NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EMERGENT SOCIAL SOFTWARE PLATFORMS FOR SHARING AND COLLABORATION ON CRIMINAL INFORMATION AND INTELLIGENCE

by

Richard A. Alexander

September 2012

Thesis Advisor:	Rodrigo Nieto Gómez
Second Reader:	Lauren Wollman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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

13. ABSTRACT (maximum 200 words)

Information sharing and collaboration between federal, state, and local agencies has been repeatedly stressed as a part of the national security strategy. The emphasis has been on inter-agency communication and has largely left unaddressed the need for internal information systems improvements.

This thesis will examine how Web 2.0 technology as part of an emergent social software platform (ESSP) can be used to improve intra-agency law enforcement criminal information sharing and collaboration. Challenges in implementing these technologies were also examined. Two case studies were conducted to examine current applications of Web 2.0 technologies in secure environments. The hypothesis was that ESSPs have the potential of revolutionizing policing by providing personnel with an advanced means of information sharing and collaboration. The resulting data and information will benefit internal and external intelligence activities.

Human-computer interfaces that provide ease of use along with a structure that is mission focused will aid in implementation of an ESSP. Integration with current systems and mobility are also important. However, implementing an ESSP is not simply a technical issue, but a cultural one. For any ESSP to be successful, a culture that values the free and efficient flow of information over traditional hierarchical systems is needed.

14. SUBJECT TERMS Social media, social intranet, social collaboration, knowledge management, data, big data, information, intelligence, intelligence-led policing, emergent social software platform, sharing, living intelligence, emergent intelligence, Intelink, CopBook, Intellipedia			**15. NUMBER OF PAGES** 147
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EMERGENT SOCIAL SOFTWARE PLATFORMS FOR THE SHARING OF AND COLLABORATION ON CRIMINAL INFORMATION AND INTELLIGENCE

Richard A. Alexander
Captain, Tulsa (Oklahoma) Police Department
B.A., University of Oklahoma, 1995

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
September 2012**

Author: Richard A. Alexander

Approved by: Rodrigo Nieto Gómez
Thesis Advisor

Lauren Wollman
Second Reader

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information sharing and collaboration between federal, state, and local agencies has been repeatedly stressed as a part of the national security strategy. The emphasis has been on inter-agency communication and has largely left unaddressed the need for internal information systems improvements.

This thesis will examine how Web 2.0 technology as part of an emergent social software platform (ESSP) can be used to improve intra-agency law enforcement criminal information sharing and collaboration. Challenges in implementing these technologies were also examined. Two case studies were conducted to examine current applications of Web 2.0 technologies in secure environments. The hypothesis was that ESSPs have the potential of revolutionizing policing by providing personnel with an advanced means of information sharing and collaboration. The resulting data and information will benefit internal and external intelligence activities.

Human-computer interfaces that provide ease of use along with a structure that is mission focused will aid in implementation of an ESSP. Integration with current systems and mobility are also important. However, implementing an ESSP is not simply a technical issue, but a cultural one. For any ESSP to be successful, a culture that values the free and efficient flow of information over traditional hierarchical systems is needed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CIA	Central Intelligence Agency
CRIS	Criminal Records Information Systems
CFR	Code of Federal Regulations
DNI-U	Director of National Intelligence - Unclassified
ESSP	Emergent Social Software Platform
FBI	Federal Bureau of Investigation
FOUO	For Official Use Only
IACP	International Association of Chiefs of Police
IIR	Institute for Intergovernmental Research
LEIU	Association of Law Enforcement Intelligence Units
NCISP	National Criminal Information Sharing Plan
RPD	Redlands (CA) Police Department
SAR	Suspicious Activity Report
SQL	Standard Query Language
TALC	Technology Adoption Life Cycle
TPD	Tulsa (OK) Police Department

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I felt that being selected for the NPS CHDS program was one of the top honors of my career, even before I fully realized what an incredible opportunity it had afforded me to study with some of the brightest and most dedicated homeland security leaders from across the nation. It has been a humbling experience, and I am honored to be a part of it.

I would like to thank the NPS CHDS staff and professors for their unfailing support, encouragement and enthusiasm throughout the program. Dr. Christopher Bellavita is an epitome of a great leader. Dr. Richard Bergin was essential in helping me shape my thesis. I would also like to thank my advisor, Dr. Rodrigo Nieto Gómez and Second Reader, Dr. Lauren Wollman for their guidance and support. Dr. Gomez's enthusiasm, wisdom, and vision have been truly inspiring.

I owe a special thank you to Chief Mark Garcia, Dr. Travis Taniguchi, and Sgt. Rachel Tolber of the Redlands (CA) Police Department. Their leadership in the use of social media in policing is blazing the path for the rest of the nation's law enforcement.

I would also like to thank Chief Jordan of the Tulsa Police Department, and the City of Tulsa for allowing me to participate in this endeavor. I appreciate Major Julie Harris's support and patience for those times when I was away from the office, and for when I was consumed by thoughts of paper deadlines, theses, and a variety of homeland security topics. I also want to thank my fellow officers who took up the slack while I was gone.

I want to recognize my parents, Jimmy and Connie Alexander. Their lessons on the value of perseverance and hard work, not to mention their love, have made all the difference.

This paper is dedicated to my absolutely incredible wife, Jamie, as well as my children Garrett and Riley. Without their undying love, support, and patience this paper would not have been possible. Words are not enough to express the extent of my gratitude.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> The individual, however intelligent and knowledgeable, can no longer do all the thinking. The organization needs to consider the contribution of all individuals in it, and the effect of their interactions on strategy.
>
> -Kees van der Heijden, The Art of Strategic Conversation

> The only irreplaceable capital an organization possesses is the knowledge and ability of its people. The productivity of that capital depends on how effectively people share their competence with those who can use it.
>
> -Andrew Carnegie, 1835–1919

A. PROBLEM SPACE

Policing is knowledge an intensive endeavor. The actions of police officers and support staff are dependent on knowledge including goals and objectives, available resources, criminal activity, law, etc.[1] Due to a post-9/11 focus on terrorism investigations and intelligence functions as part of the law enforcement mission, there has been an ongoing emphasis on increasing knowledge sharing between local, state, and federal law enforcement agencies. The intelligence community recognizes the importance of streamlining information sharing between these agencies as a key factor in improving their ability to prevent future terrorist attacks. The U.S. law enforcement community has seen great strides in improving interagency sharing environments, such as fusion centers, and in sharing resources online through systems, such as the DOJ's LEO.gov (Law Enforcement Online) website, and the DHS LLIS.gov (Lessons Learned Information Sharing) website. However, these and other similar resources are focused on interagency knowledge sharing and have limited value in improving intra-agency communication.

