NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

HOMELAND SECURITY: THERE'S AN APP FOR THAT

by

Christopher Michael DeMaise

March 2017

Thesis Advisor: Rodrigo Nieto-Gomez
Second Reader: David O'Keeffe

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE HOMELAND SECURITY: THERE'S AN APP FOR THAT	**5. FUNDING NUMBERS**
6. AUTHOR(S) Christopher Michael DeMaise	
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 number N/A.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Situational awareness is essential for first responders to critical incidents. Failure to achieve effective awareness of an event can impede decision making and result in drastic consequences. Limitations on the agility and interoperability of proprietary technology and current communications devices prevent effective situational awareness from being achieved and shared. Off-the-shelf mobile applications provide a unique opportunity for this objective to be accomplished. The universal acceptance of mobile technology and free or low-cost mobile applications can be used to enhance situational awareness during critical incidents and even enable sharing ad hoc at the event. While the adoption of this technology presents many cost-effective opportunities to its users, it also presents many challenges related to its adoption. Agencies must be made aware of the logistical, cultural, and policy challenges related to off-the-shelf mobile application adoption and address these issues early in order to effectively employ these technologies during critical incidents.

14. SUBJECT TERMS homeland security, situational awareness, off-the-shelf mobile applications, COTS mobile applications, mobile technology acceptance, interoperability, interdisciplinary information sharing, mobile application policy, NYPD Mobility Initiative, mobile devices	**15. NUMBER OF PAGES** 129
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

HOMELAND SECURITY: THERE'S AN APP FOR THAT

Christopher Michael DeMaise
Lieutenant, New Jersey State Police
B.A., Rowan University, 1997
M.A., Seton Hall University, 2003

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
March 2017**

Approved by: Rodrigo Nieto-Gomez, Ph.D.
Thesis Advisor

David O'Keeffe
Second Reader

Erik Dahl, Ph.D.
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Situational awareness is essential for first responders to critical incidents. Failure to achieve effective awareness of an event can impede decision making and result in drastic consequences. Limitations on the agility and interoperability of proprietary technology and current communications devices prevent effective situational awareness from being achieved and shared. Off-the-shelf mobile applications provide a unique opportunity for this objective to be accomplished. The universal acceptance of mobile technology and free or low-cost mobile applications can be used to enhance situational awareness during critical incidents and even enable sharing ad hoc at the event. While the adoption of this technology presents many cost-effective opportunities to its users, it also presents many challenges related to its adoption. Agencies must be made aware of the logistical, cultural, and policy challenges related to off-the-shelf mobile application adoption and address these issues early in order to effectively employ these technologies during critical incidents.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials
ASD	Australian Signals Directorate
BYOD	bring your own device
CHDS	Center for Homeland Defense and Security
DAS	Domain Awareness System
DHS	Department of Homeland Security
EOC	emergency operation center
FDNY	Fire Department of New York City
FedRAMP	Federal Risk and Authorization Management Program
FTC	Federal Trade Commission
GPS	Global Positioning System
IS	information system
IT	information technology
LMR	land mobile radio
LTE	Long Term Evolution
MIM	mobile instant messaging
NCCIC	National Cybersecurity and Communications Integration Center
NG911	Next Generation 9-1-1
NIST	National Institute of Standards and Technology
NYPD	New York City Police Department
OS	operating system
PEnE	policy enforcement engine
PRA	Paperwork Reduction Act
SA	situational awareness
SOA	service-oriented architecture
SMS	Short Message Service
TAM	technology acceptance model
VSMWG	Virtual Social Media Working Group
WTC	World Trade Center

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Mobile technology and software applications are assuming an increasing role in homeland security operations. First responders are using these technologies more frequently to collaborate with each other and alert the public during critical incidents.[1] Agencies that are able to procure proprietary mobile technologies have used these systems to improve operations, but these systems typically do not enable collaboration with outside agencies. Further, 62 percent of public service agencies report they cannot afford proprietary mobile solutions.[2] Marc Goodman of the Future Policing Institute suggests that to combat terrorism, advanced technologies cannot be available to only a select few.[3] Fortunately, off-the-shelf mobile application technologies offer a variety of alternative solutions and, in some cases, are free. This thesis examines the viable alternative offered by off-the-shelf mobile applications for enhancing situational awareness for collaborative homeland security operations.

Off-the-shelf mobile technology and applications are developed daily to meet the personal and professional needs of mobile-device users. A recent survey indicates that 68 percent of American adults possess smartphones, and more than 77 percent have downloaded applications to their devices.[4] Off-the-shelf mobile applications were used by local law enforcement to resolve communication issues during a recent terrorist attack in Belgium. After suicide bombings at the country's train station and airport, mobile and terrestrial radio networks began to fail.[5] The Belgian officers were using the mobile

---

[1] M. Jae Moon, "From Egovernment to Mgovernment," IBM Center for the Business of Government, November 2004, http://www.uquebec.ca/observgo/fichiers/28540_mgovernment.pdf.

[2] Governing, *Mobile Strategy Survey: Where Are You on the Roadmap from Apps to Enterprise Management?* Washington, DC: e.Republic, 2013. https://www.business.att.com/content/whitepaper/Creating-a-Mobility-Strategy-Survey-Results.pdf.

[3] Marc Goodman, "How Technology Makes us Vulnerable," CNN, July 29, 2012, http://www.cnn.com/2012/07/29/opinion/goodman-ted-crime/index.html.

[4] Kenneth Holmstead and Michelle Atkinson, "The Majority of Smartphone Users Download Apps," Pew Research Center, November 10, 2015, http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/.

[5] "Brussels Police Were Forced to Use WhatsApp during Attack," BNO News, March 26, 2016, http://bnonews.com/news/index.php/news/id3969.

application WhatsApp, through local WiFi hotspots, to share information. While much has been written regarding social media as a tool to communicate with the public during critical incidents, this example identifies that mobile applications can be used by public safety professionals to communicate securely.[6]

Implementation and sustainment challenges may develop for agencies that attempt to adopt such technologies. Policy gaps exist in information security and retention through off-the-shelf mobile applications that are cloud hosted. Applications such as Slack's free version only retain the last 10,000 messages. Data retention requirements of agencies will need to be considered for homeland security agencies that adopt these platforms. Additionally, there is always the potential that a homeland security practitioner will use the application for personal functions, commingling personal and duty-related information.

Currently, there is limited policy uniformity for the procurement and use of off-the-shelf mobile applications by homeland security agencies. There are several draft policies being developed for the federal government, but state and local governments do not have uniform regulations or guidance to safely take advantage of these emerging technologies. The homeland security community would benefit from a thorough examination of off-the-shelf mobile technologies for situational awareness needs. This research presents an analysis of the technology adoption concerns for federal, state, local, and tribal agencies that seek to use these mobile solutions. An examination of how these systems will integrate into homeland security operations is also conducted. The research provides an academic review of technology adoption theories as well as case studies showing how similar mobile technology platforms were integrated.

Any agency seeking to use off-the-shelf mobile applications for situational awareness should consider these recommendations. There are numerous benefits to adopting these technologies to increase the interoperability and coordination between the various disciplines of homeland security. The costs of not adopting mobile applications

---

[6] "Apps, The Basics," IACP Center for Social Media, accessed November 30, 2016, http://www.iacpsocialmedia.org/Technologies/Parent/Platform.aspx?termid=155&depth=3.

for situational awareness are diminished inter-agency coordination and compromises in first responder safety. This thesis offers the pros and cons of off-the-shelf mobile applications to inform the reader. A hypothetical scenario is offered to present the potential of off-the-shelf mobile applications for homeland security situational awareness needs. The recommendations provided are consistent with federal guidelines for application security and identify how homeland security can embrace these technologies for current and future needs.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

It has been a tremendous honor to participate in the CHDS program. The Naval Postgraduate School is a life-changing experience and one that has made me a more aware homeland security practitioner. The academic rigor required by the program has led to a great deal of sacrifice on the part of my personal and professional life. While there are too many individuals to thank for my growth as a result of this experience, there are a few that really stood out.

First and foremost, I must express my appreciation to the New Jersey State Police, civilian and enlisted, that have supported me throughout the experience. LTC Ponenti believed enough in me to spark my interest, and LTC Chris Schulz (ret.), LTC Ray Guidetti, Lt. Tim Coyle, and Ray Bisogno et al. kept me going throughout. Your sage advice and words of encouragement were truly appreciated, and I can only hope to encourage the next NJSP participant half as much. I would also like to extend my sincere gratitude to the NJSP staff who supported my participation. NJSP superintendent Colonel Joseph R. Fuentes and many others provided the organizational support to accomplish this task. Your faith in my abilities to represent "the outfit" is humbling and something I will never forget.

The staff of the CHDS program and my classmates made this experience more enriching than I could have imagined. Instructors such as Chris Bellavita and Richard Bergin were always available to support my academic needs or run ideas by. My thesis committee members, Dr. Rodrigo Nieto-Gomez and David O'Keeffe, were a remarkable sounding board, and they have driven me to work hard and extensively research an evolving topic. Noel Yucuis, of the Graduate Writing Center, was an invaluable resource and is directly responsible for my growth as a writer. The 1505/1506 Cohort is a remarkably close group, and I will cherish your friendship. The spirited debates and late-night dialogue contributed immensely to the learning environment, but more importantly, it has forged bonds that will last a lifetime.

Last, but certainly not least, it is with great appreciation for the sacrifices of my family that I present this thesis. My wife, Chrissy, and our three children, Tyler, Emma, and Layla, had to endure my countless hours writing in the attic and at the library. To my children: I often express to you the importance of education if you are going to make a difference in the world. I can only hope that you one day find an environment as special as the Naval Postgraduate School to build relationships while learning from, and with, the most respected people of your profession.

I. INTRODUCTION

To examine the potential of off-the-shelf mobile applications on the homeland security enterprise, this thesis addresses the following question: How can homeland security agencies adopt off-the-shelf mobile applications to support situational awareness needs?

A. PROBLEM STATEMENT

Mobile technology and software applications are assuming an increasing role in homeland security operations. First responders are using these technologies more frequently to collaborate with each other and alert the public during critical incidents.[1] Mobile devices and software have been used to improve situational awareness and collaboration of response efforts at events dating back to Hurricane Katrina in 2005.[2] Unfortunately, this is more the exception than the norm. Agencies that are able to procure proprietary mobile technologies have used these systems to improve operations, but typically do not enable collaboration with outside agencies. Further, 62 percent of public service agencies report they cannot afford proprietary mobile solutions.[3] This thesis examines the viable alternative offered by off-the-shelf mobile technology for enhancing situational awareness for collaborative homeland security operations.

The public perception that homeland security agencies possess the technologies shown on television is largely false. In fact, many public safety agencies have trouble procuring and implementing technologies due to fiscal, cultural, or regulatory

[1] M. Jae Moon, "From Egovernment to Mgovernment," IBM Center for the Business of Government, November 2004, http://www.uquebec.ca/observgo/fichiers/28540_mgovernment.pdf.

[2] Shelly Farnham, E. Pedersen, and Robert Kirkpatrick, "Observation of Katrina/Rita Groove Deployment: Addressing Social and Communication Challenges of Ephemeral Groups," *Proceedings of the 3rd International ISCRAM Conference* (2006), 41.

[3] Governing, *Mobile Strategy Survey: Where Are You on the Roadmap from Apps to Enterprise Management?* (Washington, DC: e.Republic, 2013), https://www.business.att.com/content/whitepaper/Creating-a-Mobility-Strategy-Survey-Results.pdf.

constraints.[4] This is unfortunate because research has shown public safety agencies that utilize technological support for enterprise operations are more successful in combating crime.[5] However, most agencies do not have the funding to support such measures. Marc Goodman of the Future Policing Institute suggests that to combat terrorism, advanced technologies cannot be available to only a select few.[6] Fortunately, off-the-shelf technologies offer a variety of alternative solutions and, in some cases, can be free.

Mobile technology and software applications are rapidly integrating into the daily lives of U.S. citizens. Mobile computing use has recently surpassed desktop computing, with over two billion users worldwide.[7] The public demand for agile mobile networks and applications has driven the industry to meet consumer demands for portable solutions. Smartphones have replaced daily-use items ranging from cameras to credit cards. Evolving applications for this technology also diminish the need for personal identification cards, television remote controls, and keys to residences and automobiles.[8] As this technology has proliferated, the corporate world has taken notice. Mobile technology developers have offered many enterprise solutions to meet the demands of the employee on the move.

The rapid growth of mobile technology, omnipresent Internet accessibility, and an increasingly technologically aware generation have encouraged the private sector to adopt mobile solutions. These agencies are relying more on mobile devices and networks to support critical business operations than on employees typing away at desktop computers in office buildings. Research indicates that 76 percent of private sector organizations feel that mobile devices and/or applications have enhanced the speed of

---

[4] Community Oriented Policy Services, "The Impact of the Economic Downturn on American Police Agencies," Department of Justice, accessed May 20, 2016, http://www.cops.usdoj.gov/Default.asp?Item=2602.

[5] Ger Daly, "Embracing the Police Force of the Future," CNN, September 19, 2013, http://www.cnn.com/2013/09/18/tech/innovation/police-future-technology/.

[6] Marc Goodman, "How Technology Makes us Vulnerable," CNN, July 29, 2012, http://www.cnn.com/2012/07/29/opinion/goodman-ted-crime/index.html.

[7] Dave Chaffey, "Mobile Marketing Statistics Compilation," Smart Insights, accessed March 25, 2016, http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/.

[8] Jon Evans, "When Will Your Phone Replace Your Keys and Wallet?" *Tech Crunch*, December 27, 2014, http://techcrunch.com/2014/12/27/when-will-your-phone-replace-your-keys-and-wallet/.

decision making and employee responsiveness.[9] Mobile technology and applications may also replace the traditional tools that enhance decision making for the homeland security enterprise. The chart in Figure 1 shows further benefits increased use of mobile technology can bring to the workplace.

Figure 1. Key Mobility Benefits[10]

The continued evolution of smartphone technology could lead to a large-scale technological transition for homeland security operations. Conventional terrestrial radio systems, in which the government has made substantial investments, do not meet the situational awareness needs of the public safety community. In 2016, for example, more than 400 New Jersey State Police officers were providing security for a high-risk event at MetLife stadium in East Rutherford, New Jersey. During the event, a stabbing took place

[9] Forrester Research, "The Expanding Role of Mobility in the Workplace," Cisco, February 2012, 7, https://www.cisco.com/c/dam/en_us/solutions/trends/unified_workspace/docs/Expanding_Role_of_Mobility_in_the_Workplace.pdf.

[10] Source: Ibid., 7.

in the parking area, and the suspect fled the scene. A quick-thinking trooper responded to the scene and used his personal smartphone to obtain a photo of the suspect from a witness. The image was transmitted via the trooper's mobile Short Message Service (SMS) system to his five squad-mates, but not to the 400 other troopers or security workers working the event. Fortunately, due to the use of the smartphone's messaging system, the suspect was apprehended prior to leaving via mass transit.[11] This event draws attention to the situational awareness and technological needs of public safety personnel. Had the troopers collectively employed an existing crowdsourcing tool such as WhatsApp, the information would have been transmitted to hundreds of first responders at the event, fully encrypted, at no cost.

The New York City Police Department (NYPD) implemented its Mobility Initiative in 2014 to meet the situational awareness and technological needs of the largest police department in the United States. Through the program, the agency issued more than 36,000 smartphones and tablets to members of the department. The devices allow personnel to track events and communicate via the city's proprietary Domain Awareness System (DAS). According to Michael Bloomberg's office, DAS, a collaboration between Microsoft and the NYPD, "aggregates and analyzes existing public safety data in real time to provide a comprehensive view of potential threats and criminal activity."[12] The system was originally designed to provide the department's command center with real-time situational awareness. It has evolved into an interactive network of situational awareness between the edge user, or "cop on the beat," central command, and the network of devices integrated into the environment. The Mobility Initiative and DAS in New York City serve as an excellent case study to examine the application of proprietary mobile technology. However, most agencies do not have a budget like the NYPD's to develop such programs. Further, there is a lack of interoperability between the NYPD's proprietary technology with other first responders such as the Fire Department of New

[11] Information provided is based on the author's personal experience at the event.

[12] City of New York, "Press Release from the Office of Mayor Bloomberg" (PR-291-12), August 8, 2012, http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2012b%2Fpr291-12.html&cc=unused1978&rc=1194&ndi=1.

York City (FDNY) or law enforcement partners. Therefore, further examination of off-the-shelf technology options that can be used by all first responders is warranted.

Off-the-shelf mobile technology and applications are developed daily to meet the personal and professional needs of mobile-device users. A recent survey indicates that 68 percent of American adults possess smartphones, and more than 77 percent have downloaded applications to their devices.[13] Most downloaded mobile applications are for personal use; however, there is a growing trend of users adopting mobile enterprise applications.[14] These advantages include cross-platform utility, low upfront cost, and improved customer service.[15] The "open-ended" nature of these programs allows the applications to be updated and supported by the developers, as needed, to secure vulnerabilities.[16] Reputable mobile application developers are constantly evaluating and updating their products to ensure they meet consumer expectations and security needs.[17]

There are many emerging federal government programs that are embracing a large-scale migration to mobile technology platforms for the homeland security enterprise. FirstNet is a cellular infrastructure program that will prioritize service to mobile devices of homeland security practitioners. The goal of this program is to ensure that first responder technology works at the most critical times.[18] San Jose Police Chief Chris Moore touts the importance of this program to homeland security:

> The network will be integral to how policing is done in this country over the next 40–50 years. It's pretty clear that resources for local and state law enforcement have diminished. It's imperative that police become more

---

[13] Kenneth Holmstead and Michelle Atkinson, "The Majority of Smartphone Users Download Apps," Pew Research Center, November 10, 2015, http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/.

[14] Sanjeev Narayan Bal, "Mobile Web—Enterprise Application Advantages," *International Journal of Computer Science and Mobile Computing* 2, no. 2 (February 2013): 36, http://www.academia.edu/2580454/Mobile_Web_Enterprise_Application_Advantages.

[15] Ibid., 40.

[16] Jeffrey Voas et al., *Technical Considerations for Vetting 3rd Party Mobile Applications (Draft)* (NIST SP 800–163) (Washington, DC: U.S. Department of Commerce, August 2014), 5, http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf.

[17] Ken Yarmosh, "How Often You Should Update Your Apps," *Savvyapp*, January 12, 2016, http://savvyapps.com/blog/how-often-should-you-update-your-app.

[18] "FirstNet RFP," accessed March 25, 2016, http://www.firstnet.gov.

> efficient, and technology will allow this. We have to find ways to leverage this network to help us solve crimes more quickly and efficiently. With this broadband capability, we will be able to securely and reliably use applications that we can't even anticipate yet.[19]

Next Generation 9-1-1 (NG911) is another emerging program designed to meet the future demands of homeland security. NG911 will have the ability to support the dispatch needs of the increasingly mobile-dependent citizenry.[20] This system will allow text messages, photographs, and videos to be imported to operational dispatch centers and exported to first responder mobile device applications while they are in the field.[21] While proprietary mobile applications have not been identified for first responder mobile devices yet, off-the-shelf mobile applications may be a cost-effective tool to facilitate the situational awareness needs of first responders and dispatch centers.

Off-the-shelf mobile applications were used by local law enforcement to resolve communication issues during a recent terrorist attack in Belgium. After suicide bombings at the country's train station and airport, mobile and terrestrial radio networks began to fail. One officer deployed to the event attested, "It was a helpless situation. Orders were not received and no one knew what was being done. The mobile network was down too. Fortunately, WhatsApp was still working. Without the app we wouldn't have been able to communicate at all."[22] The Belgian officers were using the mobile application through local Wi-Fi hotspots to share information. While much has been written regarding social media as a tool to communicate with the public during critical incidents, this example identifies that mobile applications can be used by public safety professionals to communicate securely.[23]

---

[19] Ibid.

[20] "Next Generation 911 (NG911)," 911.gov, accessed March 25, 2016, http://www.911.gov/911-issues/standards.html.

[21] Federal Communications Commission (FCC), *A Next Generation 9-1-1 Cost Study: A Basis for Public Funding Essential to Bringing a Nationwide Next Generation 911 Network to America's Communications Users and First Responders* (Washington, DC: FCC, September 2011), https://apps.fcc.gov/edocs_public/attachmatch/DOC-309744A1.pdf.

[22] "Brussels Police Were Forced to Use WhatsApp during Attack," BNO News, March 26, 2016, http://bnonews.com/news/index.php/news/id3969.

[23] "Apps, The Basics," IACP Center for Social Media, accessed November 30, 2016, http://www.iacpsocialmedia.org/Technologies/Parent/Platform.aspx?termid=155&depth=3.

Implementation and sustainment challenges may develop for agencies that attempt to adopt such technologies. Policy gaps exist in information security and retention through off-the-shelf mobile applications that are cloud hosted. Applications such as Slack's free version only retain the last 10,000 messages. Agencies' data retention requirements will need to be considered for homeland security agencies that adopt these platforms. Additionally, there is always the potential that a homeland security practitioner will use the application for personal functions, commingling personal and duty-related information.

While examining the adoption of off-the-shelf mobile applications, stakeholders may have valid concerns related to security and service. Some information technology (IT) specialists have argued that firewall-protected internal servers of proprietary systems provide more security.[24] Further, certain off-the-shelf applications can be rushed to market or app stores to capitalize on evolving consumer interests.[25] Agencies that adopt off-the-shelf applications may not be able to persuade the application developers to change their security measures to meet one agency's needs. Also, if the initial terms and conditions are altered for the off-the-shelf mobile application, the user is not in a position to renegotiate. This can be problematic if the off-the-shelf application becomes an essential element of operations and interfaces with other job-related functions.

Off-the-shelf applications may present privacy concerns as well. Even though mobile applications are offered for free or at a low cost, often the fine print on the terms of acceptance acknowledges the developer's access to the user's information. The developer can sell this information to marketing or advertising agencies.[26] Therefore, potential privacy issues may result if a user's contact list or agency data are accessed. This is a significant concern for homeland security practitioners who maintain confidential sources and other sensitive personally identifiable information on the device using the application.

---

[24] John Dix, "Security: On Premise or In the Cloud," Network World, November 5, 2012, http://www.networkworld.com/article/2223442/tech-debates/security--on-premise-or-in-the-cloud-.html.

[25] Voas et al., *Technical Considerations*, 5.

[26] Ibid.

Currently, there is limited policy uniformity for the procurement and use of off-the-shelf mobile applications by homeland security agencies. The federal government initiated apps.gov in 2009 to develop an approval program for cloud-based services that enable cost-effective and flexible IT procurement.[27] However, the initial program was fraught with problems and described by some as not agile enough to keep up with private sector application vetting programs.[28] The recent release of apps.gov 2.0 allows government IT procurement specialists to examine software products that have been vetted by government security standards. The site also provides contractual stipulations and templates to be filled in by the agency that wishes to establish a relationship with the application provider.[29] While apps.com provides an open-source standard for government agencies to vet application security, it does not provide a portal for government agencies to submit requests, nor does it provide policy recommendations for use of mobile application technology.

The federal government enacted the Paperwork Reduction Act (PRA) in 1980 to encourage the use of technology to reduce the paperwork burden upon citizens and the private sector.[30] In 2010 the White House put forth guidance (44 U.S.C. § 3501) that modified the PRA to encourage its agencies to employ information system technology:

> When sponsoring an information collection online, or in any other form or format, agencies must comply with the PRA's requirement to maximize the utility of information collected, maintained, used, shared, and disseminated while minimizing the burden imposed on the public.[31]

---

[27] John Trobough, Smita Satiana, and Andrew Stroup, "The Rebirth of the Obama Administration's apps.gov," *Tech Crunch*, March 14, 2016, https://techcrunch.com/2016/03/14/the-rebirth-of-the-obama-administrations-apps-gov/.

[28] Ibid.

[29] "Products," Apps.gov, accessed October 22, 2016, https://apps.gov/products.

[30] *Paperwork Reduction Act*, 44 U.S.C. § 3501 *et seq*., (1980), see https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1289.

[31] Cass R. Sunstein, "Memorandum for the Heads of Executive Departments and Agencies and Independent Regulatory Agencies," White House, April 10, 2010, 2, https://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf.

The federal government (in 44 U.S.C. § 3506) acknowledges the utility of advanced technology and recognizes the complications presented by data created through these systems:

> Regardless of whether a particular activity is a collection of information under the PRA, agencies have an obligation to manage information resources to "improve the integrity, quality and utility of information to all users within and outside the agency." With social media and web-based interactive technologies, agencies should be aware that their activities may create new Federal information that will need to be managed like other agency information resources. For example, some uses of social media may present novel records management issues.[32]

Policies such as these were developed to engage technology such as desktop computing and the Internet. However, there is a gap in policy for mobile-device management that government agencies are struggling to catch up to.[33] There are several draft policies being developed for the federal government, but state and local governments do not have uniform regulations or guidance to safely take advantage of these emerging technologies. This gap is addressed through this thesis.

