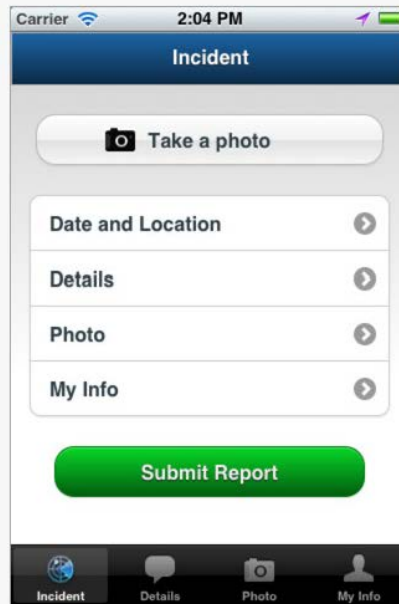
View More By This Developer

Description

The Suspicious Activity Reporting mobile application enables citizens to document people, vehicles, and a location related to suspicious activity and submit the report to multiple West Virginia and Federal law enforcement agencies instantly. Until now, the Suspicious Activity Report could only be submitted by completing and faxing a paper form or completing a web form on the WV Fusion Center Website.
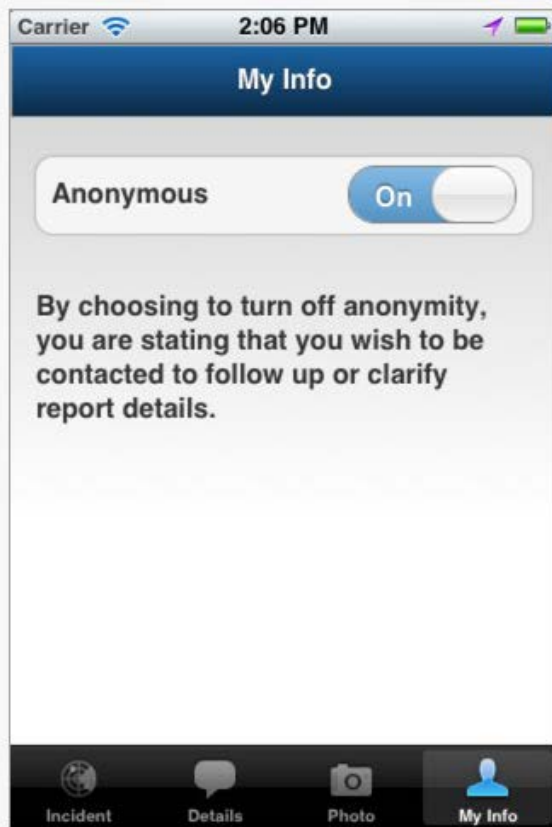
The free application gives citizens the ability to:

- Capture a photo from the app or use one that already exists on the device
- Automatically find and use the phone's location or enter an address
- Report detailed subject and vehicle descriptions
- Remain anonymous if preferred, or include contact information

*NOTE – This application is not intended for emergency purposes. Please dial 911 or your local police department in the event of an emergency.

View In iTunes

Free

Requirements: Compatible with iPhone, iPod touch, and iPad.Requires iOS 4.3 or later.

Customer Ratings

We have not received enough ratings to display an average for the current version of this application.

All Versions:
★★⯪ 9 Ratings

More iPhone Apps by NICUSA

USA Live
View In iTunes ▶

Most Wanted
View In iTunes ▶

iPhone Screenshots

115

iPhone Screenshots

APPENDIX D. CASE STUDY COMPARISON MATRIX

	Peer to Patent	Did You Feel It?	Social Media & Haiti Earthquake
Targeted Social Media Message Senders	Self-selected citizen experts	All citizens who experience an earthquake	All earthquake victims
What Information Can be Sent	Prior art (related patents and published articles)	Pre-formatted checkboxes and dropdown values	Text, photographs
Efforts to Court Participation	Messages through community leaders News postings on USPTO and P2P websites	Decades old tool Used by some educators to explain earthquake intensity	Use of traditional media (radio) SMS (text) messages from cellphone carrier
Education About Using the Tool	Step-by-step written explanation Videos Visual depiction	Printed Fact Sheet Online FAQs	None
Encouragement to Participants	News postings on USPTO and P2P websites Symbols to recognize valuable contributors "Most Active Teams" tab on P2P website	Printed Fact Sheet Online FAQs explain the merits	Self-interest Altruism
Usefulness of Received Information (Low, Medium, High)	High (based on data analysis)	High (based on data analysis)	High (based on anecdotal evidence)
Handling Erroneous Information	Unknown	Filters to remove and flag	None
Metric to Measure Success	Defined hypothesis before project began Data from P2P software Surveys	Defined hypothesis before project began Data from DYFI software	None

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1.   Defense Technical Information Center
      Ft. Belvoir, Virginia

2.   Dudley Knox Library
      Naval Postgraduate School
      Monterey, California

3.   David Brannan
      Naval Postgraduate School
      Monterey, California

4.   Patrick Miller
      Naval Postgraduate School
      Monterey, California

5.   Constantine Miniotis
      Chicago Police Department
      Chicago, Illinois