An assumption inherent in the approach of many guiding documents for the intelligence community is that information sharing within individual agencies is effective and that field personnel, detectives, and supervisors have the tools needed to contribute

[1] Paul M. Collier, "Policing and the Intelligent Application of Knowledge," *Public Money & Management* 26, no. 2 (Apr 2006, 2006), 109–116.

optimally to intelligence functions and terrorism investigations. Documents such as the *National Security Strategy*[2], *National Criminal Intelligence Sharing Plan*[3] and *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*[4] emphasize information sharing and networking between federal, state, local and tribal law enforcement agencies, as well as with other public safety agencies and the private sector. This focus is due in part to the national scope of the documents, which necessarily addresses broad based strategies. However, there is a general lack of discussion surrounding the need to improve intra-agency information sharing as well. An exception to this is the well-documented pre-9/11 information sharing barriers within the FBI that were the result of efforts to keep foreign intelligence and domestic criminal investigations separate.[5] The FBI's failed virtual case file system also demonstrates the difficulties of developing information sharing capabilities within a single agency.

In municipal law enforcement, a large percentage of officers work in patrol, an assignment that is largely an independent process involving working alone in patrol cars for the majority of their shift. This type of working environment increases the importance of technology applications for communications.[6] The tools used by law enforcement for internal information sharing have changed little in the past decade and have not kept up with the rapid changes in technology that have opened up new opportunities in communication. Email and archaic document management systems are the main methods for sharing information internally. Other systems currently used for internal information sharing are generally limited to paper distribution, records management systems, and the

---

2 *National Security Strategy* (Washington: White House, 2010]. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

3 *National Criminal Intelligence Sharing Plan* U.S. Department of Justice, 2005. www.it.ojp.gov/documents/ncisp/.

4 *Fusion Center Guideline: Developing and Sharing Information and Intelligence in A New Era* (Washington, D.C.: Dept. of Justice, Office of Justice Programs, Bureau of Justice Assistance, 2006).

5 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States.* (New York: Norton, 2004).

6 Roslin Viprakasit Hauck, "Should They Share or Not? An Investigation on the Use of Communication and Knowledge Sharing Technology in a Police Organization." (The University of Arizona), 44.

occasional chief's blog. With many of these systems, the top managers decide what information employees need to know and then provide it. Reports are created and sent into the criminal records systems, often to never be seen or heard from again. Arrests are made, but the outcome of the prosecution may never be known. Officers learn valuable lessons but are hindered in their ability to share the information outside of a classroom environment or limited interactions with other individual officers.

Each of these established systems represents vertical structures of hierarchical communication that increases knowledge flow time and reduces the ability to share knowledge among large groups of people. In addition, these systems do not provide digital knowledge repositories that would be accessible to all levels of the organizations and enable the future use of this knowledge. Improvements facilitating the flow of knowledge in law enforcement would increase the ability of officers to share information and knowledge within and between squads, shifts, and divisions to enable action based on the knowledge provided. Nissen in *Harnessing Knowledge Dynamics* refers to this process as knowing or knowledge in action.[7] Disseminating intelligence bulletins, as an example, does not have any impact, if there is no knowing as demonstrated by the actions taken by officers. Currently, feedback processes to determine the level of knowing through the action being taken by officers are also limited.

Communication systems regularly used in policing do not facilitate the capture of information within an organization. A string of emails that result in a novel solution to a problem are not likely to be captured for future reference. While email provides a means to share explicit knowledge, email systems do not allow for the sharing of the knowledge beyond the immediate recipients. Though many law enforcement agencies have moved beyond codification based on paper documentation, the structures used for the sharing of information have not changed to take full advantage of the capabilities of current technologies. Instead of having paper files scattered in offices throughout the department, the majority of information possessed by the agency is stored in digital file folders with organizational methods as varied as the individual users. Each unit has their own set of

[7] Mark E. Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning* (Hershey PA: IRM Press, 2006), 23.

digital files full of information that is usually unavailable to other areas of the department. As employees transfer and retire, the information that has been captured runs the risk of being lost in a sea of digital files and folders, or simply deleted.

Systems and processes used by the majority of the nation's police departments do not provide sufficient means for personnel to take full advantage of intelligence products, or to share and collaborate on effective practices and crime reduction efforts. Information and knowledge sharing among officers and supervisors on a problem plaguing a neighborhood is often limited to the squad room and conversations over lunch. When sharing does occur, the information and lessons learned are rarely stored and made available for future use. Currently, limited means of information and knowledge storage, and transfer results in a diminished capacity to connect the dots. Connections between sets of information resulting in knowledge that could have allowed for breakthroughs in terrorism investigations may not be made. Crimes that have a terrorism nexus may go unsolved.

Contrast the systems being used by police with those now freely available to the general public. Twitter allows the sharing of tweets (micro-blogs) at the user's whim. Hashtags help users categorize tweets for easy access. Blogs allow for knowledge sharing on topics of importance to the writer. Facebook provides the ability for users to create pages to allow those granted access to view the activities of a user. Wikis allow for collaborative work on documents. Information and knowledge can be stored and transferred at an unprecedented rate thorough the use of these tools, yet, they remain unavailable to police for internal communication. Businesses are finding that employees now desire the same level of functionality of technology within the work environment as are available in the consumer market.[8]

These tools, collectively referred to as "Web 2.0," also enable the creation of additional sources of valuable information for "big data" and new opportunities for data mining. Organizations are using information garnered from big data to innovate, to

---

8 Jeff Cummings, Anne P. Massey, and V. Ramesh, "Proceedings of the 27th ACM International Conference on Design of Communication - SIGDOC '09; Web 2.0 Proclivity," 2009), 259.

increase growth, and to improve productivity.[9] As software is developed to mine, process, organize, and interpret the mountains of new data being created daily, the importance of big data will grow exponentially.