The homeland security community would benefit from a thorough examination of off-the-shelf mobile technologies for situational awareness needs. This research presents an analysis of the technology adoption concerns for federal, state, local, and tribal agencies that seek to use these mobile solutions. An examination of how these systems will integrate into homeland security operations is also conducted. The primary audience for this research is the homeland security practitioners who are responsible for developing technology adoption strategies for situational awareness. The research provides an academic review of technology adoption theories as well as case studies showing how similar mobile technology platforms were integrated.

---

[32] Ibid., 3.

[33] Henry Kenyon, "Why Federal Agencies Lag behind in Mobile Technology," *Information Week*, August 26, 2014, http://www.informationweek.com/government/mobile-and-wireless/why-federal-agencies-lag-behind-on-mobile-tech/d/d-id/1306625?itc=edit_in_body_cross.

B. LITERATURE REVIEW

The homeland security threat environment of the United States is constantly evolving. Dynamic weather events, civil unrest, and violent extremism present a number of complex challenges to agencies tasked with preventing, responding to, and mitigating these events. To tackle these issues, homeland security agencies are turning to mobile technology solutions to facilitate their situational awareness needs. However, proprietary mobile applications can be cost prohibitive and inhibit the ability of diverse first responder groups to share information. The proliferation of off-the-shelf mobile technology and software applications (apps) presents many opportunities to aid first responders in achieving situational awareness when deployed to these events. An examination of academic theory and previous case studies identifies some of the challenges and opportunities this technology brings. This literature review examines the costs and benefits of off-the-shelf mobile applications to support the situational awareness needs of homeland security.

1. Why Is Situational Awareness Important?

Simply put, situational awareness (SA) is the state of knowing what is going on in the surrounding area. The knowledge of one's operating environment in the context of the moment is essential for good decision making during times of crisis. The military has identified that, during these critical moments, command and control are only successful if the assets in the operational theater have current situational awareness.[34] Effective incident command of homeland security operations is also dependent upon this awareness. Mica Endsley's research expands on the utility of SA for decision making in complex environments. Endsley breaks SA theory into three phases: perception, comprehension, and projection.[35] Each level is dependent on the previous one and identifies how decision-makers process information (see Figure 2). *Perception* is the individual's ability to identify the crisis situation. During the *comprehension* phase, the individual takes this perception and identifies how the environment impacts the event.

[34] Ibid., 1.

[35] Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37, no. 1 (March 1995): 35.

These environmental considerations include weather, terrain, and population. The individual then uses *projection* to predict the outcome of various responses to the event, prior to executing a decision.[36] Without effective SA, Endsley proposes, the perception of the problem can adversely impact the subsequent stages of the process and lead to poor decisions.

[36] Ibid., 35.

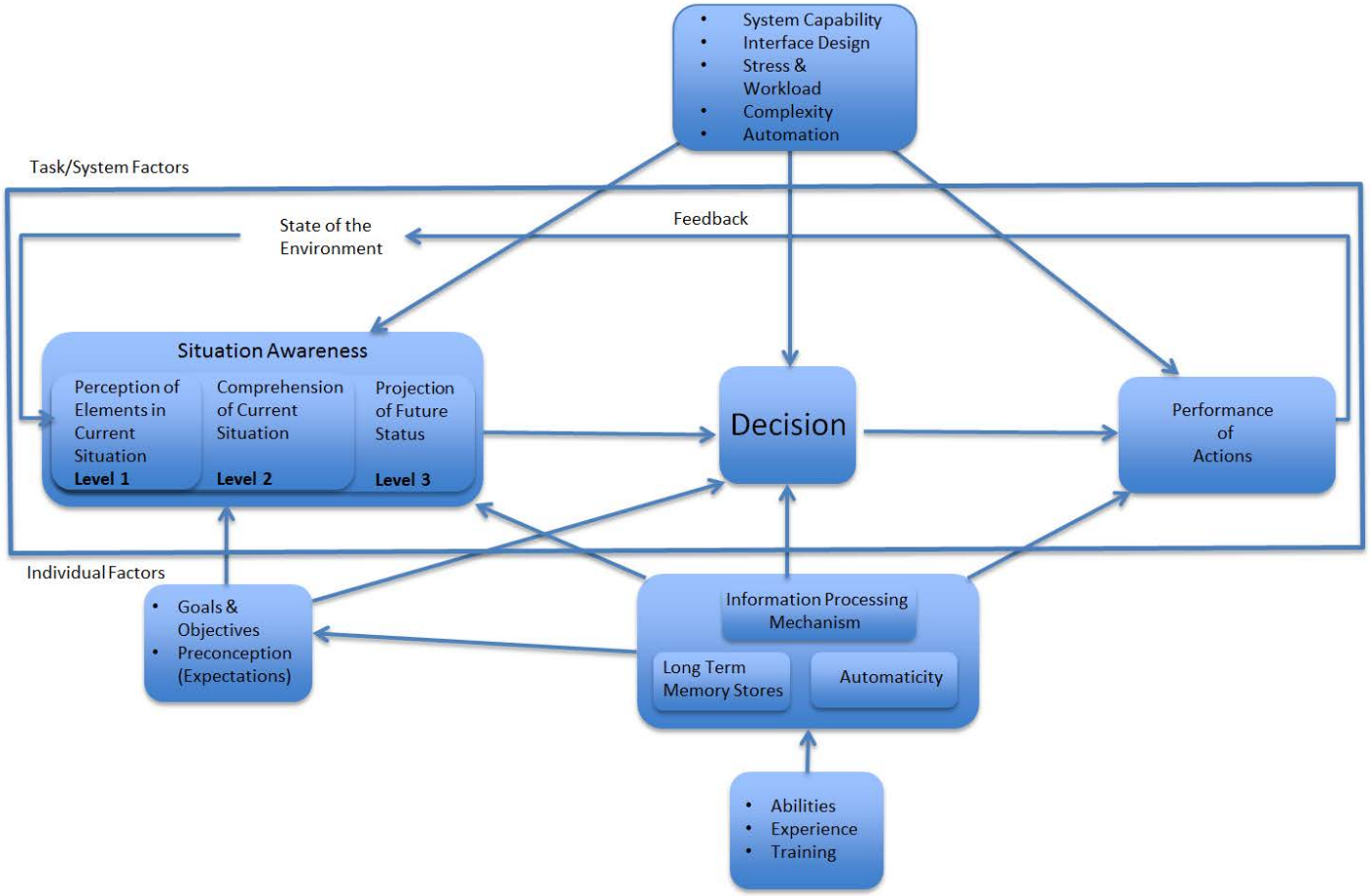

Figure 2. Endsley's Situational Awareness Model[37]

[37] Adapted from Endsley, "Situation Awareness in Dynamic Systems," 35.

Other authors who assess decision making in complex environments confirm the importance of SA data. Specifically, Messner et al. acknowledge a gap in SA theory: it neglects distribution mechanisms of data. Messner et al. contend that accurate SA information is collected swiftly and distributed to first responders.[38] The authors acknowledge that first responders need advanced systems to enhance cross-jurisdictional communication and SA technologies. Consistent with Messner et al., Jakobson, Buford, and Lewis posit that the evolving threat environment requires an investment in adaptive, interoperable communication systems to support these situational awareness needs.[39] However, how can that be achieved in complex operational environments that require the sharing of situational awareness information among diverse disciplines and agencies? Off-the-shelf mobile solutions may be the answer.

2. Sharing Situational Awareness through Off-the-Shelf Mobile Applications

Off-the-shelf mobile technologies can engage systems thinking of first responders more effectively than proprietary situational awareness technologies. A system's thinking approach reflects a group's shared understanding of an incident and its interaction with the complex environment. The Department of the Army's *Counterinsurgency Field Manual* reveals that soldiers are required to employ systems thinking to respond to dynamic tactical environments.[40] From the military's perspective, it is essential that assets in the field understand the complete threat environment before deploying. Alberts and Hayes posit that industrial-age military command structures and information systems

[38] Richard A. Messner et.al., "An Integrated Command, Control, and Communications Center for First Responders," *Proc. SPIE 5778, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense* IV (August 2005): 57, doi: 10.1117/12.603727.

[39] Gabriel Jakobson, John Buford, and Lundy Lewis, "Models of Feedback and Adaptation in Multi-agent Systems for Disaster Situation Management," *Proc. SPIE 6943, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense* VII (April 2008): 69430N, doi:10.1117/12.778635.

[40] Department of the Army, *Counterinsurgency Field Manual* (FM 3-24), (Washington, DC: Department of the Army, 2006).

are ineffective at dealing with the dynamic threats encountered today.[41] To enhance shared awareness, the U.S. military is employing off-the-shelf mobile technology to sustain information-sharing in foreign and domestic environments.[42]

General Stanley McChrystal, a renowned military strategist, feels that mobile technology is essential for enabling field elements to coordinate efforts in dynamic environments.[43] Currie and Galliers also acknowledge that advanced communications technology that can aggregate, process, and distribute data is essential to supporting dynamic operations similar to those encountered by the military and homeland security professionals.[44] Off-the-shelf mobile messaging applications such as WhatsApp can be downloaded from publicly available app stores on virtually any mobile device and enable this interoperable environment. This is essential because critical incidents may require disparate disciplines and agencies to work together despite not having a prior situational-awareness sharing strategy or platform. The NYPD and NYFD sharing situational awareness of the structural stability of the World Trade Center towers as they were burning on September 11, 2001, serves as an example. A mobile phone messaging application such as Telegram may have effectively allowed these disparate disciplines to share situational awareness.

Dr. Phil Hendrix, the founder of technology research and consulting firm immr, divides mobile applications into five broad categories. Level one applications focus on communication and can account for functions ranging from email to shared calendars. Level two represents data access applications and enables mobile access to internal and external data. Horizontal data applications constitute level three and include functions

---

41 David Alberts and Richard Hayes, *Power to the Edge: Command…Control…In the Information Age* (Washington, DC: CCRP, 2003), http://www.dodccrp.org/files/Alberts_Power.pdf.

42 Richard Clark Estes, "Inside the Military's Secretive Smartphone Program," Gizmodo, August 5, 2014, http://gizmodo.com/inside-the-militarys-secretive-smartphone-program-1603143142.

43 Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin, 2015), 162.

44 Wendy Currie and Bob Galliers, *Rethinking Management Information Systems: An Interdisciplinary Perspective* (New York: Oxford University, 1999), 54.

such as IT, operation, and field support.[45] Most homeland security situational awareness needs fall into these first three categories and are achievable via off-the-shelf mobile applications. Levels 4 and 5 are unique to the host organization and perform vertical and transformative functions that are beyond the scope of most homeland security situational awareness needs. Hendrix feels that these functions are best served by custom or proprietary applications.[46] Off-the-shelf social media mobile applications such as Twitter are representative of Hendrix's first three categories and have proven valuable to public-information needs.[47] Mobile applications such as WhatsApp can provide the horizontal, intra-agency interactions that are essential for real-time situational awareness needs.[48]

3. The Interoperability of Off-the-Shelf Mobile Applications

Off-the-shelf mobile applications can enhance first responder performance through the technologies' ability to engage collaboration. According to Dillon, collaboration is "the linking or sharing of information, resources, activities, and capabilities by organizations to achieve jointly an outcome that could not be achieved by the organizations separately."[49] High levels of cooperation such as this are integral to achieving effective resolutions to complex threats. Dillon posits that consumer products, such as smartphones and off-the-shelf apps, can be used to achieve inter-agency and inter-discipline collaboration. Walker concurs with Dillon that off-the-shelf mobile technologies offer easily adaptable options for companies and that interoperable devices are essential. Certain data may not be accessible for homeland security collaboration if

---

[45] Phil Hendrix, "Mobilizing the Enterprise with off-the-Shelf Apps and Custom Mobile Solutions," immr, August 2012, 5, http://www.immr.org/downloads/mobilizing-the-enterprise-with-off-the-shelf-apps-and-custom-mobile-solutions-dr-phil-hendrix.pdf.

[46] Ibid.

[47] Department of Homeland Security (DHS), *Lessons Learned: Social Media and Hurricane Sandy* (Washington, DC: DHS, 2013), 32, https://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20Social%20Media%20and%20Hurricane%20Sandy.pdf.

[48] Salim Ismail, Michael S. Malone, and Yuri Van Geest, *Exponential Organizations* (New York: Diversion Books, 2014), ebook.

[49] John M. Bryson et al., *Designing and Managing Cross-sector Collaboration*: *A Case Study in Reducing Traffic Congestion* (Washington, DC: IBM Center for the Business of Government, 2007), http://www.businessofgovernment.org/report/designing-and-managing-cross-sector-collaboration-case-study-reducing-traffic-congestion.

the appropriate application program interface is not available. This can be a concern for proprietary mobile applications, as they are typically not designed for use by anyone other than the host agency. Fortunately, the majority of off-the shelf mobile devices and applications such as WhatsApp are designed to interface with other devices and programs.[50]

Michael Dimario confirms the importance of interoperability of technology at various levels.[51] Dimario identifies challenges and opportunities for the military in achieving interoperability through technology. Challenges include legacy systems and new systems not interacting, evolving complexity of operating environment, and operators' trust in the system. While the U.S. military's interoperability concerns for multinational and multidisciplinary agencies may seem daunting, the needs from domestic homeland operations are equally challenging. However, from Dimario's perspective, off-the-shelf technologies can aid in developing systems that produce capabilities far greater than the sum of their parts.[52] In other words, a clearer picture of the operating environment can be achieved if more first responders contribute situational awareness via mobile devices to a common operating platform.

Public safety dispatchers are also taking steps to address the concerns of interoperability for first responders. The Association of Public-Safety Communications Officials (APCO) is developing a standard for mobile applications interface for public safety communications systems.[53] The organization is attempting to develop American National Standards Institute (ANSI) guidelines to ensure that off-the-shelf mobile applications are interoperable and reliable with public safety communications networks. In accordance with ANSI, APCO has identified "Key Attributes of Effective Apps for

---

[50] Guy H. Walker et al., "From Telephones to iPhones: Applying Systems Thinking to Networked, Interoperable Products," *Applied Ergonomics Journal* 40, no. 2 (March 2009): 209.

[51] Michael J. DiMario, "System of Systems Interoperability Types and Characteristics in Joint Command and Control," *2006 IEEE/SMC Conference on System of Systems Engineering*, doi: 10.1109/SYSOSE.2006.1652302.

[52] Ibid., 236.

[53] "Key Attributes of Effective Apps for Public Safety," Application Community, August 18, 2013, 8, http://appcomm.org/wp-content/themes/directorypress/thumbs/AppComm_Key_Attributes.pdf.

Public Safety and Emergency Response."[54] These attributes include interoperability, security, and relevant content to public safety applications as essential to meeting the needs of first responders.[55]

Currently, there is a groundswell of government support in addressing homeland security interoperability issues. In 2014, Congress ordered the Department of Homeland Security to develop information technology systems to exchange real-time voice, data, and video information during acts of terrorism, daily operations, planned events, and emergencies.[56] This amendment to the Homeland Security Act of 2002 has provided the legislative support for the development and utilization of situational awareness technologies for homeland security applications. This bill supports the points of McChrystal, Dillon, and Alberts et al. that advanced technology is needed to support the situational awareness and collaboration needs of the first responders of homeland security. Siever's research acknowledges that crowdsourcing tools can take the form of free off-the-shelf instant messaging applications such as WhatsApp or Twitter.[57]

4. Will Off-the-Shelf Mobile Applications Be Embraced?

Developing proprietary situational awareness software solutions can present many complications for homeland security agencies. *Forbes* contributor Chuck Cohn identifies that the costs associated with product development, maintenance, and training of proprietary systems can often exceed the budgetary constraints of most public safety agencies.[58] There may be a lack of IT-trained personnel in the agency to troubleshoot and develop the product. Off-the-shelf solutions offer an affordable alternative, but not without detractors. Cohn points out that off-the-shelf applications may not meet every

---

[54] Ibid.

[55] Ibid.

[56] *Interoperable Communications*, H.R. 4289 113th Congress.

[57] Jesse Sievers, "Embracing Crowdsourcing: A Strategy for State and Local Governments Approaching 'Whole Community' Emergency Planning," *State and Local Government Review* 4, no. 1 (March 2015): 61.

[58] Chuck Cohn, "Build vs. Buy: How to Know When You Should Build Custom Software Over Canned Solutions," *Forbes*, September 15, 2014.

need of the agency nor interact with other proprietary programs.[59] However, they can serve the very important function of maintaining situational awareness across disciplines during critical incidents.

Land mobile radios and desktop computers that served as situational awareness platforms for military and homeland security agencies are beginning to be replaced. Advances in Long Term Evolution (LTE) mobile networks, enabled devices, and off-the-shelf applications are proving to be more agile and accessible than legacy systems. Ushahidi, a free online mapping application, was used to assist with relief efforts after the earthquakes in Haiti in 2010.[60] Volunteers initiated the free off-the-shelf program to allow Haiti citizens to collaborate. However, Ushahidi was eventually adopted by various agencies in the U.S. Departments of Homeland Security and Defense to support rescue situation awareness. Harvard Professor Clayton Christensen developed disruptive innovation theory to identify the value added versus the threats posed by emerging technology.[61] Christensen points out that these innovations can transform a marketplace and displace previous technologies.[62] Alberts and Hayes concur that off-the-shelf mobile technologies can transform public and private sector operations through the interconnectivity of assets.[63] The developing field of mobile technology and applications could lead to the replacement of traditional situational awareness platforms with a more capable and "accepted" platform.[64] Salim Ismail examines the shift to information-based technologies to improve enterprise performance in his treatise, *Exponential Organizations*. Ismail posits that organizations that leverage external resources, such as off-the-shelf mobile applications, to achieve their objectives are better positioned to

---

[59] Ibid.

[60] Patrick Meier, "How Crisis Mapping Saved Lives in Haiti," *National Geographic*, July 2, 2012, http://voices.nationalgeographic.com/2012/07/02/crisis-mapping-haiti/.

[61] "Disruptive Innovation," Christensen Institute, accessed January 6, 2016, http://www.christenseninstitute.org/key-concepts/disruptive-innovation-2/.

[62] Ibid.

[63] Alberts and Hayes, *Power to the Edge*, 199.

[64] Thom Dick, "Will a Smartphone Replace Your Mobile Radio?" EMS World, July 1, 2016, http://www.emsworld.com/article/12213802/will-a-smartphone-replace-your-mobile-radio.

succeed than their competitors.[65] The emerging market of off-the-shelf mobile applications may represent the resources that can improve situational awareness for homeland security.

The technology acceptance model (TAM) presented by Davis provides insight on how off-the-shelf mobile technology will be received by government organizations. The model, developed in the mid-1980s, was designed to evaluate corporate employee acceptance of desktop information system (IS) technologies. The model takes into account a user's perceptions of a technology's ease of use and utility as well as the user's attitude.[66] Essentially, this theory identifies the social acceptance of technology. Reuver, Nikou, and Bouman argue that mobile technology application use is so prevalent that smartphone users download applications to support daily personal functions.[67] They feel that the pervasive use of mobile application technology in users' daily lives exceeds the discrete analysis of acceptance levels defined by Davis in TAM. As such, they have employed "domestication theory," which evaluates the assimilation of technology into everyday life.[68] Their research indicates that users are more apt to download and use off-the-shelf mobile applications for productivity and group communication rather than the apps that are native to the device. The messenger application WhatsApp is a profound example of domestication theory. Google Play Store reports that the application has been downloaded over 1 billion times and has a 4.4 out of 5 star assessment by users.[69]

Government agencies are in the early stages of recognizing the value of mobile application platforms for public awareness and private sector collaboration. As "broadband Internet access only" subscriptions are replacing cable television subscriptions in American households, government is communicating with the public

---

[65] Ismail et al., *Exponential Organizations*, 569.

[66] Fred D. Davis, "A Technology Acceptance Model for Empirically Testing New End User Information Systems: Theory and Results," (Ph.D. dissertation, MIT, 1985).

[67] Mark de Reuver, Shahrokh Nikou, and Harry Bouwman, "Domestication of Smartphones and Mobile Applications: A Quantitative Mixed-Method Study," *Mobile Media & Communication* 4, no.1 (June 2016): 351.

[68] Ibid., 349.

[69] "WhatsApp Messenger," Google Play, accessed November 13, 2016, https://play.google.com/store/apps/details?id=com.whatsapp.

through social media applications such as Twitter, Facebook, and Periscope.[70] These agencies are leveraging mobile application and Internet-based technologies to communicate with the public because of their acceptance. Sixty-five percent of adults are on at least one social media platform.[71] Opportunities for collaboration with mobile application services are also being exploited by government agencies. The Florida Department of Transportation signed an agreement with Waze, a community-based traffic and navigation app, to share situational awareness data and improve services to motorists.[72] This literature demonstrates the growing acceptance of mobile applications as effective platforms for enhancing situational awareness. More importantly, it demonstrates the ability of off-the-shelf applications to enhance public–private partnerships.

In 1965, psychologist Harold Leavitt developed his eponymous model to identify how the various components of an organization interact with one another.[73] The framework that Leavitt designed describes how mobile technology can empower individuals to collaborate for the benefit of the collective group.[74] The four main components of Leavitt's Diamond are people, structure, technology, and tasks. Leavitt posits that changes to one component, either positive or negative, have impacts on the other components. Organizations that acknowledge these four components and their interactions will be better equipped to engage in effective organizational change. Acknowledging barriers to change, such as organizational culture, is important for developing technology adoption strategies. Farnham, Pedersen, and Kirkpatrick posit that "getting technology into the hands of the organization is only a small part of the problem.

---

[70] Andrew Meola, "Broadband Subscribers Continue to Climb, While Cable Sees Mixed Subscriber Trends," *Business Insider*, May 23, 2016, http://www.businessinsider.com/cable-companies-lose-more-subscribers-as-cord-cutters-grow-2016-5.

[71] Laura Royden, "Now Trending #CityHall," Data-Smart City Solutions, April 28, 2016, http://datasmart.ash.harvard.edu/news/article/now-trending-cityhall-on-social-media-824.

[72] Elizabeth Birriel, "Case Study #3: Integrating Third Party Crowd Sourced Data," U.S. Department of Transportation, accessed November 13, 2016, https://www.pcb.its.dot.gov/t3/s150311/s150311_crowdsourced_data_presentation_birriel.pdf.

[73] Harold J. Leavitt, *Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches* (Chicago: Rand McNally, 1965), 1144.

[74] Leyland F. Pitt et al., "Integrating the Smartphone into a Sound Environmental Information Systems Strategy," *Journal of Strategic Information Systems* 20, no. 1 (March 2011): 28.

The larger issue is dealing with change in emergency situations."[75] Leavitt takes into account the many factors that influence how technology is adopted and how adoption affects the other elements of an organization (e.g., adopting a technology requires training people to use it). While Davis examines how technology is adopted, Leavitt examines the changes that can take place after adoption and ultimately lead to retention or removal of the technology. Leavitt's Diamond will aid in clarifying the long-term viability of off-the-shelf mobile application adoption.

5. Policy Implications for Off-the-Shelf Mobile Applications

The National Institute of Standards and Technology (NIST) has been tasked with developing policy recommendations for government agencies that use mobile applications in the course of their duties. Many of these recommendations are in draft form, pending approval. Steven Quirlogico from NIST's Computer Security Division has identified a multitude of security concerns associated with off-the-shelf mobile application technology for federal government agencies. Unauthorized access to sensitive information such as personally identifiable information, secure data, and geo-location, as well as camera and audio functions, are all concerns that NIST has identified.[76] Quirlogico also acknowledges that certain applications can lead to exhaustion of memory, the CPU, or battery life of the device.[77]

NIST is attempting to develop mobile-application security recommendations for government agencies. Michael Ogata, Barbara Guttman, and Nelson Hastings of NIST addressed some of Quirlogico's concerns in their January 2015 Public Safety Mobile Application workshop. This collaboration with public safety professionals identified potential remedies to the negative aspects of mobile applications used for situational awareness. Ogata, Guttman, and Hastings recommend requiring the application to

---

[75] Farnham, Pedersen, and Kirkpatrick, "Observation of Katrina/Rita Groove Deployment," 41.

[76] Steven Quirlogico et al., "Vetting Mobile Applications for Federal Agencies: NIST AppVet and DHS Carwash," NIST, January 28, 2016, 4, http://csrc.nist.gov/groups/SMA/forum/documents/january2016_presentations/FCSM_2016-AppVet-DHS-Final.pdf.

[77] Ibid.

- provide reports on the impact it will have on the device's battery;
- provide the possibility for remote control and monitoring should the application perform negatively;
- prove that it can network efficiently and responsibly;
- declare all information being gathered, transmitted, and retained; and
- declare what data protection has been implemented.[78]

Several federal bills have been introduced that would require mobile application developers and organizations to develop data-security measures for this emerging environment. The Application Privacy, Protection, and Security Act requires application developers to obtain the user's consent before collecting personal data. The developer must also provide the user with a method for withdrawing consent and deleting all personal data the developer has acquired.[79] The Secure and Protect Americans' Data Act requires the Federal Trade Commission (FTC) to establish information-security practices for the safe handling of personal information. The FTC must also evaluate consumer privacy programs. These evaluations allow the developer to identify any security vulnerabilities and threats as technology evolves. This bill also allows the user to "opt out" of providing personal information for marketing purposes and provides a formal process for notifying the appropriate government agencies when there is a security breach.[80] While many of these recommendations are in draft form, it is important to note that the federal government is taking steps to examine the security concerns of this rapidly evolving field.

---

[78] Michael Ogata, Barbara Guttman, and Nelson Hastings, *Public Safety Mobile Applications Security Requirements Workshop, Summary* (NISTIR 8018) (Giathersburg, MD: NIST, 2015), doi: 10.6028/NIST.IR.8018.

[79] *APPS Act of 2016*, H.R. 4517, 114th Congress. See https://www.congress.gov/bill/114th-congress/house-bill/4517?q=%7B%22search%22%3A%5B%22%5C%22mobile+application%5C%22%22%5D%7D&resultIndex=1.

[80] *Secure and Protect Americans' Data Act*, H.R. 4187, 114th Congress (2015). See https://www.congress.gov/bill/114th-congress/house-bill/4187?q=%7B%22search%22%3A%5B%22%5C%22mobile+application%5C%22%22%5D%7D&resultIndex=14.

6. Conclusion

In conclusion, most if not all of the literature reviewed places a great deal of importance on situational awareness for decision-making. Many of the authors recognize that mobile technology and, consequently, off-the-shelf applications are integral to meeting the challenges of situational awareness and interoperability. However, gaps exist in examining the challenges associated with technology that is not proprietary. While off-the-shelf mobile applications may present an affordable alternative to meet these challenges, further analysis on technology acceptance and barriers to adoption will be essential. This thesis identifies the challenges and opportunities for agencies looking to adopt off-the-shelf mobile applications to enhance situational awareness.

C. RESEARCH DESIGN

This thesis utilizes a program evaluation methodology to examine how off-the-shelf technologies are currently employed (or not employed) for homeland security. Davis' technology acceptance model (TAM) identifies why individual users adopt or refuse to adopt mobile applications.[81] The TAM framework was used to examine mobile applications' "perceived usefulness, perceived ease of use, attitude toward using, behavioral intent to use, actual use, and external variables."[82] Enterprise adoption challenges and opportunities will identify barriers and accelerators of off-the-shelf mobile application solutions. Existing surveys from the private sector support this research. Leavitt's Diamond provides the academic framework for clarifying the interaction between people, technology, structure, and tasks. This model identifies the relationships that affect technology adoption and how policy can improve or inhibit these relationships. This research also examines the current generations of homeland security professionals who are "native" to mobile technology to identify mobile application adoption trends.[83]

---

[81] Davis, "Technology Acceptance Model," 24.

[82] Ibid.

[83] "Millennial Teens," Refuel Agency, accessed March 25, 2016, http://research.refuelagency.com/wp-content/uploads/2015/07/Millennial-Teen-Digital-Explorer.pdf.

Case studies of public safety agencies and the private sector have provided the data to support this research. Publicly available information from the NYPD and its use of technology provides an example of mobile technology acceptance by homeland security. The NYPD's Mobility Initiative has distributed thousands of smartphones and mobile devices to its officers in the field. The initiative was established in 2014 with only a few devices employed for beta testing. The NYPD has recently expanded the program to include the distribution of mobile devices to all members of the department. These devices utilize proprietary software applications that interact with the agency's situational awareness systems. These systems include the Domain Awareness System (DAS), central dispatch, and shotspotter and have decreased response times to incidents by up to one minute.[84]

Off-the-shelf mobile applications such as WhatsApp, Telegram, and Periscope for homeland security situational awareness needs is examined. Currently, there are several proprietary mobile applications that support homeland security operations for agencies such as the NYPD and the State of New Jersey. As new applications and markets emerge, a thorough examination of off-the-shelf mobile technology and applications may increase cost savings for homeland security agencies and provide a vital service to the first responders of the homeland security enterprise.

Open-source surveys from the public and private sector support this research. Data from research and marketing industries, such as Pew and Foster Research Centers, acknowledge the acceptance of mobile technology applications by U.S. citizens. These surveys also identify trends that support or contradict the effectiveness of mobile applications in the workplace. Open-source government surveys aid in identifying management impediments to adopting mobile applications. The challenges range from fiscal constraints to apprehension with information security.[85] This data is integral in defining some of the challenges and opportunities in adopting this technology.

---

[84] Amanda Woods, "NYPD Response Times Faster, Thanks to Smart Phone Program," *New York Post*, April 22, 2016, http://nypost.com/2016/04/22/nypd-response-times-faster-thanks-to-smartphone-program/.

[85] Governing, *Mobile Strategy Survey*.

Academic theory synthesized with real-world applications also identifies the challenges and opportunities presented by off-the-shelf mobile applications for homeland security situational awareness needs. Academic theory was employed to evaluate practitioners' interest in adopting these technologies as well as the impact doing so will have on the operating environment. This research also examines how these technologies are currently employed and identifies related policy concerns for homeland security practitioners. This research provides objective policy recommendations regarding the adoption of off-the-shelf mobile applications for situational awareness needs.

D. CHAPTER OUTLINE

An examination of academic theory as well as current applications of proprietary technology to support situational awareness follows this introduction. Leavitt's Diamond provides the research framework to conduct a cost-benefit analysis of off-the-shelf mobile applications for first responders. An examination of the situational awareness of first responders on September 11, 2001, was conducted to identify shortfalls at the time that may have been overcome through the adoption of this technology. Finally, policy implications and recommendations are provided to agencies interested in adopting these technologies.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LEAVITT'S DIAMOND AND OFF-THE-SHELF MOBILE APPLICATIONS

Leavitt's diamond provides the framework this thesis uses to examine the adoption challenges and opportunities of off-the-shelf mobile applications. This framework (see Figure 3) proposes that organizational systems comprise four components that interact with one another: people, structure, tasks, and technology. Any changes that occur to one of these components will impact the others, as they are all interconnected.[86] This thesis examines the impact of off-the-shelf mobile applications (technology) on homeland security situational awareness needs (structure, people, and tasks.)

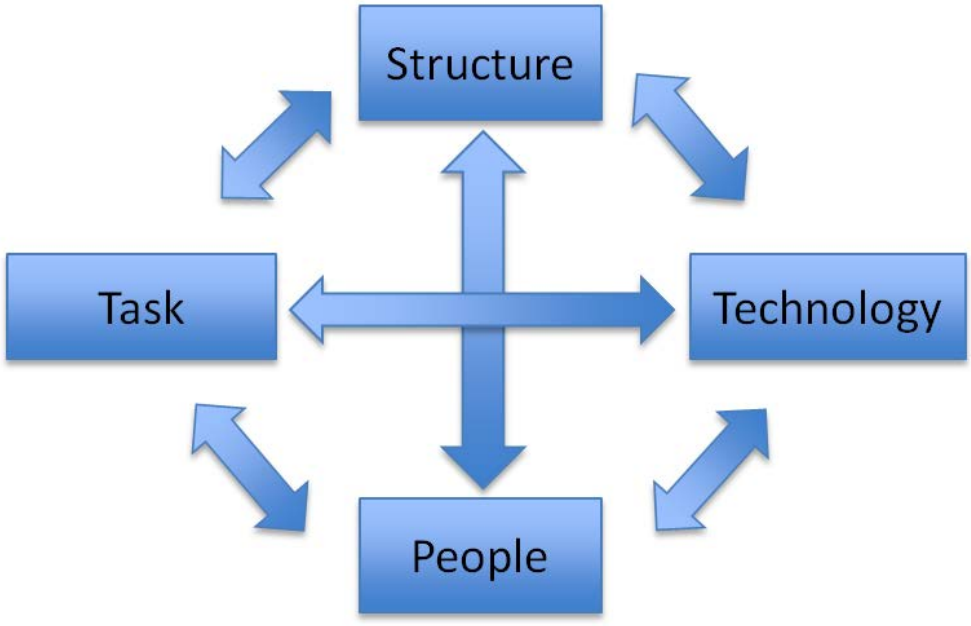

Figure 3. Leavitt's Diamond[87]

[86] Leavitt, *Applied Organizational Change*, 1144.

[87] Adapted from Leavitt, *Applied Organizational Change*.

A. TECHNOLOGY

Mobile applications, or "apps," are small, individual software units designed to operate on a mobile device such as a tablet or smartphone.[88] Previously, these software applications were limited in function when compared to software available to personal computers. However, advances in the processing speed and capabilities of mobile devices have narrowed the gap. Also impacting the proliferation of the mobile application market is the increasingly mobile-centric workplace. In 2013, a survey revealed that 61 percent of information specialists work outside of the office, with anticipation of a 66-percent increase by 2018.[89] These mobile workers have a buffet of applications for professional and personal use at their disposal. Google's Play Store and Apple's iTunes store contained over 2.9 million apps collectively, with over 200 billion downloads, as of June 2015.[90]

Device diversity is a concern for any situational awareness mobile application employed by the homeland security enterprise. The various disciplines that respond to critical incidents will employ a variety of personal and issued mobile devices. The ability of off-the-shelf mobile applications to communicate situational awareness across those spectrums is essential for first responder safety. Any application being considered by agencies to facilitate communication should be properly tested on a variety of mobile devices, as operating systems can behave differently.[91] Additionally, some mobile applications interface directly with desktop computers and these systems should also be evaluated.

Agencies should examine what off-the-shelf mobile applications are currently used by first responders for work-related functions. Surveys can identify employee

---

[88] *Techopedia*, s.v. "Mobile Application," accessed November 30, 2016, https://www.techopedia.com/definition/2953/mobile-application-mobile-app.

[89] Natalie Lambert, "Mobile Workspaces Enable Organizations to Keep up with Changing Workforce," *Citrix Blog*, March 20, 2014, https://www.citrix.com/blogs/2014/03/20/mobile-workspaces-enable-organizations-to-keep-up-with-a-changing-workforce/.

[90] "Combined Global Apple App Store and Google Play App Downloads," Statista, accessed November 30, 2016, http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/,2015.

[91] Ibid.

technology interests and needs. Field-testing of highly accepted applications should be conducted to ensure they perform as designed in the variety of situations first responders deploy to. Application analytics can inform managers to what makes an app successful or unsuccessful. There are a variety of app-analytic products that can enlighten IT program specialists to what users are doing inside the application and how it is performing.[92] Application developers use these systems to ensure they meet evolving user needs. Unlike desktop applications, which can take up to eighteen months to develop and be sustained for up to five years, mobile applications need frequent revision.[93]

Homeland security providers selecting a mobile application may need to choose from a variety of programs to meet user needs. Mobile web platforms, native apps, or a hybrid version are available and offer unique functionality. Mobile web applications use the device's browser to access the application page where data is exchanged. Ushahidi is a free, open-source mapping technology that functions in this manner. As mentioned previously, this platform was used with great success by volunteers and rescuers after a major earthquake in Haiti to support situational awareness needs of first responders.[94] These applications can easily work across a wide spectrum of devices because they are browser based.

Native applications are designed to run on the device themselves. There are many benefits to these apps because they are designed to perform simple functions and not impacted by high Internet traffic, cookies, and advertisements on the site. Native applications are also able to access the mobile device's sensors, which may be essential to aiding situational awareness. Global positioning systems of the mobile device can provide location of first responders during critical incidents, which is essential for blue force tracking. Mobile phone cameras can collect images of critical incident locations. In the future, it is likely more sensors will be integrated into mobile devices and native applications will play a larger role in enhancing first responder situational awareness.

---

[92] Ibid.

[93] Ibid.

[94] Meier, "Crisis Mapping in Haiti."

Hybrid applications provide an option that may meet agency requirements and resource constraints. These applications are written with web technologies (HTML5, CSS, and JavaScript). By using these web languages, the application processes data locally, on the browser engine of the device. This allows the application to access the device's sensors and local storage.[95] It also allows the user's device to interface with devices from other manufacturers, which is important for agencies that allow employees to bring their own personal devices to work.

Applications used for situational awareness should have a service-oriented architecture (SOA) to provide the ability to distribute data on mission and user profiles.[96] SOA allows two or more services or functions to communicate with one another.[97] Global information system (GIS) is the interaction between a mobile device and Global Positioning Systems (GPS). GPS information is essential to identify data in a spatial context. Incident location, first responders, resources, assets, infrastructure, and high-risk areas are essential information for situational awareness at critical incidents.[98] As system and mission complexity evolve, scalable functionality for situational awareness must also evolve.[99]

The continued growth and development of fourth generation (4G) LTE technology has enhanced the success of mobile enterprise solutions for the private sector. This development has led to data transmission speeds that are up to four times faster than the previous (3G) cellular network.[100] This speed rivals that of some home broadband networks and allows the user to perform complex data-driven tasks in areas that are outside of the office or home. These developments and future advances in mobile

---

[95] Tomas Agrimbau, "Developing Mobile Web Apps: When, Why, and How," Toptal, accessed December 15, 2016, https://www.toptal.com/android/developing-mobile-web-apps-when-why-and-how.

[96] ESRI, *Public Safety and Homeland Security Situational Awareness* (White Paper J-9698) (Redlands, CA: ESRI, 2008), 6, http://www.esri.com/library/whitepapers/pdfs/situational-awareness.pdf.

[97] Douglas K. Barry, "Service Architecture," accessed January 10, 2016, http://www.service-architecture.com/articles/web-services/service-oriented_architecture_soa_definition.html.

[98] ESRI, *Public Safety and Homeland Security Situational Awareness*, 4.

[99] Ibid.

[100] Tom Pica, "What Is 4G and Why it Matters," Verizon, April 30, 2012, http://www.verizonwireless.com/news/article/2012/05/what-is-4GLTE-and-why-it-matters.html.

technology will likely lead to an increase in the mobile workplace. The impact that this technology has had on the private sector is remarkable and the utility for homeland security warrants further examination.

B. PEOPLE

For the purpose of this research, the first responder of the homeland security community is considered the "people" component. The members of this community comprise the federal, state, local, and tribal agencies that respond to domestic critical incidents. Their disciplines include, but not limited to, fire, emergency medical services, and law enforcement. The equipment, training, and experience of these personnel are very diverse. The proliferation of mobile technology in the homeland security work environment has immense impact on this component.

The upcoming generation of homeland security professionals will be digital natives. This term is used to describe the youth that have grown up using technology such as the Internet, computers, and mobile devices.[101] This generation has proven itself adept at incorporating mobile devices and applications into their daily lives. Ninety-two percent of adults age twenty to twenty-four use three or more new mobile applications each month.[102] These "technology literate" employees embrace off-the-shelf mobile applications and find innovative ways to utilize them for daily functions. Proprietary systems will require a certain level of training to allow the employee to adopt and use the technology. However, off-the-shelf mobile solutions will require little training and are likely to have some familiarity with the younger generation of adopters. Challenges may exist with older generations who do not embrace mobile solutions; however, that number is decreasing. A recent survey found that 78 percent of smartphone owners over the age of fifty feel that their device represents "freedom."[103] On the other hand, 67 percent of IT

---

[101] *Techopedia*, s.v. "Digital Native- Definition," accessed June 7, 2016, https://www.techopedia.com/definition/28094/digital-native.

[102] Refuel Agency, "Millennial Teens."

[103] Aaron Smith, "The Smartphone Difference," Pew Research Center, April 1, 2015, http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

decision-makers feel that the lack of data protection measures on mobile devices is concerning.[104]

American acceptance of mobile devices consequently impacts the acceptance of of-the-shelf mobile applications in the workplace. In 2015, two-thirds of Americans identified as smartphone owners, up 35 percent from 2011.[105] Ninety percent of government employees use at least one mobile device for work-related functions.[106] Of those employees, 69 percent use a work-provided device, 15 percent use a personal device, and 16 percent use both.[107] The TAM proposed by Davis, discussed previously and shown in Figure 4, has utility in correlating this data.[108]

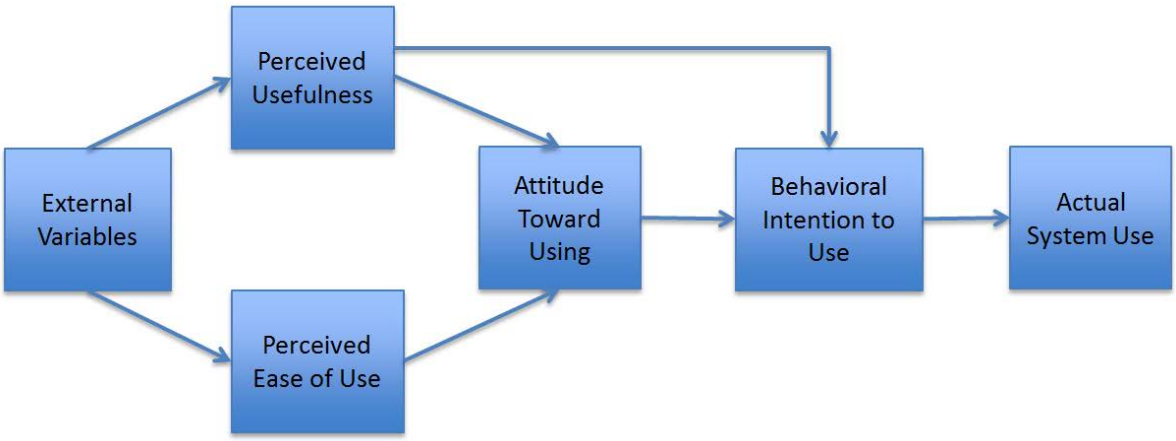

Figure 4. Technology Acceptance Model[109]

[104] "Jump Start Mobile Productivity with MDM and Secure File Sharing," Citrix, 3, accessed February 20, 2017, https://www.citrix.com/content/dam/citrix/en_us/documents/oth/jump-start-mobile-productivity-with-mdm-and-secure-file-sharing.pdf.

[105] Smith, "The Smartphone Difference."

[106] Ibid.

[107] Ibid.

[108] Davis, "Technology Acceptance Model," 24.

[109] Adapted from Davis, "Technology Acceptance Model," 24.

Government employees have a high acceptance of mobile technology and related applications. Consequently, it can be inferred that there is also a positive attitude toward using this technology attributed to a perceived ease of use and usefulness. Americans' acceptance of off-the-shelf mobile application technology indicates that homeland security professionals could effectively employ this technology. However, does this framework take into account organizational culture and resistance to change? Research has indicated that changes related to work-associated procedures can have negative outcomes ranging from temporary reduction in productivity to internal sabotage.[110] Additional research indicates that, as organizations continue to evolve and represent the populations they protect, they will reflect the same characteristics of that population. This would infer that homeland security agencies would be apt to adopt mobile application technology as the U.S. populous has.

Off-the shelf mobile applications can support situational awareness needs due to their high levels of acceptance. Users spend 90 percent of their mobile device use in apps compared to mobile web.[111] However, this data is conflicting with information regarding mobile application retention. Seventy-seven percent of average Android app users stop using apps three days after install.[112] This is important for any homeland security professional to acknowledge when examining an off-the-shelf mobile application because popular apps such as WhatsApp have retention rates of 90 percent after thirty days.[113] This level of retention demonstrates effective technology acceptance by users and

---

[110] James Hart, "The Management of Change in Police Organizations," in *Policing in Central and Eastern Europe: Comparing Firsthand Knowledge with Experience from the West*, ed. Milan Pagon (Ljubljana, Slovenia: College of Police and Security Studies, 1996), https://www.ncjrs.gov/policing/man199.htm.

[111] Simon Khalaf, "Seven Years into the Mobile Revolution: Content Is King…Again," Yahoo, August 26, 2015, https://yahoodevelopers.tumblr.com/post/127636051988/seven-years-into-the-mobile-revolution-content-is.

[112] Andrew Chen, "New Data Shows Losing 80% of Mobile Users Is Normal, and Why the Best Apps Do Better," accessed December 15, 2016, http://andrewchen.co/new-data-shows-why-losing-80-of-your-mobile-users-is-normal-and-that-the-best-apps-do-much-better/.

[113] Amir Efrati and Peter Schulz, "Which Apps Retain Their Users—And Which Ones Don't," The Information, April 7, 2015, https://www.theinformation.com/which-apps-retail-their-users-and-which-ones-dont.

therefore increased likelihood for use in sharing situational awareness during critical incidents.

Bring-your-own-device (BYOD) policies can present many challenges and opportunities for agencies. Some homeland security agencies cannot afford to supply their members with the hardware to facilitate mobile operations. Also, there are employees who prefer to use their own mobile devices due to familiarity and convenience. Policy concerns related to personal mobile technology in the workplace were observed in the email server issues of former Secretary of State Hillary Clinton; concerns of information security on personal technology drew a great deal of negative attention to the presidential candidate. This event identifies how an individual's preference to use personal technology for work-related functions can be problematic. Employees who use off-the-shelf mobile applications for personal and professional applications can create security and public perception concerns for homeland security agencies. As BYOD environments grow, appropriate policy will be needed to guide employee behavior.

Industry experts have identified many challenges when an enterprise seeks to develop and implement mobile applications into their operations. Gartner, a leading IT consulting company, advises that traditional procurement methods for desktop applications are not applicable to mobile applications.[114] Device diversity, network connectivity, and other mobile-specific considerations create challenges that most agency IT managers do not consider when examining mobile applications. Application users tend to have shorter session lengths and their experience tends to drive interest in continued use. Mobile application developers must now consider metrics for functionality, performance, load, and user experience testing, as well as an application's agility, in assessing the utility of mobile applications.[115]

A user's decision to adopt a technology is more complex than most would think. Communications scholar Everett Rogers posits that the decision to adopt or reject a

[114] Cynthia Lee, "Gartner Says Traditional Development Practices Will Fail for Mobile Apps," Gartner, August 14, 2014, http://www.gartner.com/newsroom/id/2823619.

[115] Ibid.

technology is based on an individual engaging in a five-step innovation-decision process. First, the user must be aware of the innovation and understand how it works. In the second step, the user forms an opinion of the innovation as either favorable or unfavorable. In the third step the user takes action to adopt or reject the innovation. If applicable, the user engages the fourth step, in which the innovation is put into use. Finally, in the fifth step, the individual reinforces the decision that has already been made to either adopt or reject the innovation.[116]

Rogers also identifies five qualities that can enable innovations to spread. These qualities can be used to frame evaluations of products and aid in determining up to 87-percent adoption rates.[117] First, relative advantage identifies how users perceive the innovation to be better than what precedes it. Second, the innovation must be compatible with existing practices. Third, the innovation must be simple and easy to use. If the innovation requires the adopter to develop new skills and understanding, it will struggle to be adopted. Fourth, the innovation should also be available for field testing. Testing and evaluation periods prior to procurement lead to less risk for the user. Finally, users should be able to see results from testing to diminish the need to perform their own.[118]

The diffusion of innovations model divides technology adopters into five categories: innovators, early adopters, early majority, late majority, and laggards. These categories are broken down into a bell curve distribution shown in Figure 5.[119] These groups have their own attitude to innovation adoption that reflects their interests at the time of adoption.

---

[116] Everett M. Rogers, *Diffusion of Innovations*, 4th edition (New York: Free Press, 1995), 21.

[117] Les Robinson, "A Summary of Diffusion of Innovations," Changeology, January 2009, 1, http://www.enablingchange.com.au/Summary_Diffusion_Theory.pdf.

[118] Ibid., 2.

[119] Rogers, *Diffusion of Innovations*, 281.