If law enforcement agencies are to keep up with these changes in the community in which they serve, officers must also be able to exchange and interact with information and knowledge at the same rate as public consumers. Intranet systems need to be transformed into Emergent Social Software Platforms (ESSPs) where information and knowledge can easily be stored, transferred and collaborated on with minimal effort. Rather than act as conduits for prepackaged information, intranets need to be living environments that provide the ability to add, update, and change information as it evolves. Open employee-to-employee information sharing, where all employees are empowered to be information collectors, as well as information consumers, is needed to reduce the stove piping of information.[10] The end purpose is to improve efficiency in law enforcement. Unlike in manufacturing or other businesses, improved efficiency in the case of law enforcement means a quicker recognition of threats, increased awareness of ever changing crime trends, quicker identification and apprehension of suspects, improved recognition of organized crime and its connections, and an overall safer community.

Crime bulletins are regularly disseminated throughout the department. They are posted online, emailed—sometimes multiple times to the same user, and printed out. Officers and staff have access to the information, but there is no collaboration or coordination on actions suggested by the bulletin. An officer looking at a bulletin on a wanted subject may simply dismiss it other than for informational purposes, as opposed to taking action on it. If it has been a day or two since the bulletin has been sent out, it is easy to assume that another officer has already run down the leads, so following up on it would be a waste of time. Another assumption may be that if it were good information, someone would have already picked the suspect up. If an officer does follow up on

---

9 James Manyika et al., "Big Data: The Next Frontier for Innovation, Competition and Productivity," *McKinsey Global Institute, May* (2011), 6–8.

10 The Content Economy, July 4, 2010.

bulletin only to find the suspect is now driving a different vehicle, or has moved from a known residence, the newly acquired information may not be shared with others. An officer on another shift may follow up on the bulletin only to learn the same new information, again. The flow of this information, described in detail later, is disjointed. Feedback mechanisms are generally limited to one-way communications between the originator and the source of the information. Others that may be interested in updates may not be copied on an email. Direct communication, such as phone calls or conversations, stand little chance of ensuring the information is provided to all interested parties.

In other cases, information obtained is not shared due to the small amount of new information, concerns about a source's reliability, or due to the need for a formal report to be created. As part of their time management, officers must decide if the new item of information is of enough value to warrant a field interview report.[11] If the information is shared, it may take hours to days before an updated bulletin is sent out with the new information. Meanwhile, an officer working a different area may have another piece of information, such a location where the suspect likes to hang out. Had the new vehicle information been combined with a likely hangout, the suspect may have been caught. This scenario plays out multiple times a day. Traditional systems were not sufficient to capture this type of information. Fortunately, new social medial tools used within an ESSP may provide an answer.

A current challenge law enforcement agencies face is that although access to data, information, and knowledge has increased exponentially, the means of sharing administrative, operational, and criminal information in a way that allows the user to derive meaning and value from the data has not kept up with this increase. Users are lost in a sea of big data resulting in information overload and, ironically, an inability to easily share information and collaborate with other users.

[11] Otherwise known as a Suspicious Activity Report. These are structured reports used to capture information on activity of a suspicious nature.

Much of the knowledge possessed by officers is not captured due to the perceived unfriendliness of existing systems.[12] Some of the concern is due to human-computer interaction issues, such as antiquated graphical user interfaces. In many departments, Standard Query Language (SQL) is needed to access certain types of data. The data is often stored across multiple databases, each sometimes requiring a separate logon and search. Another factor is the lack of structures to informally share information. Current information systems were not developed for the purpose of making it easy for the individual user to contribute information outside of a formal processes and structures, such as is the case with the creation of reports and manuals.

Years ago, the sharing of large quantities of rapidly changing information was impractical due to the reliance on paper based codification. With the advent of digital records, codification options have increased, but systems for efficient sharing of this information still lag behind. Individually generated information and knowledge codification outside of these formal structures is limited to word documents and similar files stored in individually managed digital file folders. Shared file folders can be difficult to navigate and to locate the information being sought. This leaves a significant amount of information that is not being codified and stored in readily accessible means, despite their potential value in informing day-to-day patrol and investigations, as well as in aiding in tactical and strategic planning. Put another way, there are few mechanisms in place to incorporate individual memory into the collective or organizational memory.[13] Collective memory contributes to big data. By incorporating individual memory and making it available as part of big data, extensive information and knowledge can be derived from the individual and made available to future employees to help further organizational goals. Failing to capture individual memory greatly limits the potential ability of individually possessed information and knowledge to impact the organizational activities.

---

[12] Collier, *Policing and the Intelligent Application of Knowledge*, 109–116, 112.

[13] Maryam Alavi and Dorothy E. Leidner, "Knowledge Management Systems: Issues, Challenges, and Benefits," *Communications of the AIS* 1, no. 2es (1999), 1, 118.

In addition, the actual means for information sharing between individuals is extremely limited. Information sharing can only be successful if the systems used to store the information are readily accessible and easy to use.[14] In today's culture, with so much information as close as your smart phone, "readily accessible" denotes immediate access to information when it is needed, not when it is convenient to provide it. Squad meetings, a traditional means of knowledge and information sharing, have not changed much over the past decades. A knowledge-sharing environment that is available for a brief time per shift provides very limited opportunities for the exchange of knowledge. What is needed in today's world of rapidly changing information is living information and intelligence.

B. CHALLENGES TO ADAPTATION OF NEW TECHNOLOGY

Issues with law enforcement information sharing are centered on an over reliance on outdated modes of communication. There are a variety of reasons that law enforcement is reliant on these systems for information sharing and collaboration. Of course, implementation cost is one factor, but with the prevalence of open source tools available on the Internet, the cost factor clearly is not insurmountable. In addition, the move to updated information sharing systems could potentially result in cost savings through increased efficiencies in information sharing, and resulting improvements in work products. The primary issues that are likely to pose the most formidable challenges to the use of social media by law enforcement agencies are that of culture, technology, and privacy and legal concerns.