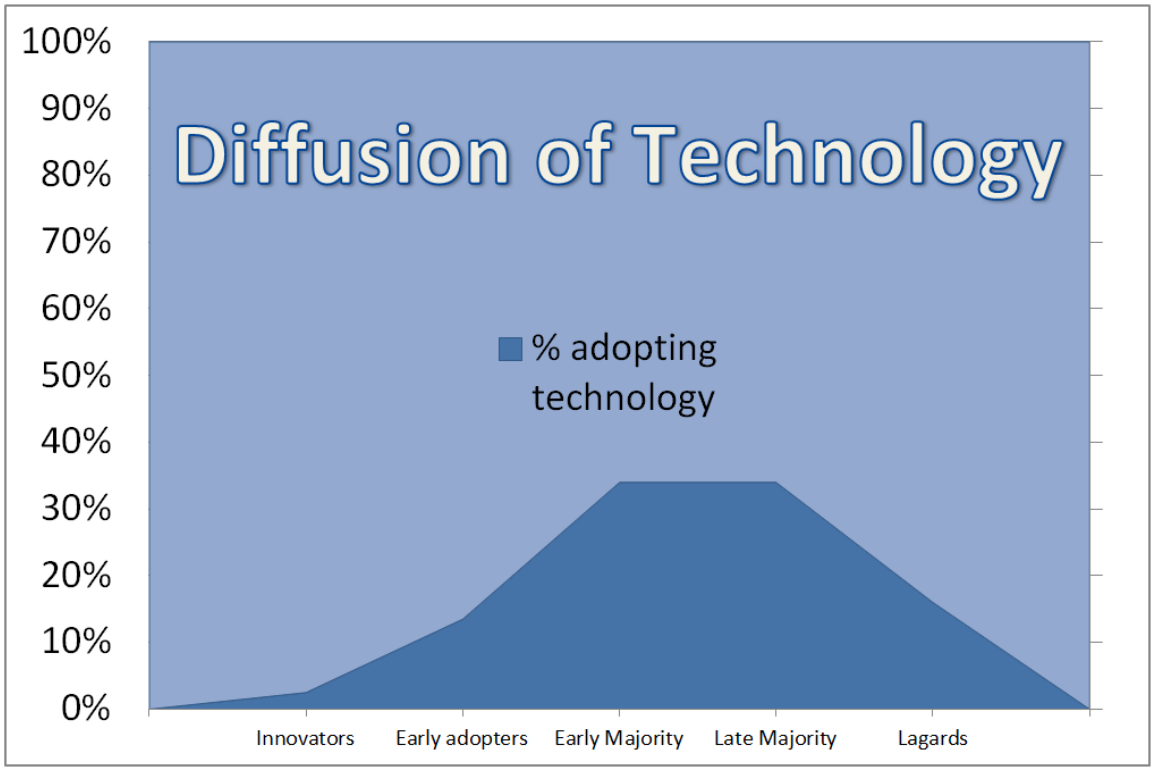

Figure 5. Technology Diffusion Graph[120]

The first group, innovators (2.5 percent), tends to be relatively small in number and spends a great deal of energy in developing new ideas. Early adopters (13.5 percent) are looking for advantages and tend to be better informed about new products or behaviors. Their integration at early stages will aid in allowing an innovation to be modified to meet mainstream needs. Early majority (34 percent) are pragmatic individuals who are comfortable with technology, but will need to see the benefits of adoption. This group tends to be risk averse, but looks for better ways to perform current tasks. They do not prefer complex solutions that require too much training. Late majority (34 percent) are risk averse and uncomfortable with new ideas. They will follow the mainstream and are easily influenced by laggards. Laggards (16 percent) see only high risk in adopting a particular innovation. However, this group can be swayed if it becomes familiar with the technology and can appreciate the advantages of adopting it.[121]

[120] Adapted from Rogers, *Diffusion of Innovations.*

[121] Ibid.

Product adoption involves the management of risk and uncertainty. One way to overcome barriers to adoption is through the successful adoption of the product by people who are known personally and are trusted. Users need to be assured by a credible person that the innovation "will not lead to embarrassment, humiliation, financial loss or wasted time."[122] Higher-risk adoptions require peer-to-peer communications to enable adoption. Marketing methods are evolving to recruit highly networked individuals to spread innovations. These "opinion leader tactics" can produce dramatic behavioral changes and aid technology adoption.[123] Effective communication will be essential for enterprise adoption of off-the-shelf mobile application technology.

C. TASKS

The tasks of first responders will change substantially with the increased use of off-the-shelf mobile application technology. Mobile technology hardware and software applications have benefited from the increased investment by the private sector in mobile enterprise solutions. Mobile enterprise solutions are required to engage a globalized economy and generations of digital natives. Mobile applications that enhance productivity for the private sector also show a great deal of promise for the public sector. However, the public sectors lack of understanding of the available technology and how to create policy to embrace it may impede its adoption.

Currently, most first responders rely upon land mobile radio (LMR) systems for communication and situational awareness. The increased capabilities of mobile phones, software applications, and ubiquitous broadband connectivity encourage a trend toward mobile devices taking a larger role in these areas.[124] Off-the-shelf mobile technology has already been incorporated into first responder missions. Israeli police have used mobile apps such as WhatsApp to provide situational awareness in critical incidents.[125]

---

[122] Robinson, "A Summary of Diffusion of Innovations," 3.

[123] Ibid., 4.

[124] Jonas Landgren and Urban Nulden, "A Study of Emergency Response Work: Patterns of Mobile Phone Interaction," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (April 2007), https://pdfs.semanticscholar.org/343d/e3a625a5367609c37288c33d85ef06e49095.pdf.

[125] Vibha Verhma, "What's up in the Police Department? It's WhatsApp," *Herald*May, 19, 2015, http://www.heraldgoa.in/Goa/What's-up-in-the-police-department-It's-WhatsApp/88703.html.

Commanders in the U.S. homeland security disciplines are frequently employing mobile email and messaging applications to send and receive round-the-clock updates on evolving situations. This evolution in tasking has changed expectations of homeland security practitioners to perform more effectively, as technology can provide a more complete picture of critical incidents.

Off-the-shelf mobile technology has the potential to drastically change the methods of communication of first responders. Disparate LMR channels and frequencies will be supplanted by a technology that over 85 percent of young adults possess and feel very comfortable with.[126] It can be further speculated that the additional functionality provided by these mobile platforms will enhance cooperation of first responders. "Peer-to-peer technology reduces many of the barriers to negotiations in cross-organizational interactions: removing excuses to not share info, providing a neutral space to foster compromise, and exposing the difference in expectations and goals."[127] Complex natural and manmade disasters demand collaborative and agile situational awareness platforms.

Off-the-shelf mobile applications can enhance the "whole of community" approach to emergency management that FEMA espouses.[128] Whole of community emergency management refers to the federal, local, state, tribal, and territorial partners as well as private sector organizations collaborating to resolve a crisis. During critical incidents, collaboration across disciplines is essential. Members of the public and private sector staff emergency operation centers (EOCs) to enable collaboration. An EOC serves as an "information processing and dissemination mechanism that supports and coordinates operations in the field."[129] Face-to face collaboration at these facilities are very effective, but may not always be possible. Off-the-shelf mobile applications provide adaptive communication systems to facilitate inter-organizational situational awareness.

---

[126] Smith, "The Smartphone Difference."

[127] Farnham, Pedersen, and Kirkpatrick, "Observation of Katrina/Rita Groove Deployment," 46.

[128] DHS Science and Technology Directorate, *First Responder Communities of Practice Virtual Social Media Working Group Community Engagement Guidance and Best Practices* (DHS2012F0918) (Washington, DC: DHS, 2012), https://www.dhs.gov/sites/default/files/publications/Virtual%20Social%20Media%20Working%20Group%20VSMWG%20Community%20Engagement-508.pdf.

[129] Jim Bailey, "5 Elements of Proactive Situational Awareness," Emergency Management, May 4, 2015, http://www.govtech.com/em/training/5-Elements-Proactive-Situational-Awareness.html.

This is important because the private sector "owns and operates an estimated 85 percent of the critical infrastructure and resources" of the nation.[130]

The program manager of the Information Sharing Environment (PMISE) acknowledges the need to share intelligence with these entities and efforts are underway to build secure networks to facilitate this.[131] However, there is no guidance on how public sector agencies can share unclassified situational awareness, in real time, with the private sector. David Miller, of the Iowa Homeland Security and Emergency Management Division, acknowledges the importance of communicating directly with the private sector. "We need to understand their emergency response efforts, and we need to share information more actively."[132] Off-the-shelf mobile applications can assist agencies in developing ad hoc information-sharing environments. A recent study on response to critical incidents revealed that "communication within the rescue service can be managed through the radio communication system. However, communication with other organizations has to be mediated through alternative channels such as mobile phones."[133] This will be beneficial to incident commands that identify emergent private sector partners with which they would like to send and receive situation updates.

Building or procuring a proprietary situational awareness system for public and private sector users can be problematic. Proprietary systems are designed to integrate back-end services to limit duplication of administrative functions. However, these systems are typically not designed to integrate private sector partners. Consequently, this can detract from collaboration. However, off-the-shelf mobile applications such as WhatsApp and Slack are designed to scale collaboration. Communication systems that are universally available and scalable are ideal for providing an effective situational awareness environment between disparate agencies.

---

130 "Critical Infrastructure and Key Resources," Information Sharing Environment, accessed January 12, 2017, https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources.

131 Ibid.

132 David Raths, "Private-Sector Organizations Earn a Seat in the Emergency Operations Center," Emergency Management, May 17, 2010, http://www.govtech.com/em/disaster/Private-Sector-Organizations-Emergency-Operations-Center.html?page=2.

133 Landgren and Nulden, "A Study of Emergency Response Work," 9.

Recommendations exist on how EOCs can develop effective situational awareness. Retired Marine Corps Intelligence Officer Jim Bailey recommends EOCs employ a five-step process to develop an effective situational awareness program.[134] Agencies should first identify what their information requirements are. This can range from field reports to status of power outages. Next, the EOC needs to determine how it will gather this information. In some cases, the information may be shared by having a representative of an agency physically present in the EOC. However, off-the-shelf mobile technology can assist with sharing situational awareness with entities that are unable to staff the center. The third step is deciding how to analyze the information received. Analysis of situational awareness is left to the recipient, as information may have different meanings to the receiver. The fourth step of a proactive situational awareness program is to determine how the information will be shared. In certain critical incidents, the EOC may need to establish separate channels for the distribution of classified information. Unclassified material can be distributed over systems that are designed for scalability. The final step of this program is to choose a technology that will help manage the information that is distributed.[135] Off-the-shelf mobile applications can be profoundly effective at sharing information to the diverse stakeholder groups of EOCs.

Simply identifying off-the-shelf mobile applications and developing policy for their use in situational awareness will not provoke acceptance. Nancy Johnson, previously the acting director of California's Office of Technology Services, advises that agencies need to build something that the user wants, needs, and will use.[136] Unfortunately, research indicates that most first responder organizations use networks that restrict communication.[137] However, smartphones and off-the-shelf mobile applications can overcome those boundaries. Identifying the value of situational

---

[134] Bailey, "5 Elements of Proactive Situational Awareness."

[135] Ibid.

[136] Colin Wood, "The Secret behind Building Successful Mobile Apps," *Government Technology*, April 30, 2012, http://www.govtech.com/policy-management/The-Secret-Behind-Successful-Mobile-Apps.html.

[137] Landgren and Nulden, "A Study of Emergency Response Work," 2.

awareness, and how to use mobile devices and applications to share it, is essential prior to critical incidents.

Lack of understanding of the importance of situational awareness can lead to first responder near-miss and casualty events. Oklahoma Task Force One realized the importance of situational awareness after a tornado struck Moore, Oklahoma in May 2013. Fortunately, the state-funded urban search and rescue team was able to use local hackers, Civic Ninjas, to develop a mapping program for the responders in a short time.[138] Research identifies that, during rescue operations, first responders are "overworked and under a lot of stress and have little time or no cognitive ability to adopt a new technology."[139] First responder agencies should consult off-the-shelf solutions for testing and evaluation prior to critical incidents.

While many first responders may not be aware of the value of situational awareness, there is little argument regarding its value to critical incident managers. Jim Bailey posits that "every single decision EOC responders make depends upon accurate, complete, and current situational awareness."[140] EOCs are actively embracing off-the-shelf, social media platforms to enhance situational awareness through the wealth of publicly supplied information.[141] It can be projected that off-the-shelf mobile applications for first responder situational awareness will also be embraced. However, first responders need to have the value demonstrated to them before large-scale acceptance can happen.

D. STRUCTURE

The adoption of mobile application technology will lead to substantial changes in the structure of homeland security. Higher levels of interoperability can be achieved

---

138 Jessica Hughes, "Civic Ninjas Find Long-Term Solutions to Government Problems," Government Technology, August 27, 2014, http://www.govtech.com/Civic-Ninjas-Find-Long-Term-Solutions-to-Government-Problems.html.

139 Farnham Pedersen, and Kirkpatrick, "Observation of Katrina/Rita Groove Deployment," 47.

140 Bailey, "5 Elements of Proactive Situational Awareness."

141 Jie Yin et al., "Using Social Media to Enhance Emergency Situation Awareness," *IEEE Intelligent Systems* 27, no. 6 (2012): 52.

through mobile applications with disparate agencies and disciplines. Currently, these agencies rely upon a centralized command structure during critical incidents; when a critical incident takes place and a multi-agency/discipline response is required, personnel must staff command post locations and receive directions from a unified command. This unified command will have an agency representative equipped with proprietary LMR communication systems and terminology. During prolonged events, this is the preferred method for command and control. However, this structure tends to take some time to establish. Emergent events for which disparate agencies respond can create challenges in communication interoperability and situational awareness.

Research indicates that, in the next decade, mobile broadband technology will have an increased role in critical incident response.[142] Mobile applications can provide more robust information to frontline first responders in real time. The enhanced information provided to these edge users will result in more efficient and effective responses.[143] Mobile application technology will empower first responders to make decisions, independent of former command and control structures. This evolution to "bottom-up" decision making will lead to drastic changes in command and control measures for homeland security incident command. While the change in command and control structure may cause some concern among para-military organizations, this movement is not without precedence. The U.S. military currently uses network-centric warfare, supported by off-the-shelf mobile technology, for special operations overseas.[144] This evolution of command and control will serve as an excellent template for the structure of homeland security.

Managing and enabling information for situational awareness is crucial for intelligence-led policing.[145] The New Jersey State Police has been utilizing intelligence-led policing since the early 2000s in order to proactively address organized crime in

---

[142] Alexander Grous, "Socioeconomic Value of Mission Critical Mobile Applications for Public Safety in the UK: 2X10MHz in 700MHz," LSE Research, November 2013, http://eprints.lse.ac.uk/69180/1/Grous_Socioeconomic_value_of_mission_critical_applications_UK_2013_author.pdf.

[143] Ibid.

[144] Alberts and Hayes, *Power to the Edge*, 199.

[145] Ibid. 7.

urban areas. The *New Jersey State Police Practical Guide to Intelligence-Led Policing* aims to achieve "better situational awareness through the collection of data and the creation, dissemination, and cataloguing of intelligence products."[146] However, intelligence processes can be delayed in nature due to the time consumed by the intelligence cycle and the manner in which intelligence products are distributed: email. In New Jersey, situational awareness information during critical incidents is also shared via email by the state emergency operations center (SEOC) and the Regional Operations Intelligence Center watch operations unit. However, research indicates that only 22 percent of emails are actually read; conversely, 98 percent of all text messages are read by mobile users.[147] This demonstrates the viability of off-the-shelf mobile applications to support real-time communication needs.

Mobile messaging systems have evolved immensely since their inception. SMS, or "texts," are brief, electronic messages between two or more mobile devices over the cellular network. SMS were originally limited to 144 alphanumeric characters, but they can now transmit images, video, sound, and user location. Recently, there has been an increase in the popularity of mobile instant messaging (MIM). MIM allows for SMS to transmit over the Internet as opposed to the cellular phone network alone. Smartphones using MIM platforms can access Wi-Fi or the device's cellular data plan to engage Internet functions to share information. The user can also embed clients for the devices that the group is communicating with and enable secure transmission of data. MIM services such as WhatsApp, Telegram, and WeChat facilitate the needs of secure communication for situational awareness that homeland security needs.

Homeland security, military, and law enforcement institutions struggle to introduce technology to the field. The dynamic mission responsibilities of these disciplines require a faster delivery of technology to the field, but doing so can be

---

[146] Ray Guidetti, *New Jersey State Police Practical Guide to Intelligence-Led Policing* (New York: Manhattan Institute for Policy Research, 2006), 2, http://www.njsp.org/divorg/invest/pdf/njsp_ilpguide_010907.pdf.

[147] Mike Kujawski, "Text Messaging vs. Mobile Instant Messaging," May 23, 2014, GovLoop, https://www.govloop.com/community/blog/text-messaging-vs-mobile-instant-messaging/.

complicated.[148] Research and development organizations want to push technology to the user for field evaluation. Operational users tend to prefer systems that have been tested and proven in the field. Dr. Tony Tether, of DARPA, feels that both parties meeting in the middle can overcome these challenges.[149] Recently, the Department of Homeland Security (DHS) has identified the value of developing social media programs sooner rather than later to support operations. DHS acknowledges that the "use of social media can be fraught with missteps and anxiety if expectations are not set with the public and employees from the beginning"; social media practitioners, by and large, "advocate the theory of 'failing fast.' To 'fail fast' means to try something—anything—and if it doesn't work, try something else. This means it's best to start using social media today before the emergency."[150] This approach mirrors a "start-up" business approach of getting the product introduced quickly to work out the kinks, instead of delaying until it is perfect and consequently irrelevant.

[148] Stephen M. Jarrett, "Transition of Advanced Technology to Military, Homeland Security and Law Enforcement Users," *Proceedings of SPIE* 5403 (September 2004): 78, doi: 10.1117/12/542420.

[149] Ibid., 79.

[150] DHS Science and Technology Directorate, *Next Steps: Social Media for Emergency Response* (Washington, DC: DHS, 2012), 9, https://www.dhs.gov/sites/default/files/publications/Virtual%20Social%20Media%20Working%20Group%20VSMWG%20Next%20Steps%20Social%20Media%20for%20Emergency%20Response.pdf.

III. SEPTEMBER 11, 2001, AND SITUATIONAL AWARENESS IN NEW YORK CITY

On September 11, 2001, the largest rescue operation in the history of New York City took place. The response efforts that fateful day have been extensively analyzed and documented. Remarkable feats of heroism and innovation likely saved thousands of lives; however, numerous gaps in response strategies to critical incidents were identified. Since the tragic event, changes in policies, training, and equipment have enhanced preparedness and coordinated response for catastrophic events. However, there are many concerns that have been left unaddressed. Currently, there is a deficiency in the ability of diverse first responder agencies and disciplines to promote situational awareness in austere environments.

Today, most first responders still rely on LMRs and proprietary technology to conduct operations. This can be very problematic as complex response scenarios, such as the September 11 attacks and the attacks in Paris on November 13, 2015, require shared situational awareness technology for response command and control. Fortunately, evolving off-the-shelf mobile applications may provide an opportunity to address these needs.

The *9/11 Commission Report* documents the importance of shared situational awareness among first responders. According to one FDNY chief commanding in the South World Trade Center (WTC), "One of the most critical things in a major operation like this is to have information. We didn't have a lot of information coming in. We didn't receive any reports of what was seen from the [NYPD] helicopters. It was impossible to know how much damage was done on the upper floors, whether the stairwells were intact or not."[151] The communications from the NYPD helicopter circling the burning towers indicated melting steel on the upper floors and falling debris that created hazardous conditions for the responders on the ground. Information as to which agency had cleared what floor of the WTC buildings also led to duplicated efforts and more time spent by

[151] National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report* (New York: W.W. Norton), 298.

first responders in the rapidly degrading structures. The attacks on September 11, 2001, identified challenges with inter-agency communications and information-sharing as well as limitations in intra-agency sharing. When the FDNY vessel on the Hudson River communicated the collapse of the South Tower over LMR systems, no one at the WTC received the message, which further delayed evacuation efforts of the North WTC Tower.[152]

The lack of communications interoperability and shared situational awareness among responding agencies that day has been acknowledged by policymakers, and efforts have been made to strengthen communications through technology and policy. However, many efforts have still not achieved this aim. Billions of dollars have been spent to upgrade the 9-1-1 call system and emergency communications infrastructure, but reliable interoperable communications has yet to be achieved. To remedy the lack of communication between the agencies, the FDNY and NYPD dispatching centers were moved to the same floor in 2011.[153] However, the recent death of two police officers in a fire has shown that dispatcher proximity does not automatically lend to shared situational awareness in critical incidents.[154]

The lack of shared situational awareness in the rescue efforts on September 11 have also been acknowledged by the National Institute of Science and Technology (NIST) in its *Response to World Trade Center* report. NIST's investigation confirms the finding in the *9/11 Commission Report* that first responders inside the WTC buildings assisting with evacuations suffered from limited situational awareness.[155] The report acknowledges that the commander's inability to see what was happening on the outside led to many challenges. Unfortunately, due to communication issues, the first responders

---

[152] Ibid., 306.

[153] Bob Hennelly, "10 Years Later, FDNY and NYPD in Radio Sync," WNYC, September 27, 2011, http://www.wnyc.org/story/\161257-blog-10-years-later-fdny-and-nypd-radio-sync/.

[154] Juan Gonzalez, "Two More Fatal Fires Highlight Consistent Communications Problems with NYC 911 System," *New York Daily News*, April 22, 2014, http://www.nydailynews.com/new-york/fires-show-nyc-911-system-troubled-article-1.1765475.

[155] S. Shyman Sunder, "NIST Response to the World Trade Center Disaster. World Trade Center Investigation Status," NIST, October 19, 2004, https://www.nist.gov/sites/default/files/documents/el/disasterstudies/ncst/NCSTACWTCStatusFINAL101904WEB2.pdf.

on the outside who could see the unfolding disaster were unable to communicate the building status to their cohorts on the inside. According to one of the FDNY chiefs at the scene, "People watching on TV certainly had more knowledge of what was happening a hundred floors above us than we did in the lobby. ... Without critical information coming in ... it's very difficult to make informed, critical decisions."[156] The lack of effective communication and situational awareness would ultimately prove catastrophic.

Traditionally, LMR systems were used to provide situational awareness during critical incidents. After the WTC bombing in 1993, the Port Authority Police Department (PAPD) of New York and New Jersey placed radio communication repeaters in the structures to enhance FDNY's communications network in the buildings. However, on September 11, the repeaters appeared not to be working properly, so the FDNY North Tower Command decided not to use them for transmitting the evacuation order after the South Tower collapsed.[157] NIST's investigation found that "emergency responders working inside of the WTC buildings who could not see what was happening outside and had good radio communications had better situational awareness than those with poor radio communications."[158] This was evident by the NYPD Emergency Services Unit members in the North Tower who received and acknowledged evacuation orders via LMR from commanders who were outside the buildings and witnessed the South Tower collapse.[159]

The first responders to the WTC attacks indicated that call volume and interference of the operating environment created communication problems on local LMR systems.[160] NIST research indicates that immediately after the North Tower was struck by the commercial aircraft, radio traffic increased to five times above normal levels. The increase in radio traffic led to roughly one-half of the voice transmission

---

[156] National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, 298.

[157] Ibid.

[158] Sunder, "NIST Response to the World Trade Center Disaster."

[159] National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, 310.

[160] Sunder, "NIST Response to the World Trade Center Disaster."

coming through incomplete or difficult to understand.[161] Such disparity in communication diminishes the situational awareness of first responders and compromises commanders' decision-making.

In response, NIST has made the following recommendations regarding communications interoperability and enhanced situational awareness. According to NIST, public safety communication networks should have:

- an overall network architecture that covers local networking at incident sites, dispatching, and wide-area urban and rural networks
- scalability in terms of the number of first responders using it that can provide radio coverage in challenging radio environments
- interoperability with existing legacy emergency communication systems
- localization techniques to identify first responders within indoor building environments[162]

NIST has recently acknowledged that LMR systems will be replaced by advances in LTE broadband networks over the next twenty years.[163] Private sector communications networks have proven capable of meeting the emerging needs of data, geo location, still imagery, and video of first responders. This situational awareness–supporting information is essential for enhancing the decision making of first responders. To support the migration to LTE networks from LMR, NIST is also exploring technology that allows this capability to work in environments where broadband networks are limited. NIST is developing the Rapidly Deployable Public Safety Research Platform, which can enable more than 200 smartphones, data terminals, and LMR systems to support communication among public safety members.[164] This system will allow mobile

[161] Ibid.

[162] Ibid.

[163] Ryan Felts et al., *Location-Based Services R&D Roadmap* (NIST Technical Note 1883) (Boulder, CO: Department of Commerce Boulder Labs, May 2015), http://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1883.pdf.

[164] "NIST's Rolling Wireless Net Helps Improve First Responder Communications," NIST, August 10, 2016, https://www.nist.gov/news-events/news/2016/08/nist's-rolling-wireless-net-helps-improve-first-responder-communications.

devices and their applications to function in austere environments where communications and broadband wireless are limited.

A. PROGRAM EVALUATION: NYPD MOBILITY INITIATIVE

The NYPD has recently spent $160 million on its Mobility Initiative, which has issued over 36,000 mobile devices to police officers. The devices use proprietary mobile applications to allow officers to be "better prepared than in the days when all their information came from a radio dispatch."[165] The mobile applications allow the device to access the agency's records, thousands of cameras, and gunshot detectors, which enhance officer situational awareness.[166] However, this proprietary technology is only available to members of the NYPD and not the other first responders in the city. This could be problematic should another large-scale event such as the recent attacks in Paris take place in New York.