1. Culture

Hierarchical cultures of communication will likely be the biggest barrier to overcome. Many of the commonly used communication tools are often limited by the hierarchical structures in which they are used. In order to upload a report into the records management system, a supervisor must approve the report. To post an item on the intranet, it must first go through a person with the authority to post it. To send an email to

[14] Brian Lehaney et al., *Beyond Knowledge Management* (Hershey, PA: Idea Group Pub., an imprint of Idea Group, 2004), 22.

the entire department; staff must first approve it. These restrictions are primarily by design. Traditional hierarchical styles of leadership require careful review of communications prior to information being passed up the chain of command. For reports, a review prior to storage in the system is important to ensure accuracy and completeness. Sending an email to everyone who could potentially have an interest in its contents would quickly overwhelm inboxes. While there are well-established practical reasons for some of the limitations, the end result is that the flow of information is limited by a series of stovepipes. These systems of structured internal knowledge were not designed to facilitate informal internal knowledge.

Codification efforts within police departments often fail due in part to a cultural history that favors word-of-mouth communication and avoids the addition of increased amounts of paperwork.[15] A personalization strategy of knowledge management, as opposed to a codification strategy, is often favored by officers due to its focus on person-to-person transfers of knowledge consistent with a long history of sharing knowledge.

The development of police departments was based on a hierarchical military model that valued discipline and order over information sharing and collaboration. As the old adage goes, information is power. Control over information provided a means of exerting power over officers under a supervisor's command. Those that possess information often filter and channel it for short-term personal benefits.[16] To this day, control over the dissemination of information is valued as an indicator of the information holder's power and prestige. When a police officer's evaluation was primarily based on the number of tickets written and arrests made, the need for information sharing was of less importance.

With the advent of CompStat, intelligence-led policing, and predictive policing, the need for information sharing and collaboration has grown well beyond the capabilities of traditional hierarchical means of communication. Changing the tools will not change

---

[15] T. Dave Chavez, Michael R. Pendleton, and Jim Bueerman, "Knowledge Management in Policing," U.S. Dept. of Justice, Office of Community Oriented Policing Services, 40.

[16] Donella H. Meadows, *Thinking in System: A Primer* (White River Junction, Vermont: Chelsea Green Publ, 2010), Kindle location 3266 of 4207.

communication styles unless leaders within the traditional hierarchical systems of police agencies are able to adapt to the new technology.

2. Current Technology Acceptance

Innovators within a police agency may find resistance to new technologies due to overall satisfaction with current information systems. Officers and staff may not recognize how current technologies restrain them from operating at peak efficiency. Maintaining the status quo of current systems including email, static intranets, and traditional squad meetings may be deemed as sufficient for officer needs.

Email is a commonly used means of communication but is limited in its ability to transfer information and knowledge to those not specifically included in the email dissemination group. An email discussion resulting in new information regarding a particular crime bulletin will not be included on the intranet page where the crime bulletin is posted. Though phones and email are effective at transferring information between the two officers in this example, they do not include storage mechanisms that permit outside access to the information. Others in the chain of command, or on other shifts, may have a need for the information but will not have access to it.

Intranets, as a means of information dissemination, area positive moves forward but often still lack many modern capabilities available to the general public. The current Tulsa Police Department intranet, as an example, includes blogs and document storage, but it lacks any means of lateral transfer of, or of personalized access to, information and knowledge. It also lacks a means of easily transferring knowledge from one officer to another. Put another way, common intranets provide improvements in human-computer interactions, but they come up short when it comes to improving human-computer-human interfaces. Current police intranet systems are designed primarily to push prepackaged information that changes little over time, short of the originator republishing an update.

For example, detectives and analyst often create crime bulletins to update officers on crime trends and wanted suspects. The bulletin may include a description of the incident(s), suspect vehicle descriptions, and suspect information including photos if available. An example is shown in Figure 1. These crime bulletins are published in a PDF

format and sent out by email to select recipients, and posted on the intranet. In some cases, they are also printed and distributed at squad meetings. If an officer seeing the bulletin recognizes the suspect shown in it, this is information that would clearly be of value to all officers. However, if the bulletin needs updated on a Friday night, it may well be Monday morning before the update is posted online.

Figure 1. Example of a Crime Bulletin

In the meantime, the bulletin is outdated and effectively dead, in that no updates based on new information or action taken will be available until the creator of the document is able to make the update and redisseminate. Information sharing is treated as a process that must be limited and controlled rather than encouraged. One similarity in these systems is that it is incumbent on the user to seek out the information, or hope that it is emailed to them, in order to benefit the user. There is no means for the user to establish a pull type system, meaning a system where the user can customize the information being provided based on the individual's needs and interest areas.

Squad meetings, email, and intranets, are forms of information silos. The term "information silos" in this context refers to systems that lack of means of sharing information between the disparate systems. Information provided at a squad meeting, in

an email conversation, or on an intranet page, may not result in effective sharing between these systems, or even among the individual systems—e.g., information shared between individual officers at one squad meeting, more often than not, will not be shared at the next shift's squad meeting since no codification occurs. Most importantly, the knowledge possessed by individual employees will not be readily accessible to others once that employee transfers to another shift or division, or retires. All the knowledge the employee has developed over the years related to their experience in a particular beat or squad will be gone, unless systems are present to allow the codification of that knowledge and are used by that employee.[17]

Currently, piecemeal improvements are often made without sufficient respect to the end product that is desired. Contrary to intent, these systems could actually reduce communication through increasing complexity, or simply fail due to a lack of an overreaching implementation plan.

3. Legal and Privacy Issues

Additional areas that must be addressed in discussions concerning increasing information sharing within an organization, as well as with other organizations, is the legal and privacy issues that apply to law enforcement issues. There is a prevalent concern in law enforcement that the use of social media applications to share criminal information and intelligence, even in a secure internal environment, may violate existing federal and state statutes. The laws usually referenced are Title 28 of the Code of Federal Regulations, part 23 (28 CFR Part 23), and the 1976 Privacy Act. Due to the importance and complexity of these statutes and their appropriate application, Chapter V will be dedicated to coverage of this issue. A key part of this discussion will revolve around the issue and definition of intelligence. To understand the laws that impact information and intelligence sharing, there must be a clear understanding of what the terms of information and intelligence actually mean. The handling of intelligence information within federal data systems is strictly regulated and controlled. The same regulations apply to state and local systems that received certain federal grant funding. Other state and local systems

[17] Lehaney et al., *Beyond Knowledge Management*, 23.

voluntarily adopt 28 CFR Part 23 as a nationally recognized guideline for the responsible handling of intelligence. The question that then follows is, when does information and knowledge become classified as "intelligence?" Academic literature, books on intelligence, and 28 CFR Part 23 have differing interpretations. The issue is further clouded due to 28 CFR Part 23 having been published in 1980 with revisions made in 1993.[18] This regulation was not designed to address the sharing of information over the Internet or within the context of social media and ESSPs. Needless to say, this complicates information sharing efforts that either are required to or choose to follow this regulation.