The members of the NYPD have used their issued mobile devices and proprietary applications extensively since their deployment in 2013. The most-used application on the device is the 911 app. This app provides the officer operational information that would normally be announced over the agency's LMR systems.[167] There are many benefits to transmitting critical incident information via text format. Essential information such as addresses and suspect descriptions are provided directly to the officer for his or her review and clarification as needed. This detailed situational awareness can increase the safety for officers and lead to faster response times.[168] Furthermore, this allows officers to take the information obtained from the dispatcher and directly populate their reports, reducing administrative time and allowing the officer to spend more time in the community.

---

165 Gary Silverman, "New York's Top Cop Embraces Smartphone Revolution," *Financial Times*, June 5, 2016, http://www.ft.com/cms/s/0/ea90e172-29c9-11e6-8ba3-cdd781d02d89.html#axzz4K0iZHnjc.

166 Ibid.

167 Susan Crawford and Laura Adler, *Culture Change and Digital Technology: The NYPD under Commissioner William Bratton, 2014–2016* (Research Publication No. 2016-13) (Cambridge, MA: Berkman Klein Center, 2016), 40.

168 Ibid., 24.

The NYPD uses a proprietary app called "Finally, One Record Management System" (FORMS) to help officers complete their reports in the field on their smartphone or tablet.[169] Access to the 911 app and FORMS requires officers to enter a personal identification number (PIN) and swipe a card for every four hours of use. Unfortunately, smaller agencies cannot afford proprietary applications that provide this level of security and access to agency records management systems. However, off-the-shelf apps, such as Crime Scene Tracker, are being developed to allow officers to collect and share information in the field and add to records management systems later at the station.[170]

NYPD's proprietary application, Crime Information Center, allows secure methods for members of the agency to promote situational awareness. On February 9, 2016, members of the NYPD used the application to share a flier of a suspect who had been exposing himself on the city's subway system. Several members of one precinct recognized the suspect as someone they had recently encountered. Due to the immediacy of information-sharing through the mobile device, the officers were able to go to the hospital where the suspect was being treated and take him into custody before he was discharged.[171]

The NYPD's messaging application is very unique in its ability to distribute messages among members of the department. The application can create message groups based on a user's temporary assignment, precinct, rank, or location. This application will allow officers to immediately communicate with other officers from different assignments that arrive at the scene. Recently it has been used effectively for pre-planned events, such as the 2016 Thanksgiving Day Parade, and emergent events, such as the September 2016 bombing in New York City's Chelsea neighborhood.[172]

---

[169] Ibid., 40.

[170] "Crime Scene Tracker," Google Play, accessed December 9, 2016, https://play.google.com/store/apps/details?id=de.crimescenetracker&feature=also_installed#?t=W251bGwsMSwxLDEwNCwiZGUuY3JpbWVzY2VuZXRyYWNrZXIiXQ.

[171] "NYPD Smartphones Help the Finest Arrest Man Wanted for Lewdness on Subway," *NYPD News*, February 9, 2016, http://nypdnews.com/2016/02/nypd-smartphones-help-the-finest-arrest-man-wanted-for-public-lewdness-on-subway/.

[172] Alfred Ng, "This is NYPD's New Crime Fighting Phone," CNET, October 13, 2016, https://www.cnet.com/news/nypd-new-york-police-official-crime-fighting-windows-phone/.

NYPD is also using the smartphone as a means to deliver training to its personnel. The program, NYPD University, allows police officers to view training videos and other learning materials while in the field. They can also use the device to take quizzes to ensure comprehension of the learning material.[173] Prior to this breakthrough, officers would have to attend in-service training at the department's academy in Queens. With a department of more than 36,000 members, this was not very cost effective and removed patrol units from the streets. Mobile applications to facilitate training increase the member's time in the community while meeting the complex training demands of one of the nation's premier policing agencies.

In addition to using its proprietary mobile applications, the NYPD has also had great success in using off-the-shelf mobile applications on agency-issued mobile devices. Patrol officers now have an issued device that can facilitate direct communication with the community. Off-the-shelf mobile applications, such as Twitter and Facebook, are being used more frequently by the department to enhance community relations at times when police–community relations are strained. Referencing community relations prior to the Mobility Initiative, one senior officer stated, "We did a great job at communicating at the public, but we'd never, in my opinion, done an effective job of communicating with the public."[174] Officers who use these applications in the field can share information with the public on suspect information and critical incidents. The Boston Police Department's use of Twitter during the hunt for the Boston Marathon Bombers in 2013 identified the utility of these applications for first responders. With effective trust-building through social media prior to the bombing, the department was able to communicate accurate information with the public on the investigation and subsequent manhunt.[175]

Communication with the public during critical incidents is essential for homeland security. However, this can be particularly challenging in diverse areas such as New York

---

[173] Ibid.

[174] Crawford and Adler, *Culture Change and Digital Technology*, 25.

[175] Edward F. Davis III, Alejandro A. Alves, and David Alan Skalansky, "Social Media and Police Leadership: Lessons from Boston," *New Perspectives in Policing*, March 2014, https://www.ncjrs.gov/pdffiles1/nij/244760.pdf.

City, where 28 percent of residents do not speak English at home.[176] In November 2016, Patrolman Krystopher Valentin was standing post on the New York City Marathon route when he observed a Paralympian in distress on the course. The wheelchair-bound athlete, Zou Lihong, only spoke Chinese and was unable to communicate with the officer. The officer opened a language translation application on his department-issued mobile device. Through an off-the-shelf application he was able to successfully communicate with the athlete and address her concerns.[177]

A recent study by NIST identified that many first responders carry smartphones for personal and professional use. First responders to Hurricane Katrina in 2005 acknowledged that their cell phones were their primary form of communication.[178] Whether personally owned or agency issued, mobile devices and applications are used to support enterprise communication and geo-locate resources in a variety of environments. NIST acknowledges a "lack of detailed procedures and methods for gathering, processing, and delivering situational information to all first responders."[179] Improved procedures and methods could incorporate off-the-shelf mobile applications standardization to ensure interoperability among the various disciplines of homeland security. These standards would need to be integrated into the National Incident Management Systems (NIMS) to ensure that standards among first responders are established before agencies proceed with technology procurement and policy development strategies.

B. HOW MOBILE DEVICES MAY HAVE IMPACTED THE SEPTEMBER 11 RESPONSE

Deputy Chief Joseph Pfeifer, a September 11 first responder and graduate from the Naval Postgraduate School's Center for Homeland Defense and Security (CHDS) program, has learned firsthand that severe consequences can develop if agencies such as

176 "New York: Languages," City-Data, accessed February 19, 2017, http://www.city-data.com/states/New-York-Languages.html.

177 "Officer Uses Smartphone," *NYPD News.*

178 Farnham, Pedersen, and Kirkpatrick, "Observation of Katrina/Rita Groove Deployment," 41.

179 Sunder, "NIST Response to the World Trade Center Disaster."

the NYPD and FDNY do not share situational awareness.[180] While the attacks of September 11, 2001, have resulted in many effective changes in the organization structures of first responders and intelligence-sharing, gaps still exist in situational awareness sharing. Off-the-shelf mobile applications represent a cost-effective and efficient means to enhance interagency collaboration. Research indicates that many off-the-shelf mobile phone applications demonstrate a high degree of acceptance by mobile phone users.[181] These applications may represent the mechanism for bottom-up collaboration among first responders.

Off-the-shelf mobile applications such as WhatsApp and GroupMe are very effective for developing self-organized information-sharing networks. Smartphone ownership by adult Americans is greater than 66 percent of the population.[182] Users' ability to download simple applications on these devices may prove effective at enhancing the relationships of first responders. Messaging app GroupMe was put to use, for example, on the first day of the CHDS master's program for the 1505/1506 cohort. This free mobile app allowed the diverse members of the class to share information critical to the educational process. Deadlines for papers and project status were shared and referenced on the app, along with situational awareness information related to critical incidents in classmates' jurisdictions.

Mobile applications alone will not enhance first responder relationships. Effective policy must be in place to ensure that participants remain respectful of one another while using these applications. As demonstrated in the 2016 presidential election, mobile applications such as Twitter can be very divisive to relationships. Policy that is comprehensive for these platforms, with appropriate consequences for violations, will be essential to ensuring they are a viable mechanism for situational awareness information-sharing. If these tools are used improperly further division between agencies can be realized. An asset to situational awareness can be perceived as a liability.

---

[180] Joseph Pfeifer, "Understanding How Organizational Bias Influenced First Responders at the World Trade Center," in *Psychology of Terrorism*, eds. Bruce Bongar, Lisa Brown, Larry Beutler, James Breckenridge, and Philip Zimbardo (New York: Oxford Press, 2007), 211.

[181] Smith, "The Smartphone Difference."

[182] Ibid.

To ensure that these tools are used effectively, training and exercises should be established between agencies. Exercises will prove the value of the technology and identify challenges. By taking the time to examine these options prior to the next critical incident, users will have greater acceptance of these tools when they are truly needed. CHDS graduate and FDNY Firefighter Sean Newman posits that "group bias will never be eradicated, but it can be transferred. As the research shows, participants that train and work together, sharing a common identity, will form that critical primary bond, but simply working closely together on a regular basis is just one of the triggers to promote cohesion."[183] Communicating through mobile applications in the training environment may engender better relationships during critical incidents.

Newman acknowledges that disparate agencies need to work together on a regular basis in order to promote cohesion. Community-building approaches with clear, consistent lines of communication are essential to diminishing any barriers to cooperation. Through off-the-shelf mobile applications, these agencies can have a platform to share organizational activities at pre-event status. This communication line can be strengthened through inter-agency training and exercise. With the aid of these tools, critical incident response will be more effective as the agencies will have the ability to communicate situational awareness to one another on a secure platform.

Chief Pfeifer confirms the need for first responders to develop innovative thinking to establish effective lines of communication. He posits that emergency responders need to be "innovative at the desktop, as well as on the ground or during a firefight."[184] Off-the-shelf mobile innovations have the potential to enhance first responder missions. Israeli police have used mobile apps such as WhatsApp to provide situational awareness in critical incidents.[185] Unfortunately, terrorist organizations have also found these off-the-shelf mobile applications to be very effective at establishing secure information-sharing networks during their attacks. Newman and Pfeifer posit that we should learn

[183] Sean S. Newman, "Braving the Swarm: Lowering Anticipated Group Bias in integrating Fire/Police Units Facing Paramilitary Terrorism," (master's thesis, Naval Postgraduate School, 2011), 56, https://www.hsdl.org/?view&did=5482.

[184] Ibid., 42.

[185] Verhma, "What's Up in the Police Department?"

from their adaptation and innovation for agile response strategies. Agile approaches to communication are needed for taskforce organizational structures. These structures incorporate members from different agencies and disciplines to develop networked response groups. In the case of the FDNY and NYPD, these groups would work together to meet the challenges of attacks that could include a combination of firearms, smoke, fire, or explosives.

Networked command and information-sharing is essential to resolving large-scale incidents. Pfeifer stresses the need for this type of organizational structure at complex events such as the attacks on September 11.

> I've talked about network command, or the ability to connect the operations centers. So we have two things happening: the hastily-formed network at the scene, where responders need to figure out what to do, and talk about it, within the incident command structure. And then we have the ability for networks, or EOCs [emergency operations centers], to connect and to give a large picture of what's happening at the local scene. Without that, you are lost and will have no idea if it's one terrorist, or ten terrorists, or whatever the case may be.[186]

Off-the-shelf mobile applications may allow organizations such as the NYPD and the FDNY to collaborate and share situational awareness at critical incidents with little to no cost to the respective agency.

C. HYPOTHETICAL SCENARIO

A New York City Police officer is on patrol in Brooklyn, New York, on a Saturday afternoon in the spring. There is a report over the LMR from central dispatch indicating an explosion has just taken place outside Barclays Center on Atlantic Avenue. The officer is aware there is road construction in the vicinity blocking his ability to access the Center from his current location. He turns to his department-issued smartphone and, using the Waze application, he is able to find the most direct route to the location that avoids construction and other emerging traffic conditions. While en route, his partner opens his Periscope social media app and views live-streamed video from witnesses at the scene. Upon arrival, the officer posts a WhatsApp message indicating the geolocation

[186] Newman, "Braving the Swarm," 42.

of the incident command post he has established. Responding agencies from various disciplines of public safety—fire, emergency medical services, and law enforcement—acknowledge receipt of the location along with the officer's geo-tagged photos of the scene. Next Generation 9-1-1 also receives similar text and photo data from citizens in the area until the private cellular networks collapse due to volume. Fortunately, the first responders in possession of issued mobile devices are still operating on the cellular network, as FirstNet's public safety prioritization allows their devices to function despite the local cellular traffic increases.

The officer contacts a local trauma center and uses Apple's FaceTime app to conduct a live video call with a trauma physician, who assists with field triage. This physician receives situational awareness of the mass casualty incident and forwards information to other hospitals in the area. Additional officers at the scene attempt to locate witnesses and a tourist with pertinent information is identified but does not speak English. The officer downloads Google Translate onto his phone and is able to verbally communicate with the witness and obtain the description of a suspect. Using MIM app Telegram, the witness shares a video of a suspicious person placing a backpack in the area of the explosion. The officer is able to isolate an image of the suspect and distribute it to his local responder network as well as the regional fusion center for analysis. The suspect is located within minutes at another location and subdued before he can detonate another package in his possession. The officer searches the suspect and a letter written in Arabic is found in his pocket. The officer, taking the suspect into custody, then translates the document using Google Translate. The translated document reveals several locations within the area where suspicious packages are identified and rendered safe.

This imaginative scenario is one that could potentially play out in the very near future as all of these technologies are currently in service or in development. Government workers and first responders are using off-the-shelf mobile applications for both personal and professional uses, on personal and department-issued devices. However, little policy or uniformity exists in this area and consequently the behavior of the user as well as the mobile application could create complications for future use. It is essential that the

challenges, opportunities, and policies be examined to define this area before the next critical incident.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. OPPORTUNITIES AND CHALLENGES

Off-the-shelf mobile applications have demonstrated the ability to enhance private sector enterprise operations.[187] However, government agencies have been slow to adopt them. Steve VanRoekel, former U.S. federal chief information officer, identifies that, "For too long, the government has employed 20th-century tools to solve 21st-century problems. We fell behind in making smart investments in technology that yield productivity gains in the private sector every day."[188] There are a variety of factors that contribute to this deficit, but there are also many reasons to overcome these challenges and adopt off-the-shelf mobile applications for situational awareness. This chapter identifies the opportunities and challenges associated with homeland security's adoption of these technologies.

A. OPPORTUNITIES

1. Cost Effectiveness

The demand for mobile applications is growing exponentially. These simple software programs allow mobile devices to engage the user in activities previously relegated to desktop computers. Mobile devices allow the user remote access to stored information and enhance productivity at work. The rapid growth in this market has led to multiple applications competing for customers. Innovative application developers are offering a variety of programs that meet diverse organizational and individual needs to expand their share of the market. Low-cost or free off-the-shelf mobile applications may be able to support situational awareness for first responders.

Developing a proprietary enterprise solution can be cost prohibitive. The NYPD has deployed a mobile situational-awareness platform costing more than $160 million.[189] While the program is very progressive and meets the situational awareness needs of the

[187] William D. Eggers and Joshua Jaffe, "Gov on the Go," Deloitte University Press, February 19, 2013, https://dupress.deloitte.com/dup-us-en/industry/public-sector/gov-on-the-go.html#endnote-16.

[188] Ibid.

[189] City of New York, "Press Release from the Office of Mayor Bloomberg."

department, most police agencies in the United States do not have the funding to support such a program. As an option to achieve enterprise connectivity, homeland security agencies can turn to low-cost off-the-shelf solutions to meet their situational awareness needs.

2. Frugal Information Systems

Resource-constrained enterprises are turning to frugal information systems to meet customer needs. Frugal information systems support agency needs by reusing existing infrastructure. For any frugal IS to be successful, it must meet four information drivers of the consumer. These drivers, referred to as U-constructs, include ubiquity, uniqueness, unison, and universality.[190] Ubiquity represents the user's ability to access information, anytime, anyplace. Americans expect access to information wherever they are. Smartphones allow users to communicate, access the Internet, and use mobile apps for professional and personal needs. Seventy-two percent of U.S. citizens report owning a smartphone.[191] This high degree of acceptance facilitates the use of mobile devices and applications in innovative ways to meet business and personal needs.

Uniqueness refers to knowing an individual's identity and location. This is accomplished using the GPS, sensors, and unique identifiers within a smartphone. This element is important for homeland security practitioners for purposes such as "blue force tracking," or knowing where friendlies are located. It is also important to have situational awareness of the location and status of an unfolding event. Spatial context is essential information for effective situational awareness.

Unison refers to information consistency or the democratization of data. All members engaged in a critical incident should have real-time access to information. This information includes, but is not limited to, the geo-location of assets, condition of those

[190] Richard Wilson, K. Kunene, and Sirajul Islam, "Frugal Information Systems," *Information Technology for Development* 19, no.2 (2013): 178, http://dx.doi.org/10.1080/02681102.2012.714349.

[191] Jacob Poushter, "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies," Pew Research Center, February 22, 2016, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-Internet-usage-continues-to-climb-in-emerging-economies/.

assets, and status of the event. Conflicting information can result in confusion, indecision, and time wasted resolving differences.[192]

Universality represents the ability of the application to overcome information-system incompatibility. Wilson, Kunene, and Islam posit that "a frugal IS must be compatible with existing systems so that it does not add to the incompatibility problem."[193] The authors indicate that smartphones are an "obvious delivery platform" for information services due to the interoperable design of the devices.[194] Off-the-shelf mobile applications are specifically designed to reach as much of a customer base as possible and, in turn, disparate devices and operating systems.

Proponents of frugal information systems have made recommendations for their procurement. First and foremost, system designers need to have very low limits on spending to accomplish their objectives. Open-source software should serve as a default choice when available. These applications are typically free and demonstrate more "universality" than proprietary programs.[195] Applications that are already in participants' possession should also be given priority. In this case, the near-universal acceptance of the smartphone as an enterprise solution should be leveraged. Crowd-sourcing the most accepted applications is effective in highly constrained environments such as government enterprises. Frugal IS proponents recommend using interns, students, and new employees to aid in developing software programs. These individuals are not encumbered by assumptions of how to acquire and develop a software solution. Furthermore, presuming that they are less affluent, these individuals tend to have experience working in resource-constrained environments.[196] Short deadlines should also be set in order to deliver the system sooner rather than later. Delays that would inhibit the program's acceptance can be overcome if information specialists are frugal with time. Finally, to send a positive

[192] Wilson, Kunene, and Islam, "Frugal Information Systems," 178.

[193] Ibid., 179.

[194] Ibid.

[195] Ibid., 180.

[196] Ibid., 181.

message to employees, any savings achieved through these measures should be celebrated by management.[197]

Consultants such as XMR Fire Emergency Services Consulting are assisting public safety agencies in procuring and deploying low-cost off-the-shelf mobile applications to support operations.[198] For limited fees, a consultant provides support services, training, security management, storage backup, and mobile-device management to the agency. The company deploys a suite of Google apps, including Gmail, Google Calendar, Google Drive, Google Docs, and Hangouts, a messaging application, to support agency operations. The agency commits to securing and preserving the user's data through the use of open application program interfaces to migrate the data should the user terminate service.

3. Communication Options

Smartphones provide a variety of methods for groups to communicate situational awareness. Mobile phones were originally designed solely to make phone calls, but other forms of communication through the device have been gaining in popularity. Texting is one such communication method. Ninety-six percent of smartphone users "text."[199] While people primarily use texting for personal use, 70 percent of employees feel that their companies should use texting to communicate. Further, almost 75 percent would prefer it over phone calls for crisis communication.[200]

Text messages use the cellular network–based SMS to transmit messages and photos to other users. Recently, native smartphone SMS messaging applications have evolved to transmit audio, video, and even the location of users. These added capabilities have led to Americans spending about twenty-six minutes a day texting.[201]

---

[197] Ibid.

[198] "Google Apps," XMRFire, accessed November 8, 2016, http://www.xmrfire.com/services/google-apps-for-fire-and-ems.

[199] Kujowski, "Text Messaging vs. Mobile Instant Messaging."

[200] "SMS Communication in Business," Vitiello Communications Group, October 14, 2010, http://vtlo.com/blog/sms-communication-in-business-2/.

[201] Corilyn Shropshire, "Americans Prefer Texting to Talking, Report Says," *Chicago Tribune*, March 26, 2015, http://www.chicagotribune.com/business/ct-americans-texting-00327-biz-20150326-story.html.

Unfortunately, there is limited research that identifies how frequently first responders use SMS messaging systems for situational awareness. However, corollaries can be drawn from the public's use of these applications.

Collaboration software applications for information-sharing are on the rise among mobile phone users. Ninety-eight percent of texts are read, as opposed to 22 percent of emails, 29 percent of tweets, and 12 percent of Facebook posts.[202] Text messaging on mobile phones also has immediate connectivity to the recipient. Ninety-one percent of Americans keep their mobile devices within reach, and almost all of these devices are SMS enabled. Most text messages receive responses within ninety seconds, while email can take up to ninety minutes.[203] This communication system has proven very reliable to citizens; however, there may be complications related to first responders using texting for homeland security functions.

One of the concerns regarding first responders' increasing use of messaging applications for situational awareness is record retention. Policies related to text-message retention on agency devices are only recently being addressed. In the State of Washington, public service agencies are responsible for retaining messages related to government business.[204] Phone companies comply with their own retention policies and/or those that are established contractually with the customer. If a public service agency does not obligate the provider to retain text-messaging records, the agency must ensure these messages are retained and compliant with records policies. Fortunately, there are a few options for agencies to record this data. The user can manually save text messages to an agency-controlled storage device such as an enterprise content management system or server. A second option is configuring the text message service, or third-party software, to automatically record each text sent and received. This data can be stored remotely or sent regularly as an email to the agency. As a third option, an

---

[202] Ibid.; Kujowski, "Text Messaging vs. Mobile Instant Messaging."

[203] Melani Deyto, "6 Benefits of Text Messaging: Why Your Organization Should Use SMS," *Textmarks*, February 18, 2015, https://blog.textmarks.com/benefits-of-text-messaging/.

[204] "Records Management Advice," State of Washington, April 2015, https://www.sos.wa.gov/_assets/archives/RecordsManagement/Advice-Sheet-Capture-and-Retention-of-Text-Messages-April-2015.pdf.

agency can have a vendor capture and store public-record text messages that are compliant with agency retention policies.[205]

MIM systems such as WhatsApp can store messages in the cloud or on the user's device.[206] These mobile applications are designed for collaboration and allow the user to reference the group's dialogue as needed. This collaboration could include, but is not limited to, images, text, video, and documents that were previously transmitted through the application. This is essential when attempting to maintain situational awareness during dynamic critical incidents. A "be on the look-out" (BOLO) flyer of a suspect transmitted through the application is one example. The ability to query and reference reports such as this is essential to maintaining effective situational awareness. These images and other situational awareness data will need to be preserved to comply with the agency's records retention policies. MIM applications like WhatsApp may facilitate this function through cloud-based servers.

B. CHALLENGES

1. How Free Are Free Apps?

To generate revenue in this competitive market, app designers are utilizing one of four options. The first is one-time pay apps that allow the user to purchase the application from an app store with the expectation that updates and upgrades are free. Some one-time pay apps require the user to pay for upgrades that meet evolving needs. Others enable automatic updating for free for security and performance. "Freemium" applications, or free apps, are a second option; they pose no cost to the user but have limited features. If desired, the user can pay for upgraded features. Free apps with advertising imbedded in them are a third option. When these apps are used, a banner or pop-up advertisement reveals itself to the user. The advertiser compensates the app developer for every download that exposes the product to a user. Finally, there are free apps that do not have pop-up advertisements, but that share the user's data with third parties; these seem to be

[205] Ibid.

[206] Elissa Loi, "26 WhatsApp Features You Didn't Know You Had, Let Alone Could Use," *Stuff*, March 30, 2016, http://www.stuff.tv/sg/features/19-whatsapp-features-you-might-not-be-aware.

the most popular form of application monetization. These monetization processes are so popular that 90 percent of apps in use are available for free in app stores. More than 50 percent of the tops twenty-five apps are free.[207]

The data acquired by the application developer are highly coveted by marketing companies that want to understand user interests. Data can be directly extracted from the device without the user knowing it. The app purchaser agrees to provide the developer access to the data through the terms of service for the application. Unfortunately, a third party's access to the data on the device can inhibit its performance. Data transmission that is not essential can encumber the device's power, memory, and processing speeds, which may be needed to support other essential functions.