C. HYPOTHESIS/TENTATIVE SOLUTION

The author's hypothesis is that an Emergent Social Software Platform (ESSP), which allows for open, secure discussions by officers, staff, detectives, and other authorized personnel, may greatly improve the ability of police departments to communicate in order to effectively fight crime and address other community concerns. This hypothetical system would be based on currently existing tools, and implemented and operated in a manner that takes into account the cultural, technological, and legal concerns. The system could also be used to capture the experience and knowledge of officers used to address a wide variety of issues. Another key element of this system would be the integration of the currently disparate storage and information resources currently being used. An ideal system would greatly simplify person-to-person communication and human-computer interaction by incorporating elements of email, records management systems, intranets, document management software, and a variety of information sources. Further efficiency would be gained by the removal of communication intermediaries that slow down or prevent the free flow of information.

There seems to be belief in law enforcement, as in other organizations, that if you gather enough data, answers to ongoing problems will manifest themselves and provide self-evident paths for future action. The reality is that data is of limited value to most

[18] "28CFR FAQ," http://www.iir.com/28CFR_Program/~/Home/28CFR_Program/28CFR_FAQ/#q6.

patrol officers and detectives without the context provided by information and knowledge. Even then, the existence of information and knowledge within an agency has little to no value, if it is not accessible to the users. As accessibly increases, so does the value.[19] A caveat to this is that large amounts of information and data, so called "big data" may prove to be of significant value to analysts and planners.

Though one system may not be able to address all the problems with how information is currently shared and collaborated, ESSPs may provide a solution that addresses many of the issues. A crucial need at this time is a vision to work towards that would meet the communication and knowledge management needs of officers.

D. RESEARCH QUESTION

Primary question:

How can Web 2.0 technology and emergent social software platforms be used to improve intra-agency law enforcement criminal information sharing?

This leads to a secondary question:

What are the challenges in implementing emergent social software platform criminal information sharing in a policing environment?

After gathering data on how Web 2.0 technology and emergent social software platforms are being used for information storage and transfer, and how they are being applied internally in private and government environments, the methods that are found to be successful will be used to develop recommendations for their implementation and use in a law enforcement environment.

E. SIGNIFICANCE OF RESEARCH

Historically, policing has been primarily a reactive process. Traditional measures of success included arrest data, the number of tickets written, response time to calls, etc. With the advent of CompStat and Intelligence-led policing, there has been an increasing

[19] Thomas H. Davenport and Laurence Prusak, *Working Knowledge: How Organizations Manage What They Know* (Boston, Mass: Harvard Business School Press, 1998), 18.

focus on the reduction of crime through proactive efforts.[20] This change is bringing knowledge management, information sharing, and collaboration to the forefront of policing. While an individual's access to data and related analysis is an essential element needed to address crime issues, the actual practice of policing is not a solitary practice. Though police staff provides goals and objectives, and resources, it is the communication in and between squads, analysts, detectives, supervisors and other personnel that has the biggest potential to positively impact crime reduction efforts. Drapeau and Wells describe this process within an agency as *inward sharing;* otherwise described as intra-institutional sharing or the sharing of information within a department.[21] Inward sharing has the potential to reduce the knowledge gaps that exists between officers in the field, detectives, analyst, and staff. Emergent Social Software Platforms (ESSPs) expands the ability between employees for inward sharing and offer the potential to improve human-computer interactions to increase access the value of data.

[20] Collier, *Policing and the Intelligent Application of Knowledge*, 109–116, 110.

[21] Mark Drapeau and Linton Wells, "Social Software and National Security an Initial Net Assessment," Center for Technology and National Security Policy, National Defense University, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497525, 7.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

One of the challenges of research into Web 2.0 social media as applied to social intranets is the limited research in this area. Use of social media as an internal communication tool is less documented in contrast to the more common application of Web 2.0 technologies in social media designed to interact with the general public. In this context, Web 2.0 can also be referred to as Enterprise 2.0 and Government 2.0.

Web 2.0 includes concepts such as social networking, micro-blogs, wikis, RSS feeds, and media sharing, among others. Research on integrating Web 2.0 technologies in corporate environments, let alone internal law enforcement environments, is limited. Most of the research this researcher has found focuses on the use of these technologies as a marketing tool or as a tool for improving communication and interaction with the public. Even though research on Web 2.0 implementation in policing may be lacking, the research on core concepts behind it is not. These include network structures, intelligence processes, knowledge management, and information sharing.

A. CURRENT RESEARCH ON COLLABORATIVE SOFTWARE

One first step in researching how technology can be used in the intelligence process to improve information sharing and collaboration is to observe how the technology is currently being used. Organizations examined included private industry, intelligence agencies, and other governmental agencies.

A 2001 paper entitled *Building an Infrastructure for Law Enforcement Information Sharing and Collaboration: Design Issues and Challenges* delves into the basic problems law enforcement personnel face when attempting to gather information. The authors address the need for a single user interface or portal that allows officer direct access to the vast amount of information that is currently available.[22] The authors also recognize the need to filter the information, so that the information relevant to the user is available and not lost in an ocean of data. The creation of information monitoring

[22] Michael Chau et al., "Building an Infrastructure for Law Enforcement Information Sharing and Collaboration: Design Issues and Challenges,"

systems and personalization tools is recommended. Their research shows that searches used for information access could be improved through data mining and machine learning techniques.[23] Though this paper is somewhat dated, most of the problems described still exist in law enforcement today, and the insights provided are still relevant. One of the advantages of today's perspective is that we can readily find examples of data mining and improved search functions, as well as other social media tools in commercial applications used by companies such as Amazon, Google, and Facebook.