A recent study in the *ACM SIGMOBILE Computing and Communications Review* focused on smartphone app "overheads," or data traffic that was not related to the application itself.[208] Zhang, Gupta, and Mohapatra classified these overheads into two categories: advertisements and analytics.[209] Advertisements represent text, images, audio, or videos that appear while the application is in use, unrelated to its function. Analytics refer to data forwarded to a third-party server to analyze app popularity or user behavior. Neither of these functions is needed for the app to perform, but this is one of the methods for-free application developers use to generate revenue. Unfortunately, this activity on the mobile device can consume the user's data and inhibit the normal performance of the device. Incurring high fees for exceeding a user's data limits can make free smartphone applications a costly endeavor.

Overhead activity by off-the-shelf mobile applications can impair device performance. The device's battery is drained as these unnecessary functions work in the background of the mobile device.[210] The additional drain on the device's battery can be very problematic to the homeland security user during critical incidents. Research

[207] Mythreyi Velury, "A Report on the 'Methods Used by Free Apps to Earn Revenue and its Increasing Popularity," *Imperial Journal of Interdisciplinary Research* 2, no. 4, (2016): 345.

[208] Li Zhang, Druv Gupta, and Prasant Mohapatra, "How Expensive Are Free Smartphone Apps?" *ACM SIGMOBILE Mobile Computing and Communications Review* 16 no. 3, (July 2012), 20.

[209] Ibid., 21.

[210] Ibid., 22.

indicates that 77 percent of the top free apps download data via third-party ads.[211] Unfortunately, these ads can consume a remarkable amount of energy. Researchers estimate 65 to 75 percent of the battery can be needed for the advertisement itself.[212] Homeland security professionals working in an austere environment need their devices to perform efficiently during prolonged events. If an agency employs a free off-the-shelf mobile application to support situational awareness, power management is essential to the performance of first responders.

Privacy issues also abound with the use of free apps. Grace et al. examined a series of Android applications to identify what data is being collected by application developers. The developers targeted the phone's international mobile equipment identifier, user's location, accounts, contact list, and camera information.[213] This information would be considered sensitive data to most homeland security users. However, the developer may be able to access this data if the user agrees to the terms and conditions for the use of the mobile application. Unfortunately, users rarely read the fine print on these terms of service and readily accept them without considering the consequences.[214]

When one considers the impact overhead traffic has on the user's device, it appears that free apps are not really free. Given the excessive data and power consumption as well as diminished performance of the device, a free application can cost as much as thirteen times more than a similar purchased app.[215] While there may be an initial cost savings associated with adopting these applications as an enterprise solution, the impact these background activities have on the device can lead to decreased

---

[211] I. Leontiadis et al. "Don't Kill My Ads!: Balancing Privacy in an Ad-Supported Mobile Application Market," *Proceedings of the Twelfth Workshop on Mobile Computing Systems* 12, no. 2 (2012).

[212] A. Pathak, Y. C. Hu, and M. Zhang, "Where Is the Energy Spent inside My App?" *Proceedings of the 7th ACM European Conference on Computer Systems* 12 (2012).

[213] M. C. Grace, W. Zhou, X. Jiang, and A.-R. Sadeghi. "Unsafe Exposure Analysis of Mobile In-app Advertisements," *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, 12 (2012).

[214] "Why Do We Blindly Sign Terms of Service Agreements?" NPR, accessed November 13, 2016, http://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements.

[215] Ibid.

performance during critical incidents. Homeland security agencies that employ them will have to examine the risks vis-à-vis the rewards.

2. Mobile Communications for Situational Awareness Survey

One concern of enterprise communication programs is the lack of issued mobile devices for first responders. A recent survey was conducted in Washington State to gauge public health employees' interest in using personal devices for business-related notifications. The evaluation was initiated in the fall of 2011 to determine if an opt-in, employer-based texting program would be acceptable by the staff.[216] Out of 1,536 employees, only 828 responded to the emailed survey to gauge interest in participating in the program. The survey revealed that the employees were interested in emergency and site closures, which would improve their situational awareness. The survey also revealed that older users were less interested in the text messaging service than younger users. However, all users identified significant concerns related to receiving messages from their employer.[217] Nearly one-third, or 238, of the employees who participated in the survey indicated that they would likely participate in the program. Of this result, 51 percent of respondents aged 18–29 advised that they would be willing to participate, whereas only 18.5 percent of respondents aged 60 years and older were willing. This data is consistent with other research on the acceptance of smartphone technology by Americans aged 65 years and older.[218]

To recruit volunteers for the survey, an email was sent to the public health employees of a county in Washington State. The email indicated that the program was voluntary—with opt-out at any time—limited to emergency communications, had no accountability for information received, and guaranteed the user's phone number would not be shared. Only 22.7 percent of the 1,536 employees signed up by December

---

[216] Hilary Karasz, Sharon Bogan, and Lindsay Bosslet, "Communicating with the Workforce during Emergencies: Developing an Employee Text Messaging Program in a Local Public Health Setting," *Public Health Reports* 129, Supp. 4 (2014): 62.

[217] Ibid.

[218] Aaron Smith, "Older Adults and Technology Use," Pew Research Center, April 3, 2014, http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/.

2011.[219] In January 2012, a winter storm struck the county where the study was conducted. One-third of homes lost power, and many of the area roads were unsafe due to snow and ice-related conditions. Several of the health clinics participating in the study lost power for up to four days. The emergency notifications were sent via text to participants in the program. The feedback from the respondents was positive, with only 5 percent of respondents reporting the program as "not helpful." Seventy percent learned at least one piece of information before receiving it later through other communications means such as an agency website, email, or hotline. During the five-day weather event, 165 additional employees subscribed to the program. Comments from employees indicated that the messaging system was very helpful to those who had lost power and were unable to access email and the Internet.[220]

Updates in mobile device contracts may impact the data of similar studies in the future. At the time of the Washington State study, the majority of cellphone data plans had contractual limitations on the number of text messages. If those limitations were exceeded, charges would be incurred by the phone's owner. Fifty-six percent of the staff surveyed for this program indicated that cost associated with text messages was a limiting factor related to their decision to opt into the program.[221] Currently, there has been an increase in the number of unlimited text messaging plans. A recent survey indicates that almost 90 percent of Americans have unlimited texting.[222] The immediate situational awareness provided by programs such as this would likely increase the participation of those in the messaging program. The ubiquity of Wi-Fi would also add to the participation of members who use MIM programs. Those who are concerned about saving data will benefit from the increasing availability of free Wi-Fi connectivity and more affordable data plans.

---

[219] Karasz, Bogan, and Bosslet,"Communicating with the Workforce," 64.

[220] Ibid.

[221] Ibid.

[222] Josh Zagorsky, "Almost 90% of Americans Have Unlimited Texting," *Instant Census*, December 8, 2015, http://instantcensus.com/blog/almost-90-of-americans-have-unlimited-texting.

The Washington State study reveals that the program coordinators should have been more effective in communicating the mobile service to the employees. Unfortunately, it took an extreme weather event for the staff to appreciate the value of the program to enhance their situational awareness of the work environment. Agencies that develop messaging programs for employees' personal mobile devices should clearly identify the value of opting in for situational awareness and solicit the employees' opinions in the development stage. This will likely enhance participation in the program at the outset.

3. User Acceptance

Even with effective communication, individual users may be reluctant to embrace free off-the-shelf mobile applications that access too much personal information. A recent Pew Research Center survey revealed that 60 percent of mobile phone users who regularly download apps refuse to install apps that require excessive personal data.[223] The average app that was examined in this study required five permissions before a user installed it. Unfortunately, communication apps, which could enhance situational awareness, tend to require the most permissions to function. Ninety percent of the app downloaders surveyed identified their personal data as a concern when deciding to download an app.[224] This concern can inhibit participation in communication application downloading. Any requirements for downloading the application must be articulated to the user, in addition to the service it will provide the user and the agency.

Approval from other users can enhance acceptance of situational awareness applications. A recent Pew Research Center study identified that 57 percent of app downloaders feel that it is important to know how many times an app has been downloaded. Further expanding user acceptance is the user's app rating in the app store. A recent survey by Apptentive, a company that builds mobile engagement software, revealed that 92 percent of consumers feel the online app store rating for a mobile app

[223] Kenneth Olmstead and Michelle Atkinson, "App Permissions in the Google Play Store," Pew Research Center, November 10, 2015, http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/.

[224] Ibid.

influences their decision to download. Ninety-six percent of those surveyed would consider downloading an app with a 4 stars out of 5 rating, whereas only 50 percent would consider a 3 star–rated app.[225]

MIM is gaining the interest of mobile device users, as it offers more capabilities than standard texting. MIM uses the Internet to transmit messages and information to other users that are not available under SMS instant messaging formats. MIM users do not have to use cellular data if free Wi-Fi is available to send messages. This messaging began to gain high levels of acceptance due to the increasing availability of free Wi-Fi around the world. Consequently, in 2013, more WhatsApp messages were sent globally than all SMS messages put together.[226]

4. Agency Acceptance

Security is a major concern for any public safety agency that uses digital communications. MIM systems tend to have more encryption and security than standard SMS messaging systems. Messaging systems such as Telegram use advanced encryption methods to keep users' information secure. The company is so confident in its security that it has offered $300,000 to anyone who can hack the app.[227] This is an important consideration for homeland security agencies, which may have to transmit sensitive information.

MIM systems have the ability to connect with other users securely through two methods. Messaging apps such as WhatsApp, Telegram, and WeChat use embedded client or software connections that are specific to the device.[228] The programs downloaded to the device establish the ends of the encryption chain that even prevent the service provider from seeing the information transmitted. Some apps use clientless platforms that are browser based. These apps do not download any software onto the

---

[225] Ayaz Nanji, "How Influential Are Mobile App Star Ratings," MarketingProfs, May 22, 2015, http://www.marketingprofs.com/charts/2015/27665/how-influential-are-mobile-app-star-ratings.

[226] Ibid.; Kujowski, "Text Messaging vs. Mobile Instant Messaging."

[227] Rahil Bhagat, "5 Reasons You Might Want to Switch From WhatsApp to Telegram," *Stuff*, May 11, 2016, http://www.stuff.tv/sg/features/5-reasons-you-might-want-switch-whatsapp-telegram.

[228] Ibid.

device.[229] Similar to email accounts, users can access the application from any network or device provided they have the right login credentials and browser. This is beneficial for users who want to access the application via a desktop computer.

MIM systems can share information in a variety of ways. Most MIM systems use the Internet to communicate with other users. Mobile device users are cognizant of the data they consume while using their mobile device on cellular networks. The ubiquitous availability of free Wi-Fi allows users to use MIM systems to communicate with friends and save contractually established data for other functions. This secondary means of data transmission can also ensure that the user will not be prevented from transmitting messages when cellular networks are compromised by excessive traffic. This frequently occurs during critical incidents, when citizens are attempting to contact emergency services or loved ones, and can disable first responder cellular network devices. If the user can access Wi-Fi, the first responder can continue to transmit messages over this platform independent of cellular networks.

The capability of MIM systems to share diverse pieces of information such as documents, live video feeds, and other media is remarkable. As such, some feel that social networking software such as Slack and WhatsApp are poised to replace email. This type of social collaboration software is proving to be more efficient in the work environment. These programs reduce the time workers spend checking email, and provide for more meaningful collaboration and transparency.[230] All of these factors would prove valuable to enhancing first responders' situational awareness.

5. Implementation Challenges

Research indicates that government agencies struggle to implement new technology for a variety of reasons. Government procurement processes tend to work against the efficient adoption of technology due to complex, costly, and lengthy

[229] Ibid.

[230] Tim Eisenhauer, "7 Reasons to Replace Email with Collaboration Software," Axero, accessed December 11, 2016, https://axerosolutions.com/blogs/timeisenhauer/pulse/167/7-reasons-to-replace-email-with-collaboration-software.

procedures.[231] In many cases, new technologies mature faster than the procurement cycle and the delivered technology tends to be outdated. Other factors contribute to delays in the procurement process. The public budgeting process is deliberate and spending plans discourage innovative thinking and adaptable spending. The New Jersey State Police spent eighteen months procuring Digital Sandbox DS7, a software as a solution (SaaS) product for situational awareness. The program required many layers of review prior to its delivery one month before the 2014 Super Bowl held in MetLife Stadium in East Rutherford, New Jersey. Unfortunately, the product was not available when Superstorm Sandy made landfall in October 2012. The program would have been valuable in supporting rescue operations.

Further complicating the information technology procurement is the support staff needed for technology. Public sector salaries generally lag behind the private sector, meaning the best IT personnel do not gravitate to government service. Oftentimes government employees with little interest in the discipline can be promoted into critical positions, further impeding progressive procurement. Unfortunately, the pace of change in technology continues to accelerate while government processes tend to get worse.[232] Policy that permits aggressive procurement of affordable off-the-shelf applications can overcome some of these barriers.

Organizational Strategist Rick Maurer reports that 70 percent of all major changes inside an organization, including the integration of new software systems, fail.[233] Rogers points out that the failure to adopt innovations can result from cultural barriers to change, weak innovation, competition from other innovations, or lack of awareness. These failures can result in missed opportunities that have financial impacts or impede an organization's advancement. There are numerous examples of private and public sector

---

[231] Mark Headd, "Built to Fail: Why Governments Struggle to Implement New Technology," GovLoop, June 23, 2014, https://www.govloop.com/community/blog/built-to-fail-why-governments-struggle-to-implement-new-technology/.

[232] Ibid.

[233] Rick Maurer, "Getting beyond the Wall of Resistance," *StrategyDriven*, July 19, 2010, http://www.strategydriven.com/2010/07/19/getting-beyond-the-wall-of-resistance/.

agencies that failed to embrace change, which led to catastrophic results.[234] Gilley, Godek, and Gilley point out that much of the resistance to technology adoption can be overcome through effective leadership, employee involvement, and effective communication.[235]

6. Overcoming Implementation Challenges

Gilley, Godek, and Gilley feel that effective leadership is fundamental to an organization embracing a change such as mobile application adoption. Strong leadership is needed "to emphasize the common purpose across organizations, and help the organization piece together how they will accomplish these goals."[236] Incentives, stress management, and negotiation may be needed to facilitate technology adoption and sustainment. Gradual implementation of these approaches, starting with small test groups, will also aid in the process. Incremental changes are perceived as "more manageable, less threatening, and easier to integrate into existing processes."[237]

Research suggests that employee involvement in the early stages of integrating a change is essential to overcoming barriers to adoption. By integrating employees early on, psychological ownership of the change is engaged.[238] Further, employees feel a sense of accountability for the adoption's success. Accountability can increase employee contributions that will aid change adoption. However, certain employees will always be resistant to change. Those resistant to change can be encouraged when organizations are upfront about addressing apprehension to change.[239] Research indicates that opinion leaders within an organization can help win over those against change. Opinion leaders

---

234 "10 Businesses That Failed to Adapt," Business Pundit, November 3, 2014, http://www.businesspundit.com/10-businesses-that-failed-to-adapt/.

235 Ann Gilley, Marisha Godek, and Jerry Gilley, "Change, Resistance, and the Organizational Immune System," *SAM Advanced Management Journal* 74, no. 4 (2009), http://www.freepatentsonline.com/article/SAM-Advanced-Management-Journal/222313523.html.

236 Farnham, Pedersen, and Kirkpatrick, "Observation of Katrina/Rita Groove Deployment," 41.

237 Ibid.

238 Ibid.

239 Zareen Husain, "Effective Communication Brings Successful Organizational Change," T*he Business & Management Review* 3, no. 2 (2013), http://www.abrmr.com/myfile/conference_proceedings/Con_Pro_12315/7-dubai13.pdf.

are generally defined as those who have the ability to influence others due to their expertise.[240] Marketing campaigns engage these individuals to generate interest in products or services. Public service organizations will benefit from using opinion leaders within their agencies to assist mobile application adoption strategies.

Effective organizational communication can reduce resistance to change. Organizational communication is the process through which employees receive information from their organization, including information on change.[241] This information transaction reduces uncertainty and clarifies management objectives. Dialogue between management and employees will aid in conveying the need for the change, what the changes are, and how they will affect operations and the employee.[242] Effective communication can also lead to enhanced trust between the employee and management. Trust in the employee–manager relationship results in higher levels of cooperation and performance.[243] Face-to-face interaction is preferred over email and text messaging when communicating change, but organizations may not be able to do this. Off-the-shelf mobile technologies, such as Slack, can actually serve as a communication platform that would encourage its own diffusion.[244]

C. CONCLUSION

Off-the-shelf mobile applications present affordable solutions to enhance first responders' situational awareness. The availability of these products to diverse populations makes them an attractive option to groups that seek to develop ad hoc information-sharing environments. The security and scalability of the programs allow multiple groups to be established as needed to segregate information that may be of a classified nature. While these benefits are salient, there are challenges to app adoption.

---

240 "Opinion Leaders," Boundless, accessed January 11, 2017, https://www.boundless.com/marketing/textbooks/boundless-marketing-textbook/consumer-marketing-4/social-influences-on-the-consumer-decision-process-42/opinion-leaders-214-4122/.

241 Husain, "Effective Communication," 44.

242 Ibid., 45.

243 Ibid., 46.

244 "How Slack Can Help Increase Productivity and Improve Communication," Webrevolve, April 15, 2016, https://www.webrevolve.com/slack-can-help-increase-productivity-improve-communication/.

Effective leadership and communication will be essential to ensuring these programs are effectively adopted. Modification to the terms of agreement established by the developer can aid in reducing unneeded overhead functions. To overcome the challenges and take advantage of the opportunities provided by off-the-shelf mobile applications, effective policy must be formulated.

THIS PAGE INTENTIONALLY LEFT BLANK

V. POLICY

The public sector has been slow to provide guidance through policy on how to limit vulnerabilities associated with mobile applications. Lack of policy can negatively impact the adoption of these technologies. This is concerning because *Governing Magazine* recently reported that nearly half of the government agencies surveyed in 2013 were in the process of developing enterprise mobile strategies, and 58 percent reported deploying new mobile apps in 2015.[245] As off-the-shelf mobile enterprise applications become more prevalent in the public sector, policies are essential to ensure that these tools are assets, not liabilities. The U.S. homeland security community needs to examine current deficiencies in this area to identify effective security standards in adopting this evolving technology.

A. BACKGROUND

Many of the delays related to the development of U.S. policy for mobile application security may be due to the diversity of mobile devices used in the workplace. A recent government survey revealed that 90 percent of government employees use at least one mobile device for work purposes; of these employees, 69 percent use an organization-provided device.[246] Unfortunately, 15 percent of the government employees that use agency-supplied devices have downloaded apps unrelated to work on these devices.[247] These applications represent an unregulated vector for threat intrusion into the agency's networks. Additionally, 15 percent of government employees utilize personal devices for work and 25 percent use personal email accounts for work documents.[248] A recent survey indicated that "50 percent use their personal devices for work email, and 17 percent store work-related documents on personal file-sharing

[245] Governing, *Mobile Strategy Survey*, 2.

[246] "2014 Mobilometer Tracker, Mobility, Security and the Pressure in Between," Cisco, January 13, 2014, http://www.mobileworkexchange.com/uploads/3000/2837-Place_Holder.pdf.

[247] Ibid.

[248] Ibid.

apps."[249] The use of personal devices and applications can create unregulated vectors for intrusion to agency networks.

A recent survey of federal agencies indicated fiscal and technological challenges of developing effective communication networks. Fifty-two of 100 federal agencies surveyed in 2011 indicated they lacked adequate funds to support communications with customers, both public and private. Data from this survey was consistent with information acquired from a 2007 survey, which means the problem is going ignored.[250] Thirty-two percent of the agencies surveyed felt their communication technologies were out of date. This is likely attributed to the survey participants' knowledge of more effective communication methods available in off-the-shelf applications. In some cases, members of government are taking risks using these communication applications for work-related functions.

In October 2016, the news broke that Australian Prime Minister Malcolm Turnbull and his cabinet ministers were using WhatsApp to conduct private discussions.[251] According to Australian policy, elected officials are required to use a government-run communication system for official business. Australia's cyber security minister defended the practice, despite it not being on the approved list of applications developed by the Australian Signals Directorate (ASD). Opposing political parties have questioned the practice as a threat to national security. The ministers using the app have claimed it was not used for confidential information, and no violation had occurred. However, this practice has been subject to public scrutiny, similar to the response to 2016 U.S. presidential candidate Hillary Clinton's use of a private email server for State

[249] PR Newswire, "Lookout Study: Nearly 40 Percent of Government Employees Ignore Policies Prohibiting Mobile Device Use, Put Sensitive Data at Risk," August 19, 2015, http://www.prnewswire.com/news-releases/lookout-study-nearly-40-percent-of-government-employees-ignore-policies-prohibiting-mobile-device-use-put-sensitive-data-at-risk-300130821.html.

[250] DPRA, "2011 Federal Contact Center Survey," September 30, 2011, https://www.digitalgov.gov/files/2014/07/2011-Federal-Contact-Center-Survey-Final-Report-Sept30th2011-Prepared-for-GSA-OCSIT.pdf, 15.

[251] James Massola, "Turnbull Government Risking National Security, Cabinet Material by using WhatsApp: Dreyfus," *Sydney Morning Herald*, October 13, 2016, http://www.smh.com.au/federal-politics/political-news/turnbull-government-risking-national-security-cabinet-material-by-using-whatsapp-dreyfus-20161013-gs1dje.html.

Department communications. Clinton's use of her own server resulted in Senate hearings, criminal investigations by the FBI, and repeated attacks by rival candidate and election winner Donald Trump.

Prime Minister Turnbull feels that there is value to using off-the-shelf technology for government functions. Turnbull is renowned for espousing new technology such as the Apple Watch and collaboration applications Wikr and Slack.[252] Australia's Freedom of Information Act does not allow the public to access the minister's personal documents, documents of a political nature, or those held in the minister's capacity as a member of parliament.[253] Craig Searle, founder of cybersecurity firm Hivint, feels that governments should be using secure messaging applications, but they must be approved. He confirms that staff should be aware of data classifications and use products from the ASD-approved whitelist.[254] Tobias Freakin, a cyber security expert from the Australian Strategic Policy Institute, submits that despite end-to-end encryption devices, security remains a problem. Security concerns are related to devices being misplaced and potentially accessed, or compromised, through phishing scams.[255] Phishing is a result of malware executed on a device through a link or attachment opened through the app. However, government-run email applications and servers are also susceptible to these threats.

Government-to-government applications fall into two categories. The first category applies to apps that are designed for traditional functions that support information and transactions in the field and back office. Applications in this category include email and proprietary computer-aided dispatch systems. The second category, most applicable to shared situational awareness across disciplines, includes novel

---

[252] James Massola, "Malcolm Turnbull and Senior Cabinet Ministers Using WhatsApp Could Pose Security Risk: Experts," *Sydney Morning Herald*, October 12, 2016, http://www.smh.com.au/federal-politics/political-news/malcolm-turnbull-and-senior-cabinet-ministers-using-whatsapp-could-pose-security-risk-experts-20161012-gs0cuj.html.

[253] Ibid.

[254] Ibid.

[255] Ibid.

functions that support information and transactions in the field and back office.[256] MIM systems such as WhatsApp and Telegram are in this category, as there is no formal structure for their use at this time.

The challenges that the U.S. homeland security community faces are as diverse as the agencies charged with responding to them. Natural disasters, terrorism, and large-scale industrial accidents all require input from multiple disciplines and numerous layers of government. Many of the challenges these agencies encounter involve a lack of situational awareness and communication interoperability during critical incidents. The proliferation of mobile technology provides an opportunity to resolve the challenges with devices and software that are dynamic enough to meet a multitude of needs. It is essential for responders to understand and contribute to the knowledge of an unfolding event, and off-the-shelf mobile apps are a viable solution. In an interview with *Emergency Management*, one first responder stated mobile devices and applications "can help us with reports, checklists, geo-location and situational awareness. Almost all of our phones can download an app. I think apps would allow us to work across jurisdictions and across organizations and provide a common platform."[257] Off-the-shelf mobile applications can support first responder operations and encourage collaboration if formal programs are properly developed.

Off-the-shelf mobile applications can provide real-time updates from critical incident locations. Social media platforms used by the public and first responders provide invaluable information from the scene that aids decision-makers.[258] During the 2016 Democratic National Convention held in Philadelphia, Pennsylvania, the New Jersey incident command received information that a protest group planned to block vehicular traffic on the Benjamin Franklin Bridge which connects the two states. New Jersey police were able to use an off-the-shelf mobile application called Periscope to view a real-time

[256] Hans J. Scholl, "The Mobility Paradigm in Government Theory and Practice: A Strategic Framework,"378, https://pdfs.semanticscholar.org/86d7/22cbc9d0c1a655b2dca9c69130c36863470b.pdf.

[257] Margaret Steen, "Emergency Management: There's an App for That," Emergency Management, April 2, 2014, http://www.emergencymgmt.com/training/Emergency-Management-App.html?page=2.

[258] Elodie Fichet et al., "Eyes on the Ground: Emerging Practices in Periscope Use during Crisis Events," University of Washington, accessed February 19, 2017, http://faculty.washington.edu/kstarbi/ISCRAM2016_Periscope_FINAL.pdf.

video feed of the protestors. This feed confirmed that the marchers had no mal-intent and planned to use the pedestrian walkway. The situational awareness provided by the streaming technology allowed the security detail to focus on other security concerns related to the event.

B. NEED FOR UNIFORM POLICY

As mobile devices and applications permeate the homeland security disciplines, it will be important to identify policy requirements to protect users and agencies. Off-the-shelf mobile applications are free in most cases, and studies have shown that individuals who download these applications give little consideration to the potential risks.[259] In some cases, an application's terms and conditions can exceed the needs of the app. A geo-location app could pose security and privacy concerns by requesting access to a consumer's contacts.[260] Unfortunately, some consumers consider the sharing of personal information appropriate in light of the service provided.[261]

IT managers are concerned with mobile applications as a vector for intrusion into the very networks they are tasked with protecting. Reports of malicious mobile applications that attempt to pass themselves off as the desired application reinforce this concern.[262] In this scenario, cyber-criminals download the original version of certain applications and reverse-engineer them to execute ransomware or perform other malicious functions.[263] Previously these malicious applications were only available on websites, not credible application stores. However, there has been a recent trend in these applications appearing on reputable app stores such as Google Play. The malicious app Install Pokemongo was downloaded by 10,000 to 50,000 victims.[264] "Fake apps" such as

---

[259] Mark Harris, Robert Brookshire, and Amita Chin, "Identifying Factors Influencing Consumers Intent to Install Mobile Applications," *International journal of Information Management* 36 (June 2016), doi: 10.1016/j.iijnfomgt.2016.02.004.

[260] Ibid.

[261] Ibid.

[262] Stephanie Hochstadter, "Fake Apps They're Popping Up at The App Store, What You Need To Know," Power Wallet, November 15, 2016, https://www.powerwallet.com/fake-apps/.

[263] Zeljka Zorz, "Pokemon Go! Malicious Apps Lurk on Google Play," Help Net Security, July 16, 2016, https://www.helpnetsecurity.com/2016/07/15/android-malware-impersonating-pokemon-go/.

[264] Ibid.

these that attempt to profit from the popularity of legitimate games (in this case, the legitimate app-based game Pokémon Go) take advantage of uninformed users through "scareware," advertisements that trick the user into paying for unnecessary security services.[265]

To address the security concerns of applications being downloaded onto government mobile devices, DHS has engaged the private sector. Carwash, an application security tool, was jointly developed by DHS and Blackstone Technology Group. The software is designed to standardize and archive the scanning results of mobile applications prior to the device downloading the application. This security check reduces the time to market for proprietary and off-the-shelf mobile applications for DHS.[266]

Currently, there is a lack of uniform security policy that regulates mobile applications used on federal, state, local, and tribal devices. NIST is attempting to provide recommendations for public safety agencies to consider when using mobile application technology, but these are more suggestions than requirements.[267] As situational awareness applications may be used across communities, e.g., federal to state information-sharing, a uniform set of security principles is essential to ensure that off-the-shelf applications do not corrupt the devices of the agencies that participate. The federal government is uniquely positioned to develop policy for local agencies through its grant assistance programs.

C. MOBILE APPLICATION RECOMMENDATIONS

There are efforts underway to make recommendations to government agencies on technology security standards. This section examines some of the proposed legislation and policy recommendations with the intent of developing a whole-of-government approach to policy for mobile applications for situational awareness. The scope of this

---

265 "Malicious Pokemon Go Apps Land in Google Play," *SecurityWeek*, July 18, 2016, http://www.securityweek.com/malicious-pokémon-go-apps-land-google-play.

266 "Carwash Success: New DHS Policy Requires Carwash for All Mobile Applications," PRWeb, April 13, 2016, http://www.prweb.com/releases/2016/04/prweb13338405.htm.

267 "Key Attributes of Effective Apps," Application Community.

examination comprises four categories of information security that directly impact mobile application technology.

The first category identifies the existing mobile application policy for government-issued mobile devices. It does not examine personal devices that are used for government-related work. The second category identifies the value of IS security training required for government agencies. As identified previously, there is a propensity for government employees to download applications to their mobile devices without concern for device security. Training will likely increase employees' threat awareness. The third category examined is the presence of breach-notification requirements. The sharing of breach information across the enterprise is integral to addressing the concerns posed by these applications to the security environment. Finally, application whitelisting is evaluated as an option for homeland security. Application whitelisting is the process of identifying and approving mobile applications for use by the enterprise. A whitelist can take the form of an agency "app store" or list that allows government employees to download and utilize approved software that is compliant with the enterprise's security requirements.

D. EVOLVING POLICY

Several bills have been introduced that require mobile application developers and organizations to implement data-security measures for this emerging environment. The Application Privacy, Protection, and Security (APPS) Act of 2016 requires application developers to obtain the user's consent before collecting personal data. The developer must also provide the user with a method to withdraw consent and delete all personal data acquired.[268] NIST is developing policy recommendations for third-party mobile applications used by government agencies. In May 2016, NIST released its workshop report entitled *Identifying and Categorizing Data Types for Public Safety Mobile Applications*. The goal of this workshop was to identify the types of data that will flow

[268] *APPS Act of 2016*, H.R. 4517, 114th Congress.

through public safety mobile applications.[269] The report identifies security, privacy, and technical concerns for agencies that use this technology. Identifying security concerns is the first step in building mobile application policy recommendations that are effective without being restrictive.

DHS is attempting to develop security standards and policy recommendations for mobile application adoption. Most federal agencies vet applications, but there are disparities among the various departments. Currently, the Pentagon uses proactive approaches through its Defense Information Services Agency (DISA) to certify apps for troops prior to use.[270] DHS uses the vulnerability assessment tool Carwash for applications after they are downloaded on agency-issued devices.[271] NIST is also developing standards for vetting apps, but nothing has been approved. Whitelisting, or pre-approving mobile applications for homeland security, allows federal, state, and local agencies to be aware of safe applications. An unfortunate byproduct may be that the whitelisted application may be targeted by cyber-threats. Measures must be taken to address reporting of any compromise of these systems.

The National Cybersecurity and Communications Integration Center (NCCIC) is tasked with sharing threat information among private and public sector agencies.[272] To enhance this information-sharing initiative, several pieces of pending legislation address issues related to security breaches and notification. The Secure and Protect Americans Data Act requires the FTC to establish information-security practices for the treatment and protection of personal information. Developers are required to evaluate their consumer privacy programs and identify any security vulnerabilities and threats to the NCCIC. The Secure and Protect Americans Data Act also allows the user to "opt out" of providing personal information for marketing purposes and provides for a formal process

---

[269] Michael Ogata, *Identifying and Categorizing Data Types for Public Safety Mobile Applications: Workshop Report* (NISTIR 8135) (Gaithersburg, MD: NIST, 2016), 1, doi: 10.6028/NIST.IR.8135.

[270] Aliya Sternstein, "DHS Official: Create a Government-wide Seal of Approval for Apps," Nextgov, August 27, 2014, http://www.nextgov.com/mobile/2014/08/dhs-official-create-governmentwide-seal-approval-apps/92564/.

[271] Ibid.

[272] "NCCIC Overview," DHS, accessed August 20, 2016, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.

of notifying the appropriate government agencies when there is a security breach.[273] The Security and Data Protection Act requires agencies to report security breaches within ten days to the following agencies:

- the FTC
- the FBI
- the U.S. Secret Service
- the Federal Communications Commission (FCC)
- the Attorneys General of affected states

The act also requires developers to notify those who have been impacted by a breach within 30 days. If more than 5,000 people are breached the developer must also notify major consumer reporting agencies. This notification must be in print and broadcast media to reach the individuals that may be affected.[274]

E. SELECTING AN APP

DHS has recently released a set of best practices for mobile application adoption. The report acknowledges the value of mobile applications in enhancing situational awareness, responder safety, and productivity. Additionally, the guidance warns against the threats that this technology presents. Some of these threats include:

- hijacking of other applications
- stealing, broadcasting, and/or altering data
- denying the authorized user access to service
- allowing unauthorized users access to service
- accessing medical, data personnel records, incident reports, and/or video evidence
- reporting on sensitive information of the user, such as location information, to a third party

[273] *Secure and Protect Americans' Data Act*, H.R. 4187, 114th Congress (2015).

[274] Ibid.

- violating or disrupting the confidentiality, integrity, and availability of all other legitimate apps through shared memory or other methods[275]

The Federal Risk and Authorization Management Program (FedRAMP) has developed an accreditation path for baseline security standards for cloud-hosted systems before federal employees log in.[276] Using this framework, the federal government can develop a program that ensures the mobile applications used by federal and grant-funded state, local, tribal, and territorial agencies are utilizing mobile apps that meet a baseline security standard. The current whitelisting attempt on apps.gov is limited and does not include the variety of mobile applications that can support situational awareness.[277]

DHS proposes a three-step process for selecting mobile applications for homeland security functions. First, the agency should define benefits and seek approval. After approval, users should then apply best practices to avoid any security threats related to use of the application. Finally, the user should monitor performance of the application to ensure that it is performing as designed.[278] This process is designed to not only aid in the selection of an off-the-shelf mobile application but also the continued evaluation of the function of the application throughout its life-cycle.

The first step of the process focuses on selecting and obtaining approval for the use of the application. An agency examining mobile applications for enterprise use should determine what the desired functions are, and how the application will achieve them. The app must be user friendly, easily downloaded, and technically supported, and the developer should provide maintenance.[279] As mentioned previously, technology acceptance is dependent on a user's positive experience. Data retention and retrieval should also be required due to evidenced retention requirements.[280] The application

---

275 "Mobile Application Adoption Best Practices," DHS, accessed November 17, 2016, https://www.dhs.gov/sites/default/files/publications/Mobile%20Application%20Adoption%20Best%20Practices%20Guide-508%20compliant%20FINAL%20041316.pdf.

276 "FedRAMP Compliant Systems," accessed August 1, 2016, https://www.fedramp.gov/marketplace/compliant-systems/.

277 "Products," apps.gov.

278 Ibid.

279 Ibid.

280 "Records Management Advice," State of Washington.

should also meet operational demands. Customer reviews are very effective at determining viability of the application; however, field-testing should still be conducted if possible. If field testing is denied, agencies should obtain documentation of an app's ability to work on the desired platforms as well as other users' evaluations. Evaluators should also seek information on an application's impact on processor speed, media capacity, and the ability to queue information in times of congestion. Other considerations include the cost, type, and interoperability with other apps used by the enterprise.[281]

In the second step of the evaluation process the user should identify and avoid security concerns. Data and mobile-device security should be a primary concern for agencies adopting mobile application programs. First and foremost, the application should be downloaded from a trusted source. Information technology specialists should vet these sources to make sure they meet public safety security standards. Any app that requires the device to be jailbroken or sideloaded (directly interfaced with a desktop computer to transfer media) should be suspect. By jailbreaking a device, the user allows an application designed for certain operating systems to be used on another operating system, an example being an Apple app used on an Android device. Apps that need to be sideloaded are also concerning, as this presents an additional vector for security intrusion.[282]

Users must acknowledge full understanding of the permissions associated with the application. All permissions granted to the application must be legitimate and necessary to its function. Applications that access personal contacts and user locations may exceed the scope of this purpose. However, when developing a situational awareness environment for large groups of responders, they may be essential.

The agency should acknowledge which types of data could be compromised if the app succumbs to malware. Popular off-the-shelf applications are targets for intrusion, so the classification of data passing through them should be a consideration of the host

[281] "Mobile Application Adoption," DHS.

[282] Ibid.

agency. The program manager should ensure that users engage in safe security practices. Personal identification numbers or passwords to unlock the device should be a requirement, as well as an automatic locking function after a period of inactivity. Remote wiping of data on the device as well as device tracking are also measures that should be considered should the application access sensitive data.[283]

Beta testing of the application should be conducted prior to rollout. A small cadre of users should evaluate the application for its ability to facilitate situational awareness. Availability, reliability, responsiveness, resiliency, scalability, and accuracy are all evaluation measures that should be considered for enterprise adoption.[284] When the application is approved, regular software updates should be mandatory to avoid performance and security flaws. When conducting updates, any permission changes must be acknowledged. If the user transitions to another device, any changes to the security and performance should be acknowledged when downloading the app.[285]

In the third step of the process, the user should evaluate the performance of the application. When adding an application to a device, users should monitor battery, memory, and processing power consumption. Any applications that are not being used should be deleted to reduce clutter and save resources. Users should also limit push notifications and automatic updates on infrequently used apps to preserve device performance. If any unexpected behavior occurs through the use of the application, it should be reported immediately to the agency network administrator and the developer.[286]

F. ISOLATING THE APP FROM THE ENTERPRISE

In order for agencies to adopt mobile applications to improve situational awareness, a basic understanding of mobile-device architecture and security may be required. Mobile devices have many similarities to desktop computers. Both systems are

[283] Ibid.

[284] Ibid.

[285] Ibid.

[286] Ibid.

composed of hardware, firmware, and software, which interact with one another and must "trust" the security of the others. This section identifies the relationship between these components.

The lowest level, hardware, refers to the device itself. Mobile devices are portable computers with their own power supply and one or more radios used to connect the device to a network. Hardware that supports data connectivity include cellular, Wi-Fi, Bluetooth, and near field communication (NFC) systems.[287] Other hardware components on the device may include media players, cameras, GPS receivers, and other sensors such as the accelerometer, gyroscope, proximity, and compass.[288] Security at the hardware level is essential because it is the foundation on which the other layers operate. Firmware is the next layer in the stack and represents the special code that controls the hardware functions. The device manufacturer typically writes this code and can update it through the device provider. The operating system (OS) is where the kernel and policy enforcement engine (PEnE) reside. The OS kernel isolates applications from one another. This is important for off-the-shelf mobile application users who have secure data on other applications. Cooperation and "trust" between hardware and firmware components are needed to ensure the integrity of application data.[289] Mobile devices segregate apps to a separate layer on the device to isolate them from secured information. The kernel allows applications that reside in this layer to access hardware and firmware. This access is needed for application performance, yet the kernel prevents the applications from accessing information processed, stored, and transmitted by other applications.

The PEnE allows the information owner to exert control over his or her information and protect it as required by policy.[290] Some malware can extract sensitive data from the device, resulting in a loss of confidentiality. NIST reports, "Any complex software, including mobile applications, will have latent exploitable conditions, (i.e.,

---

[287] Lily Chen, Joshua Franklin, and Andrew Regenscheid, *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)* (Special Publication 800-164) (Gaithersburg, MD: NIST, 2012), 11, 12, http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

[288] Ibid., 12.

[289] Ibid.

[290] Ibid., 10.

vulnerabilities) that could allow an unauthorized entity to gain control of the context within which the application runs, or otherwise cause an application to behave in a manner other than the information owner or application developer intended."[291] While application isolation is a practical solution, messaging applications that support situational awareness needs must share information such as a central contact list and location.

NIST recommends that policymakers develop device identity policies. These policies will ensure that the device and information owners are able to authenticate and maintain the information security of the device and its storage.[292] The PEnE should enforce this policy on the device. This would include policy related to data retention and protection of the information owner's data. Finally, the device and information owners shall reserve the right to reject or accept the conditions of this agreement prior to granting access to the device.

G. TEMPLATES FOR POLICY

FedRAMP has developed an accreditation path for baseline security standards for cloud-hosted systems before federal employees log in.[293] Using this framework, the federal government can develop a program that ensures the mobile applications used by federal and grant-funded state, local, tribal, and territorial agencies meet a baseline security standard.

Recently developed social media policies for government users may aid in policy development for situational awareness applications. To develop best practices, the Virtual Social Media Working Group (VSMWG) was assembled in July 2011. The VSMWG has developed recommendations that can serve as a template to agencies interested in using off-the-shelf technologies for situational awareness. In January 2012, DHS published its recommendations for social media for emergency response.[294] Many of the social media

[291] Ibid., 18.

[292] Ibid., 15.

[293] "FedRAMP Compliant Systems."

[294] DHS Science and Technology, *Next Steps*.

platforms recommended are free, off-the-shelf mobile applications designed for mass communication. These programs have become essential components of emergency preparedness, response, and recovery.

Off-the-shelf mobile applications pose many concerns that need to be communicated to the user. The VSMWG recommends that users disclose an application's use of "cookies" for information retention.[295] Any agency seeking to use this technology should make sure that its members are familiar with all terms of use required by use of the application. Organizations that use these technologies should provide a brief synopsis for employees to read, comprehend, and reference as needed. This is of particular importance to agencies that allow employees to use personal devices for work-related functions. Appropriate BYOD policies reflecting best security practices should be developed, if applicable.

The VSMWG also recommends that users be made aware of best practices related to the use of these software applications. Restrictions should be placed on the disclosure of any health-related information as well as other personal information.[296] Records should be retained in compliance with all agency requirements and users should acknowledge the level of security related to the information shared over these networks. Situational awareness should be considered open source for most operations; however, exigency may require for-official-use-only information to be distributed through these networks—for example, photos of the suspects in the Boston Marathon Bombing released to law enforcement agencies prior to the public writ at large. The VSMWG suggests that agencies consider with whom they are sharing information, and provide guidance on restrictions of that data as necessary.[297] Professional behavior on these platforms should be communicated to users as well. Members should be made aware of concerns related to comingling of data through personal and professional use of these systems.

[295] Ibid., 9.

[296] Ibid., 10.

[297] Ibid., 10.

Training and education programs should be provided to reinforce these recommendations as well as any other policies of the agency. Those who use off-the-shelf mobile technology for situational awareness should be provided with "safe surfing" etiquette as well as protocols for security breaches. VSMWG also recommends that users procure the appropriate technology to assimilate these applications and apply safe practices, such as password protection of devices and applications, as needed.[298] Agencies should also incorporate this technology into regular training and exercises to reinforce the role of these technologies and the policy that regulates them.

The majority of U.S. homeland security agencies are in the development phases of mobile-application technology policies. This is attributed to the evolving nature of the technology as well as delays associated with policy formulation. Homeland security agencies should collaborate to develop uniform policy and adoption strategies for these technologies. Failure to do so further hampers program development.[299] Effective leadership and implementation of minimum security standards are also essential for making situational awareness applications safe and effective for homeland security agencies.

(1) Recommendation #1

Effective leadership that embraces change is essential to agencies adopting off-the-shelf mobile application technologies. There are many barriers to technology adoption, but effective organizational communication and leadership will aid in the implementation of these applications for situational awareness.

(2) Recommendation #2

Policymakers should examine technology policies of other agencies when developing policy for off-the-shelf mobile applications used by homeland security agencies. FedRAMP cloud computing policy and NIST recommendations for social media serve as excellent frameworks. Additionally, policymakers should seek to

[298] Ibid., 12.

[299] Henry Kenyon, "Why Federal Agencies Lag."

renegotiate terms of use with app providers if possible to protect applications used for official functions.

(3) Recommendation #3

Uniform training should be required for all agencies that employ off-the-shelf mobile application technology in the course of their homeland security functions. Training for safe practices in application downloading and utilization will ensure employees embrace appropriate behavior while using these tools. Refresher training and exercises will ensure users are aware of best practices and breach notification procedures.

H. CONCLUSION

This thesis identifies how homeland security agencies can adopt off-the-shelf mobile applications for situational awareness. It provides background on the importance of situational awareness and how these technologies can enhance it during critical incidents. Barriers to adoption are discussed as well as ways to overcome them. Security, training, and policy concerns are also acknowledged along with recommendations for addressing them.

There are numerous benefits to adopting off-the-shelf mobile technologies to increase the situational awareness and inter-operability of the various disciplines of homeland security. The costs of not adopting mobile applications for situational awareness are diminished inter-agency coordination and compromises in first responder safety. The pros and cons of off-the shelf mobile applications will inform the reader and identify how homeland security can embrace these technologies for current and future needs.

I. FUTURE RESEARCH

This thesis examines how homeland security agencies can adopt off-the-shelf mobile applications for situational awareness needs. Future topics of research should focus on the proliferation of BYOD programs and work-related mobile application use as fiscal restraints and user preference of personal devices evolve. Additional research into the evolution of command and control due to the democratization of situational

awareness is also warranted. As ubiquitous mobile networks, devices, and applications begin to take a larger role in homeland security situational awareness, concerns with self-deployment, uncoordinated response, and modified interagency response may develop as formal top-down, hierarchical structures are diminished by technology.

LIST OF REFERENCES

911.gov. “Next Generation 911 (NG911).” Accessed March 25, 2016. http://www.911.gov/911-issues/standards.html.

Agrimbau, Tomas. “Developing Mobile Web Apps: When, Why, and How.” Toptal. Accessed December 15, 2016. https://www.toptal.com/android/developing-mobile-web-apps-when-why-and-how.

Alberts, David, and Richard Hayes. *Power to the Edge: Command…Control…In the Information Age*. Washington, DC: CCRP, 2003. http://www.dodccrp.org/files/Alberts_Power.pdf.

Application Community. “Key Attributes of Effective Apps for Public Safety.” August 18, 2013. http://appcomm.org/wp-content/themes/directorypress/thumbs/AppComm_Key_Attributes.pdf.

Apps.gov. “Products.” Accessed October 22, 2016. https://apps.gov/products.

Bailey, Jim. “5 Elements of Proactive Situational Awareness.” Emergency Management. May 4, 2015. http://www.govtech.com/em/training/5-Elements-Proactive-Situational-Awareness.html.

Bal, Sanjeev Narayan. “Mobile Web—Enterprise Application Advantages,” *International Journal of Computer Science and Mobile Computing* 2, no. 2 (February 2013): 36–40. http://www.academia.edu/2580454/Mobile_Web_Enterprise_Application_Advantages.

Barry, Douglas K. “Service Architecture.” Accessed January 10, 2016. http://www.service-architecture.com/articles/web-services/service-oriented_architecture_soa_definition.html.

Bhagat, Rahil. “5 Reasons You Might Want to Switch From WhatsApp to Telegram.” *Stuff*. May 11, 2016. http://www.stuff.tv/sg/features/5-reasons-you-might-want-switch-whatsapp-telegram.

Birriel, Elizabeth. “Case Study #3: Integrating Third Party Crowd Sourced Data.” U.S. Department of Transportation. Accessed November 13, 2016. https://www.pcb.its.dot.gov/t3/s150311/s150311_crowdsourced_data_presentation_birriel.pdf.

Boundless. “Opinion Leaders.” Accessed January 11, 2017. https://www.boundless.com/marketing/textbooks/boundless-marketing-textbook/consumer-marketing-4/social-influences-on-the-consumer-decision-process-42/opinion-leaders-214-4122/.

"Brussels Police Were Forced to Use WhatsApp during Attack." BNO News. March 26, 2016. http://bnonews.com/news/index.php/news/id3969.

Bryson, John M., Barbara C. Crosby, Melissa M. Stone, and Emily O. Saunoi-Sandgren. *Designing and Managing Cross-sector Collaboration*: *A Case Study in Reducing Traffic Congestion*. Washington, DC: IBM Center for the Business of Government, 2007. http://www.businessofgovernment.org/report/designing-and-managing-cross-sector-collaboration-case-study-reducing-traffic-congestion.

Business Pundit. "10 Businesses That Failed to Adapt." November 3, 2014. http://www.businesspundit.com/10-businesses-that-failed-to-adapt/.

Chaffey, Dave. "Mobile Marketing Statistics Compilation." Smart Insights. Accessed March 25, 2016. http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/.

Chen, Andrew. "New Data Shows Losing 80% of Mobile Users Is Normal, and Why the Best Apps Do Better." Accessed December 15, 2016. http://andrewchen.co/new-data-shows-why-losing-80-of-your-mobile-users-is-normal-and-that-the-best-apps-do-much-better/.

Chen, Lily, Joshua Franklin, and Andrew Regenscheid. *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)* (Special Publication 800-164). Gaithersburg, MD: NIST, 2012. http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

Christensen Institute. "Disruptive Innovation." Accessed January 6, 2016. http://www.christenseninstitute.org/key-concepts/disruptive-innovation-2/.

Cisco. "2014 Mobilometer Tracker, Mobility, Security and the Pressure in Between." January 13, 2014. http://www.mobileworkexchange.com/uploads/3000/2837-Place_Holder.pdf.

Citrix. "Jump Start Mobile Productivity with MDM and Secure File Sharing." Accessed February 20, 2017, https://www.citrix.com/content/dam/citrix/en_us/documents/oth/jump-start-mobile-productivity-with-mdm-and-secure-file-sharing.pdf.