Shortly after the events of 9/11, the Defense Advanced Research Projects Agency (DARPA) created a program with the objectives of developing "a technology architecture and infrastructure to support collaboration, analytical reasoning and information sharing between analysts in different agencies and organizations…"[24] This program has a broad focus intending to address federal, state, and local authorities, but the research also has direct application to internal sharing applications. A 2004 DARPA research paper discusses the need for collaborative applications in the intelligence environment. Current information sharing structures are designed for large environments where broad scale information sharing is needed. Such centralized structures do not facilitate collaboration among small teams. The systems were not designed for sharing or collaboration and do not provide the mechanism needed in today's quickly changing environment. The primary use of these systems, intended or otherwise, is their use as an information silo or document repository.[25]

The researchers also cover "edge-based technology." The term applies to information that is created and stored on the "edge" of a noncentralized network. Contrary to traditional systems, these emergent edge-based systems are not geared towards broad information storage or dissemination. The article goes on to discuss how organizations can increase productivity by implementing web-based technology, methods

---

23 Hsinchun Chen et al., "COPLINK: Managing Law Enforcement Data and Knowledge," *Communications- ACM* 46 (2003), 28–34.

24 Margaret Arney, Brad Cohen, Brad Medairy, and Booz Allen Hamilton, "Impact of Advanced Collaborative Architectures on Intelligence Analysis" 2004), 3176.

25 Ibid.

and processes that already exist within the intelligence community.[26] The authors' conclusion is that "an advanced collaborative architecture creates an extremely powerful and flexible collaborative system." This system can be used to not only increase the creation of internal collaborative efforts but also those with other organizations.[27]

Current research on other collaborative software was often limited to a few articles or web pages on the topics. Though often focused on single software applications, the articles and other nonacademic sources provide a general idea of the state of current and future software and applications. Additional research is needed on how these programs are increasing collaboration and aiding agencies in their efforts to achieve their goals and objectives.

B. WEB 2.0

There is no shortage on research and publications on Web 2.0 technologies. A paper by Kaplan and Haenlein provides an in-depth discussion of social media concepts. The authors provide distinct definitions of the terminology and elements involved.[28] This is unusual in that many authors seem cautious in establishing concise definitions, which is probably due in part to the rapidly changing aspect of the terms and technologies. Web 2.0 is also referred to as social media, Enterprise 2.0 (in the corporate environment), and Government 2.0. In the Kaplan and Haenlein definition, the term of social media is limited to publically available websites. This places government and enterprise efforts at improving collaboration within the internal work environment under the umbrella of Web 2.0 rather than the more specific concept of social media. Understanding the differences between the two should help to focus future research. Despite this, the technologies used by Web 2.0 and social media are often used interchangeably and can be difficult to distinguish. Nissen uses the term "groupware" to describe tools that support knowledge

---

26 Margaret Arney, Brad Cohen, Brad Medairy, and Booz Allen Hamilton, "Impact of Advanced Collaborative Architectures on Intelligence Analysis" 2004), 3178–3179.

27 Ibid.

28 Andreas M. Kaplan and Michael Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media," *Business Horizons* 53, no. 1 (2, 2010), 59–68.

work. He gives the examples of email, chat, and discussion boards, all of which fall under the Web 2.0 umbrella. According to Nissen, groupware includes infrastructure tools that are used to provide support for knowledge work. Groupware facilitates the creations and management of data, information, and knowledge. These tools can be especially valuable in environments where face-to-face communication is impractical. [29] Nissen distinguishes web portals and search engines from other technology infrastructure. He credits these additional tools as providing a higher level of contribution to knowledge management. A knowledge management program that provides infrastructure and more advanced tools, such as web portals, may improve the transfer of knowledge, but interpersonal interaction is still the central to knowledge transfer.

The 2008 article *Change Your World or the World Will Change You* provides an introduction to Web 2.0 in the context of government agencies.[30] While very brief in its approach, the article provides a general understanding of how Web 2.0 can be used to improve government services and operations. *What is Web 2.0?* provides a thorough introduction to Web 2.0 concepts geared towards the business environment.[31]

In his paper, *The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community*, Andrus writes about the need for Web 2.0 technology to be integrated into the intelligence environment. He uses Complexity Theory to provide a framework under which the intelligence community can adapt to a continuously changing environment.[32] Web 2.0 tools, such as wikis and blogs, can be used to bring about the changes needed. While Andrus does not specifically address the intelligence cycle, he writes about the crucial role feedback technologies play in an intelligence framework based on the

---

[29] Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning*, 23.

[30] Paul Macmillan, Andrew Medd, and Peter Hughes, "Change Your World or the World Will Change You " Deloitte, http://www.deloitte.com/view/en_EC/ec/792ebd7690794210VgnVCM100000ba42f00aRCRD.htm.

[31] Tim O'Reilly, "What is Web 2.0?" O'Reilly Media.

[32] D. Calvin Andrus, "Toward a Complex Adaptive Intelligence Community — Central Intelligence Agency " https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Wik_and_ Blog_7.htm, 12.

Complexity Theory.[33] Feedback, also referred to as evaluation, is a key step in the intelligence cycle. Though Andrus stresses the importance of the role of feedback technologies, he does not provide substantial detail on these particular technologies. Andrus makes a particularly interesting prediction that once wikis and blogs are fully integrated into intelligence community operations, "the nature of Intelligence will change forever." [34] This paper is a key source of information on the use of Web 2.0 for improving intelligence, and it is believed to have inspired the CIA version of the wiki, Intellipedia. [35]

The authors of the paper *Web 2.0 Proclivity: Understanding How Personal Use Influences Organizational Adoption* researched the connection between the uses of Web 2.0 in a user's personal life and how the usage affects the success or failure of organization Web 2.0 adoption. This is a crucial concept to consider due to its impact on technology adoption efforts. Ideas abound about how to improve intelligence operations, but more often than not fall short when it comes to implementation. The research involved submitting 4,500 surveys to employees of a Midwestern company. Not surprisingly, the researchers found that there is a positive relation between a user's personal use of Web 2.0 technologies and their adoption of those technologies in a corporate environment.[36] The study also found that executive support for Web 2.0 implementation was found to have little impact on a user's likelihood of adopting the technology.[37] It suggests that a bottom up approach may be needed to ensure the successful adoption of Web 2.0 technologies. The study did not address how adopting Web 2.0 technologies impacted the company.

Research into general Web 2.0 concepts is comprehensive. Additional research on how Complexity Theory applies to Web 2.0 may prove to be beneficial. Specifically,

---

33 D. Calvin Andrus, "Toward a Complex Adaptive Intelligence Community — Central Intelligence Agency " https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Wik_and_ Blog_7.htm, 12.

34 Wikipedia contributors, "Intellipedia," Wikipedia, en.wikipedia.org/wiki/Intellipedia.

35 Ibid.

36 Cummings, Massey, and Ramesh, *Proceedings of the 27th ACM International Conference on Design of Communication - SIGDOC '09; Web 2.0 Proclivity* , 257, 262.

37 Ibid.

applying the Cynefin Framework along with Complexity Theory may help in understanding how Web 2.0 applications can help sort through complex communication.[38]

C. KNOWLEDGE MANAGEMENT

As part of the research, this researcher examined how elements of knowledge management, can be improved through the use of Web 2.0. Knowledge management involves four basic processes that include creating, storing/retrieving, transferring, and applying knowledge.[39] Although this paper is focused on the areas of information sharing and collaboration, a general discussion of knowledge management literature is also needed to provide clarity to the terms being used. Any system that facilitates communication to include information and knowledge sharing is in fact a type of knowledge management system.

Lee and Lan define knowledge management as "a process of creating intangible assets from the combination of knowledge and experience provided by the individuals or knowledge workers within the organization or system."[40] Knowledge management has traditionally focused on the storage of knowledge in a central knowledge repository and accessibility. Contemporary knowledge management has shifted focus to a conversational approach that emphasizes integration and collaboration.[41]

Plenty of evidence demonstrates that knowledge management can both benefit from the adoption of Web 2.0 technologies. As with the previously mentioned DARPA study, a 2007 paper by Lee and Lan addresses the limitations and future of current information, or knowledge management, processes. While knowledge management has traditionally focused on the collection of knowledge in a central repository, the

---

[38] Cynefin is a theoretical model used to describe problems, situations and systems.

[39] Maryam Alavi and Dorothy E. Leidner, "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues," *MIS Quarterly* 25, no. 1 (2001), 107–136, 113.

[40] Maria R. Lee and Yi-Chen Lan, "From Web 2.0 to Conversational Knowledge Management: Towards Collaborative Intelligence," *Journal of Entrepreneurship Research* 2, no. 2 (2007), 47–62, 51.

[41] Ibid., 51.

integration of it with Web 2.0 technologies allows for the creation of knowledge networks. These knowledge networks foster the creation of dynamic knowledge and collective intelligence. The authors identified a "pressing need to identify the current state of organizations or community groups pursuing collaborative intelligence." [42]

The terms information and knowledge are sometimes used interchangeably, which can create confusion. This is further complicated by the use the term of "knowledge management" that is used to describe processes that include information and data, as well as knowledge itself. Davenport and Prusak emphasize the importance of making clear distinctions between the terms.[43]

The knowledge hierarchy is a tool that can be used to conceptualize data, information, and knowledge. Knowledge lies at the top of the hierarchy and is differentiated by the highest level of actionability while having the lowest abundance. The definition of knowledge, as provided by Nissen, is information combined with data "that enables direct action."[44] Knowledge is also said to be highly contextualized information as shaped by individual interpretation and experience.[45] A dictionary definition of knowledge is "something that may be known; information."[46]

Some researchers take a more constrained view of knowledge by labeling it with the quality that it exists only in the realm of the mind. Once the knowledge is articulated and made explicit, it becomes information.[47] Others describe it as both a state of mind and an object by positing that it originates and is applied in the mind but can be codified into documents and digital storage mediums, as well as in organizational routines,

---

[42] Maria R. Lee and Yi-Chen Lan, "From Web 2.0 to Conversational Knowledge Management: Towards Collaborative Intelligence," *Journal of Entrepreneurship Research* 2, no. 2 (2007), 47–62.

[43] Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know.*

[44] Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning*, 250.

[45] Kowta Sita Nirmala Kumaraswamy and C. M Chitale., "Collaborative Knowledge Sharing Strategy to Enhance Organizational Learning," *J.Manage.Dev.Journal of Management Development* 31, no. 3 (2012), 308–322.

[46] "Knowledge," Dictionary.com, http://dictionary.reference.com/browse/knowledge?s=t.

[47] Alavi and Leidner, *Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues*, 107–136, 108.

processes, practices, and norms.[48] Knowledge can be categorized as personalized information, a state of mind, an object, a process, access to information, and capability.[49]

Conversely, information is defined as that which "provides meaning and context for action.."[50] Davenport and Prusak refer to it as "data that makes a difference" by providing relevance and purpose to data.[51] Information lies between data and knowledge in the hierarchy. Information has a lower abundance but greater actionability than data.[52]

Data, defined as "a set of discrete objective facts about events,"," lies at the lowest level and is differentiated from the other levels in the hierarchy by being in the greatest abundance and having the lowest actionability. [53] [54] Data's primary importance is that it provides the building blocks needed for the creation of information. It is important to understand what data does not do. Data does not provide any judgment, interpretation, or basis for action. [55] Data without the application of knowledge and information is of limited value.

Nissen points out that each of the hierarchical levels is interrelated, with far more complexity than indicated by the simple hierarchy. For instance he notes, "Knowledge without data is insufficient for action."[56] Nissen also notes the difference between knowing and knowledge. Knowing refers to knowledge in action. Without the application of knowledge, to include data and information, there is no knowing, and hence, there is a knowledge gap that exists between knowledge and knowing. In these situations, even

---

[48] Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*, 5.

[49] Alavi and Leidner, *Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues*, 107–136, 111.

[50] Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning*, 49.

[51] Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*, 3.

[52] Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning*, 49.

[53] Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*, 2.

[54] Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning*, 49.

[55] Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*, 2.