City-Data. "New York: Languages." Accessed February 19, 2017. http://www.city-data.com/states/New-York-Languages.html.

City of New York. "Press Release from the Office of Mayor Bloomberg" (PR-291-12). August 8, 2012. http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2012b%2Fpr291-12.html&cc=unused1978&rc=1194&ndi=1.

Cohn, Chuck. “Build vs. Buy: How to Know When You Should Build Custom Software Over Canned Solutions.” *Forbes*. September 15, 2014.

Community Oriented Policy Services. “The Impact of the Economic Downturn on American Police Agencies.” Department of Justice. Accessed May 20, 2016. http://www.cops.usdoj.gov/Default.asp?Item=2602.

Crawford, Susan, and Laura Adler. *Culture Change and Digital Technology: The NYPD under Commissioner William Bratton, 2014–2016* (Research Publication No. 2016-13). Cambridge, MA: Berkman Klein Center, 2016.

Currie, Wendy, and Bob Galliers. *Rethinking Management Information Systems: An Interdisciplinary Perspective*. New York: Oxford University, 1999.

Daly, Ger. “Embracing the Police Force of the Future.” CNN. September 19, 2013. http://www.cnn.com/2013/09/18/tech/innovation/police-future-technology/.

Davis III, Edward F., Alejandro A. Alves, and David Alan Skalansky. “Social Media and Police Leadership: Lessons from Boston.” *New Perspectives in Policing*. March 2014. https://www.ncjrs.gov/pdffiles1/nij/244760.pdf.

Davis, Fred D. “A Technology Acceptance Model for Empirically Testing New End User Information Systems: Theory and Results.” Ph.D. dissertation, MIT, 1985.

Department of the Army. *Counterinsurgency Field Manual* (FM 3-24). Washington, DC: Department of the Army, 2006.

Department of Homeland Security (DHS). *Lessons Learned: Social Media and Hurricane Sandy*. Washington, DC: DHS, 2013. https://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20Social%20Media%20and%20Hurricane%20Sandy.pdf.

———. “Mobile Application Adoption Best Practices.” Accessed November 17, 2016. https://www.dhs.gov/sites/default/files/publications/Mobile%20Application%20Adoption%20Best%20Practices%20Guide-508%20compliant%20FINAL%20041316.pdf.

———. “NCCIC Overview.” Accessed August 20, 2016. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.

DHS Science and Technology Directorate. *First Responder Communities of Practice Virtual Social Media Working Group Community Engagement Guidance and Best Practices* (DHS2012F0918). Washington, DC: DHS, 2012. https://www.dhs.gov/sites/default/files/publications/Virtual%20Social%20Media%20Working%20Group%20VSMWG%20Community%20Engagement-508.pdf.

———. *Next Steps: Social Media for Emergency Response*. Washington, DC: DHS, 2012. https://www.dhs.gov/sites/default/files/publications/Virtual%20Social%20Media%20Working%20Group%20VSMWG%20Next%20Steps%20Social%20Media%20for%20Emergency%20Response.pdf.

de Reuver, Mark, Shahrokh Nikou, and Harry Bouwman. "Domestication of Smartphones and Mobile Applications: A Quantitative Mixed-Method Study." *Mobile Media & Communication* 4, no.1 (June 2016): 351.

Deyto, Melani. "6 Benefits of Text Messaging: Why Your Organization Should Use SMS." *Textmarks.* February 18, 2015. https://blog.textmarks.com/benefits-of-text-messaging/.

Dick, Thom. "Will a Smartphone Replace Your Mobile Radio?" EMS World. July 1, 2016. http://www.emsworld.com/article/12213802/will-a-smartphone-replace-your-mobile-radio.

DiMario, Michael J. "System of Systems Interoperability Types and Characteristics in Joint Command and Control." *2006 IEEE/SMC Conference on System of Systems Engineering*. doi: 10.1109/SYSOSE.2006.1652302.

Dix, John. "Security: On Premise or In the Cloud." Network World. November 5, 2012. http://www.networkworld.com/article/2223442/tech-debates/security--on-premise-or-in-the-cloud-.html.

Efrati, Amir, and Peter Schulz. "Which Apps Retain Their Users—And Which Ones Don't." The Information. April 7, 2015. https://www.theinformation.com/which-apps-retail-their-users-and-which-ones-dont.

Eggers, William D., and Joshua Jaffe. "Gov on the Go." Deloitte University Press. February 19, 2013. https://dupress.deloitte.com/dup-us-en/industry/public-sector/gov-on-the-go.html#endnote-16.

Eisenhauer, Tim. "7 Reasons to Replace Email with Collaboration Software." Axero. Accessed December 11, 2016. https://axerosolutions.com/blogs/timeisenhauer/pulse/167/7-reasons-to-replace-email-with-collaboration-software.1

Endsley, Mica R. "Toward a Theory of Situation Awareness in Dynamic Systems." *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37, no. 1 (March 1995): 32–64.

ESRI. *Public Safety and Homeland Security Situational Awareness* (White Paper J-9698). Redlands, CA: ESRI, 2008. http://www.esri.com/library/whitepapers/pdfs/situational-awareness.pdf.

Estes, Richard Clark. “Inside the Military’s Secretive Smartphone Program.” Gizmodo. August 5, 2014. http://gizmodo.com/inside-the-militarys-secretive-smartphone-program-1603143142.

Evans, Jon. “When Will Your Phone Replace Your Keys and Wallet?” *Tech Crunch.* December 27, 2014. http://techcrunch.com/2014/12/27/when-will-your-phone-replace-your-keys-and-wallet/.

Farnham, Shelly, E. Pedersen, and Robert Kirkpatrick. “Observation of Katrina/Rita Groove Deployment: Addressing Social and Communication Challenges of Ephemeral Groups,” *Proceedings of the 3rd International ISCRAM Conference* (2006): 39–49.

Federal Communications Commission (FCC). *A Next Generation 9-1-1 Cost Study: A Basis for Public Funding Essential to Bringing a Nationwide Next Generation 911 Network to America’s Communications Users and First Responders*. Washington, DC: FCC, September 2011. https://apps.fcc.gov/edocs_public/attachmatch/DOC-309744A1.pdf.

FedRAMP. “FedRAMP Compliant Systems.” Accessed August 1, 2016. https://www.fedramp.gov/marketplace/compliant-systems/.

Felts, Ryan, Mark Leh, Dereck Orr, and Tracy McElvaney. *Location-Based Services R&D Roadmap* (NIST Technical Note 1883). Boulder, CO: Department of Commerce Boulder Labs, May 2015. http://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1883.pdf.

Fichet, Elodi, Dharma Dailey, John Robinson, and Kate Starbird. “Eyes on the Ground: Emerging Practices in Periscope Use during Crisis Events.” University of Washington. Accessed February 19, 2017. http://faculty.washington.edu/kstarbi/ISCRAM2016_Periscope_FINAL.pdf.

Forrester Research. “The Expanding Role of Mobility in the Workplace.” Cisco. February 2012. https://www.cisco.com/c/dam/en_us/solutions/trends/unified_workspace/docs/Expanding_Role_of_Mobility_in_the_Workplace.pdf.

Gilley, Ann, Marisha Godek, and Jerry Gilley. “Change, Resistance, and the Organizational Immune System.” *SAM Advanced Management Journal* 74, no. 4 (2009). http://www.freepatentsonline.com/article/SAM-Advanced-Management-Journal/222313523.html.

Goodman, Marc. “How Technology Makes us Vulnerable.” CNN. July 29, 2012. http://www.cnn.com/2012/07/29/opinion/goodman-ted-crime/index.html.

Google Play. “Crime Scene Tracker.” Accessed December 9, 2016. https://play.google.com/store/apps/details?id=de.crimescenetracker&feature=also_installed#?t=W251bGwsMSwxLDEwNCwiZGUuY3JpbWVzY2VuZXRyYWNrZXIiXQ.

———. “WhatsApp Messenger.” Accessed November 13, 2016. https://play.google.com/store/apps/details?id=com.whatsapp.

Governing. *Mobile Strategy Survey: Where Are You on the Roadmap from Apps to Enterprise Management?* Washington, DC: e.Republic, 2013. https://www.business.att.com/content/whitepaper/Creating-a-Mobility-Strategy-Survey-Results.pdf.

Grous, Alexander. “Socioeconomic Value of Mission Critical Mobile Applications for Public Safety in the UK: 2X10MHz in 700MHz.” LSE Research. November 2013. http://eprints.lse.ac.uk/69180/1/Grous_Socioeconomic_value_of_mission_critical_applications_UK_2013_author.pdf.

Guidetti, Ray. *New Jersey State Police Practical Guide to Intelligence-Led Policing.* New York: Manhattan Institute for Policy Research, 2006. http://www.njsp.org/divorg/invest/pdf/njsp_ilpguide_010907.pdf.

Harris, Mark, Robert Brookshire, and Amita Chin. “Identifying Factors Influencing Consumers Intent to Install Mobile Applications.” *International journal of Information Management* 36 (June 2016): 441–450. doi: 10.1016/j.iijnfomgt.2016.02.004.

Hart, James. “The Management of Change in Police Organizations.” In *Policing in Central and Eastern Europe: Comparing Firsthand Knowledge with Experience from the West*, edited by Milan Pagon. Ljubljana, Slovenia: College of Police and Security Studies, 1996. https://www.ncjrs.gov/policing/man199.htm.

Headd, Mark. “Built to Fail: Why Governments Struggle to Implement New Technology.” GovLoop. June 23, 2014. https://www.govloop.com/community/blog/built-to-fail-why-governments-struggle-to-implement-new-technology/.

Hendrix, Phil. “Mobilizing the Enterprise with off-the-Shelf Apps and Custom Mobile Solutions.” Immr. August 2012. http://www.immr.org/downloads/mobilizing-the-enterprise-with-off-the-shelf-apps-and-custom-mobile-solutions-dr-phil-hendrix.pdf.

Hennelly, Bob. “10 Years Later, FDNY and NYPD in Radio Sync.” WNYC. September 27, 2011. http://www.wnyc.org/story/\161257-blog-10-years-later-fdny-and-nypd-radio-sync/.

Holmstead, Kenneth, and Michelle Atkinson. “The Majority of Smartphone Users Download Apps.” Pew Research Center. November 10, 2015. http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/.

Hochstadter, Stephanie. “Fake Apps They’re Popping Up at The App Store, What You Need To Know.” Power Wallet. November 15, 2016. https://www.powerwallet.com/fake-apps/.

Hughes, Jessica. “Civic Ninjas Find Long-Term Solutions to Government Problems.” Government Technology. August 27, 2014. http://www.govtech.com/Civic-Ninjas-Find-Long-Term-Solutions-to-Government-Problems.html.

Husain, Zareen. “Effective Communication Brings Successful Organizational Change.” T*he Business & Management Review* 3, no. 2 (2013). http://www.abrmr.com/myfile/conference_proceedings/Con_Pro_12315/7-dubai13.pdf.

IACP Center for Social Media. “Apps, The Basics.” Accessed November 30, 2016. http://www.iacpsocialmedia.org/Technologies/Parent/Platform.aspx?termid=155&depth=3.

Information Sharing Environment. “Critical Infrastructure and Key Resources.” Accessed January 12, 2017. https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources.

Ismail, Salim, Michael S. Malone, and Yuri Van Geest. *Exponential Organizations.* New York: Diversion Books, 2014, ebook.

Jakobson, Gabriel, John Buford, and Lundy Lewis. “Models of Feedback and Adaptation in Multi-agent Systems for Disaster Situation Management.” *Proc. SPIE 6943, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense* VII (April 2008): 69430N. doi:10.1117/12.778635.

Jarrett, Stephen M. “Transition of Advanced Technology to Military, Homeland Security and Law Enforcement Users.” *Proceedings of SPIE* 5403 (September 2004). doi: 10.1117/12/542420.

Karasz, Hilary, Sharon Bogan, and Lindsay Bosslet. “Communicating with the Workforce during Emergencies: Developing an Employee Text Messaging Program in a Local Public Health Setting.” *Public Health Reports* 129, Supp. 4 (2014).

Kenyon, Henry. “Why Federal Agencies Lag behind in Mobile Technology.” *Information Week*. August 26, 2014. http://www.informationweek.com/government/mobile-and-wireless/why-federal-agencies-lag-behind-on-mobile-tech/d/d-id/1306625?itc=edit_in_body_cross.

Khalaf, Simon. “Seven Years into the Mobile Revolution: Content Is King…Again.” Yahoo. August 26, 2015. https://yahoodevelopers.tumblr.com/post/127636051988/seven-years-into-the-mobile-revolution-content-is.

Kujawski, Mike. “Text Messaging vs. Mobile Instant Messaging.” May 23, 2014. GovLoop. https://www.govloop.com/community/blog/text-messaging-vs-mobile-instant-messaging/.

Lambert, Natalie. “Mobile Workspaces Enable Organizations to Keep up with Changing Workforce.” *Citrix Blog*. March 20, 2014. https://www.citrix.com/blogs/2014/03/20/mobile-workspaces-enable-organizations-to-keep-up-with-a-changing-workforce/.

Landgren, Jonas, and Urban Nulden. “A Study of Emergency Response Work: Patterns of Mobile Phone Interaction.” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (April 2007). https://pdfs.semanticscholar.org/343d/e3a625a5367609c37288c33d85ef06e49095.pdf.

Leavitt, Harold J. *Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches*. Chicago: Rand McNally.

Lee, Cynthia. “Gartner Says Traditional Development Practices Will Fail for Mobile Apps.” Gartner. August 14, 2014. http://www.gartner.com/newsroom/id/2823619.

Leontiadis, I., C. Efstratiou, M. Picone, and C. Mascolo. “Don’t Kill My Ads!: Balancing Privacy in an Ad-Supported Mobile Application Market.” *Proceedings of the Twelfth Workshop on Mobile Computing Systems* 12, no. 2 (2012).

Loi, Elissa. “26 WhatsApp Features You Didn’t Know You Had, Let Alone Could Use.” *Stuff*. March 30, 2016. http://www.stuff.tv/sg/features/19-whatsapp-features-you-might-not-be-aware.

Maurer, Rick. “Getting beyond the Wall of Resistance.” *StrategyDriven*. July 19, 2010. http://www.strategydriven.com/2010/07/19/getting-beyond-the-wall-of-resistance/.

McChrystal, Stanley. *Team of Teams: New Rules of Engagement for a Complex World*. New York: Penguin, 2015.

Meier, Patrick. “How Crisis Mapping Saved Lives in Haiti.” *National Geographic*. July 2, 2012. http://voices.nationalgeographic.com/2012/07/02/crisis-mapping-haiti/.

Meola, Andrew. “Broadband Subscribers Continue to Climb, While Cable Sees Mixed Subscriber Trends.” *Business Insider*. May 23, 2016. http://www.businessinsider.com/cable-companies-lose-more-subscribers-as-cord-cutters-grow-2016-5.

Messner , Richard A., Frank Hludik, Dragan Vidacic, and Pavlo Melnyk. “An Integrated Command, Control, and Communications Center for First Responders.” *Proc. SPIE 5778, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense* IV (August 2005): 57. doi: 10.1117/12.603727.

Moon, M. Jae. “From Egovernment to Mgovernment.” IBM Center for the Business of Government. November 2004. http://www.uquebec.ca/observgo/fichiers/28540_mgovernment.pdf.

Nanji, Ayaz. “How Influential Are Mobile App Star Ratings.” MarketingProfs. May 22, 2015. http://www.marketingprofs.com/charts/2015/27665/how-influential-are-mobile-app-star-ratings.

National Commission on Terrorist Attacks Upon the United States. *9/11 Commission Report*. New York: W.W. Norton.

Ng, Alfred. “This is NYPD’s New Crime Fighting Phone.” CNET. October 13, 2016. https://www.cnet.com/news/nypd-new-york-police-official-crime-fighting-windows-phone/.

Newman, Sean S. “Braving the Swarm: Lowering Anticipated Group Bias in integrating Fire/Police Units Facing Paramilitary Terrorism.” Master’s thesis, Naval Postgraduate School, 2011. https://www.hsdl.org/?view&did=5482.

NIST. “NIST’s Rolling Wireless Net Helps Improve First Responder Communications.” August 10, 2016. https://www.nist.gov/news-events/news/2016/08/nist’s-rolling-wireless-net-helps-improve-first-responder-communications.

Ogata, Michael. *Identifying and Categorizing Data Types for Public Safety Mobile Applications: Workshop Report* (NISTIR 8135). Gaithersburg, MD: NIST, 2016. doi: 10.6028/NIST.IR.8135.

Ogata, Michael, Barbara Guttman, and Nelson Hastings. *Public Safety Mobile Applications Security Requirements Workshop, Summary* (NISTIR 8018). Giathersburg, MD: NIST, 2015. doi: 10.6028/NIST.IR.8018.

Olmstead, Kenneth, and Michelle Atkinson. “App Permissions in the Google Play Store.” Pew Research Center. November 10, 2015. http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/.

Pathak, A., Y. C. Hu, and M. Zhang. “Where Is the Energy Spent inside My App?” *Proceedings of the 7th ACM European Conference on Computer Systems* 12 (2012).

Pfeifer, Joseph. “Understanding How Organizational Bias Influenced First Responders at the World Trade Center.” In *Psychology of Terrorism*, edited by Bruce Bongar, Lisa Brown, Larry Beutler, James Breckenridge, and Philip Zimbardo. New York: Oxford Press, 2007.

Pica, Tom. “What Is 4G and Why it Matters.” Verizon. April 30, 2012. http://www.verizonwireless.com/news/article/2012/05/what-is-4GLTE-and-why-it-matters.html.

Pitt, Leyland F., Michael Parent, Iris Junglas, Anthony Chan, and Stavroula Spyropoulou. “Integrating the Smartphone into a Sound Environmental Information Systems Strategy.” *Journal of Strategic Information Systems* 20, no. 1 (March 2011): 27–37.

Poushter, Jacob. “Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies.” Pew Research Center. February 22, 2016. http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-Internet-usage-continues-to-climb-in-emerging-economies/.

PRWeb. “Carwash Success: New DHS Policy Requires Carwash for All Mobile Applications.” April 13, 2016. http://www.prweb.com/releases/2016/04/prweb13338405.htm.

Quirlogico, Steven, Doug Hansen, Chris Dew, and Anthony Glynn. “Vetting Mobile Applications for Federal Agencies: NIST AppVet and DHS Carwash.” http://csrc.nist.gov/groups/SMA/forum/documents/january2016_presentations/FCSM_2016-AppVet-DHS-Final.pdf.

Raths, David. “Private-Sector Organizations Earn a Seat in the Emergency Operations Center.” Emergency Management. May 17, 2010. http://www.govtech.com/em/disaster/Private-Sector-Organizations-Emergency-Operations-Center.html?page=2.

Refuel Agency. “Millennial Teens.” Accessed March 25, 2016. http://research.refuelagency.com/wp-content/uploads/2015/07/Millennial-Teen-Digital-Explorer.pdf.

Robinson, Les. “A Summary of Diffusion of Innovations.” Changeology. January 2009. http://www.enablingchange.com.au/Summary_Diffusion_Theory.pdf.

Rogers, Everett M. *Diffusion of Innovations*, 4th edition. New York: Free Press, 1995.

Royden, Laura. “Now Trending #CityHall.” Data-Smart City Solutions. April 28, 2016. http://datasmart.ash.harvard.edu/news/article/now-trending-cityhall-on-social-media-824.

Scholl, Hans J. “The Mobility Paradigm in Government Theory and Practice: A Strategic Framework.” https://pdfs.semanticscholar.org/86d7/22cbc9d0c1a655b2dca9c69130c36863470b.pdf.

“Malicious Pokemon Go Apps Land in Google Play.” *SecurityWeek*. July 18, 2016. http://www.securityweek.com/malicious-pokémon-go-apps-land-google-play.

Silverman, Gary. “New York’s Top Cop Embraces Smartphone Revolution.” *Financial Times*. June 5, 2016. http://www.ft.com/cms/s/0/ea90e172-29c9-11e6-8ba3-cdd781d02d89.html#axzz4K0iZHnjc.

Sievers, Jesse. “Embracing Crowdsourcing: A Strategy for State and Local Governments Approaching ‘Whole Community’ Emergency Planning.” *State and Local Government Review* 4, no. 1 (March 2015): 57–67.

Smith, Aaron. “Older Adults and Technology Use.” Pew Research Center. April 3, 2014. http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/.

———. “The Smartphone Difference.” Pew Research Center. April 1, 2015. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

State of Washington. “Records Management Advice.” April 2015. https://www.sos.wa.gov/_assets/archives/RecordsManagement/Advice-Sheet-Capture-and-Retention-of-Text-Messages-April-2015.pdf.

Statista, “Combined Global Apple App Store and Google Play App Downloads.”Accessed November 30, 2016. http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/,2015.

Steen, Margaret. “Emergency Management: There’s an App for That.” Emergency Management. April 2, 2014. http://www.emergencymgmt.com/training/Emergency-Management-App.html?page=2.

Sternstein, Aliya. “DHS Official: Create a Government-wide Seal of Approval for Apps.” Nextgov. August 27, 2014. http://www.nextgov.com/mobile/2014/08/dhs-official-create-governmentwide-seal-approval-apps/92564/.

Sunder, S. Shyman. “NIST Response to the World Trade Center Disaster. World Trade Center Investigation Status.” NIST. October 19, 2004. https://www.nist.gov/sites/default/files/documents/el/disasterstudies/ncst/NCSTACWTCStatusFINAL101904WEB2.pdf.

Sunstein, Cass R. “Memorandum for the Heads of Executive Departments and Agencies and Independent Regulatory Agencies.” White House. April 10, 2010. https://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf.

Troboughh, John, Smita Satiana, and Andrew Stroup. “The Rebirth of the Obama Administration’s apps.gov.” *Tech Crunch*. March 14, 2016. https://techcrunch.com/2016/03/14/the-rebirth-of-the-obama-administrations-apps-gov/.

Velury, Mythreyi. “A Report on the ‘Methods Used by Free Apps to Earn Revenue and its Increasing Popularity.” *Imperial Journal of Interdisciplinary Research* 2, no. 4, (2016).

Vitiello Communications Group. “SMS Communication in Business.” October 14, 2010. http://vtlo.com/blog/sms-communication-in-business-2/.

Voas, Jeffrey, Steve Quirolgico, Christoph Michael, and Karen Scarfone. *Technical Considerations for Vetting 3rd Party Mobile Applications (Draft)* (NIST SP 800–163). Washington, DC: U.S. Department of Commerce, August 2014. http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf.

Walker, Guy H., Neville A. Stanton, Daniel P. Jenkins, an Paul M. Salmon. “From Telephones to iPhones: Applying Systems Thinking to Networked, Interoperable Products.” *Applied Ergonomics Journal* 40, no. 2 (March 2009): 206–215.

Webrevolve. “How Slack Can Help Increase Productivity and Improve Communication.” April 15, 2016. https://www.webrevolve.com/slack-can-help-increase-productivity-improve-communication/.

“Why Do We Blindly Sign Terms of Service Agreements?” NPR. Accessed November 13, 2016. http://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements.

Wilson, Richard, K. Kunene, and Sirajul Islam. “Frugal Information Systems,” *Information Technology for Development* 19, no.2 (2013). http://dx.doi.org/10.1080/02681102.2012.714349.

Wood, Colin. “The Secret behind Building Successful Mobile Apps.” *Government Technology*. April 30, 2012. http://www.govtech.com/policy-management/The-Secret-Behind-Successful-Mobile-Apps.html.

XMRFire. “Google Apps.” Accessed November 8, 2016. http://www.xmrfire.com/services/google-apps-for-fire-and-ems.

Yarmosh, Ken. “How Often You Should Update Your Apps.” *Savvyapp*. January 12, 2016. http://savvyapps.com/blog/how-often-should-you-update-your-app.

Yin, Jie, Andrew Lampert, Mark Cameron, Bella Robinson, and Robert Power. “Using Social Media to Enhance Emergency Situation Awareness,” *IEEE Intelligent Systems* 27, no. 6 (2012).

Zagorsky, Josh. “Almost 90% of Americans Have Unlimited Texting.” *Instant Census*. December 8, 2015. http://instantcensus.com/blog/almost-90-of-americans-have-unlimited-texting.

Zhang, Li, Druv Gupta, and Prasant Mohapatra. “How Expensive Are Free Smartphone Apps?” *ACM SIGMOBILE Mobile Computing and Communications Review* 16 no. 3, (July 2012).

Zorz, Zeljka. “Pokemon Go! Malicious Apps Lurk on Google Play.” Help Net Security. July 16, 2016. https://www.helpnetsecurity.com/2016/07/15/android-malware-impersonating-pokemon-go/.

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