[56] Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning*, 21.

though the organization may possess the knowledge needed to prevent mistakes, without the application of this knowledge, there may be no knowing, and hence, a repetition of the mistakes.[57]

Regardless of the amount of latent knowledge in storage, without investment in the tools and systems needed to apply this knowledge, the full value of the knowledge cannot be realized.[58] Vast amounts of knowledge, if not accessible and available in the appropriate context, have little more value than information or even data. Systems are needed, in part, to facilitate the transfer and sharing of knowledge in a way that has meaning to the user. Web 2.0 technologies address only one aspect of knowledge transfer. The U.S. Army defines knowledge transfer as "The movement of knowledge—including knowledge based on one's expertise or judgment, from one person to another."[59] Knowledge transfer consists of two components, the transmission of information and the absorption of the information.[60] Web 2.0 is ideally suited to facilitate the transmission of information. However, knowledge transfer also involves the absorption of knowledge by the intended audience. Simply making information available does not guarantee that it will be absorbed, much less acted upon. There are a number of reasons why the user may not absorb information. These include a human-computer interfaces, organizational cultural barriers, and relevance, among others.[61] Ensuring absorption is a complicate matter that relies heavily upon the culture in which the Web 2.0 technology is implemented.

The terms "transfer" and "sharing" can be difficult to distinguish. Knowledge sharing has been defined as "a set of behaviors that involves the exchange of information

---

57 Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning*, 71–74.

58 Ibid., 75.

59 *Knowledge TransferTthrough People*, United States Strategic Command Knowledge Transfer Office, 2009), 12, 5.

60 Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*, 101.

61 Ibid.

or provision of assistance to others."[62] Another definition is "inducing knowledge to flow between different people or organizations."[63] Nissen defines knowledge transfer as simply, "sharing knowledge locally" but differentiates it as a subset of knowledge sharing that he associates with tacit knowledge and broad organizational reach.[64] In contrast, Davenport and Prusak use the term knowledge transfer in a broader sense that includes knowledge sharing.[65] Lehaney, et al., forgoes the term of knowledge transfer all together and uses the term of knowledge sharing.[66] In some writing, the term of sharing seems to take on a more personal context emphasizing individual interactions. The differences between the terms of sharing and transfer are subtle enough to be of little significance to this paper.

Regardless of terminology, the transfer and sharing of knowledge in an unstructured format is vital to an agencies success. An essential element of knowledge management is to facilitate the transfer of knowledge and information through specific strategies that encourage spontaneous exchanges.[67] While Web 2.0 tools may capture knowledge, if one takes the view that knowledge is primarily a product of the mind, Web 2.0 is essentially a tool for sharing information. For the purpose of this paper, the term "information" is be used to describe objects, usually text, that are used to give meaning and relevance to data.

ESSPs provide potential virtual meeting areas for information transfer, whether or not the information shared is transformed into knowledge will be based on the perspective and actions of the individual user. For this reason, this paper primarily focuses on information, but the close relationship of information and knowledge may

---

62 Brian D. Janz and Pattarawan Prasarnphanich, "Understanding the Antecedents of Effective Knowledge Management: The Importance of a Knowledge-Centered Culture," *Decision Sciences* 34, no. 2 (2003), 351–384.

63 Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learning*, 255.

64 Ibid.

65 Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know.*

66 Lehaney et al., *Beyond Knowledge Management.*

67 Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*, 89.

often blur the attempts at distinguishing the two terms within the processes being studied. In addition, the term "knowledge" may be used on occasion in the dictionary sense described above though care will be taken to limit its use in this sense.

Data, information, and knowledge are of little benefit, if they do not result in action. Codification's main function is to put information and knowledge into an accessible form that can be used as a basis for action.[68] Knowledge can be transformed and given permanence by putting it into "forms that can be shared, stored, combined, and manipulated in a variety of ways."[69] Unlike traditional codification strategies, ESSPs expand the ability to codify information from throughout the organization by empowering employees to digitally share personal knowledge.

Not all of an agencies' knowledge must, or should be codified. Relevance to the operational goals should be the key factor in determining what information should be codified.[70] In addition, Codification in and of itself does not provide value if the information is not accessible to the user in a context where it may be applied to assigned tasks. However, codification remains an essential step needed to provide value to information and knowledge within an organization.[71]

---

[68] Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*, 69.

[69] Ibid., 87.

[70] Ibid., 69.

[71] Ibid., 85.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESEARCH METHODOLOGY

For this research, the researcher conducted case studies of the Redland (California) Police Department and *Intelink*. An appreciative inquiry approach helped shape the research approach by encouraging the researcher to seek out the successful elements and factors organizations applied, through the use Web 2.0 technologies, to improve intra-agency knowledge flows, specifically, in regards to information sharing and collaboration. As referred to earlier, Lee and Lan stressed the importance of identifying the state of efforts by organizations and other groups in pursing collaborative intelligence.[72]

By identifying and focusing on the behaviors involved with the implementation and operation of Web 2.0 technologies used by these organizations, this researcher intends to evaluate their potential application to an emergent social software platform (ESSP) in a secure law enforcement environment.

A. SAMPLE DATA

Many law enforcement agencies have adopted social media for use as a tool for improving public relations and for providing timely information on crime. However, there is little research and data regarding the use of Web 2.0 technologies and ESSPs for facilitating the sharing of information in an internal law enforcement intranet environment.

To study the potential of ESSPs and Web 2.0 technologies in law enforcement intranets, the research was expanded beyond the limited examples of social media use in local police agencies to include other government agencies, including federal agencies and private corporations. This researcher compiled a list of organizations that were researched and contacted for further information regarding their social intranet system. Based upon the initial research, the two previously mentioned organizations were selected for an in-depth analysis. Selection criteria that were considered included

[72] Lee and Lan, *From Web 2.0 to Conversational Knowledge Management: Towards Collaborative Intelligence*, 47–62.

application in a policing environment, the level of information availability, the variety of Web 2.0 applications, types of data managed, and security requirements.

B. DATA COLLECTION

Practitioners and information technology from the two organizations were contacted by email and phone. The following information was requested:

- Strategies, plans and design documents for the implementation of social media tools
- Data and process flow diagrams
- Descriptions of integration levels with information systems
- Standard operating procedures
- Legal and security documentation (policies, procedures, and technological means of protecting data)
- Narrative descriptions of challenges overcome in implementation and success stories regarding the use of the system
- Statistical documentation on adoption and usage rates or related information

The level of available data is expected to vary to the relatively recent adoption of Web 2.0 in social intranet environments, as well as varying organizational documentation practices and other factors.

C. DATA ANALYSIS

The data analysis will include the review of the applications, correspondence, research notes, and other documents. As applicable, process models will be used to reflect the flow of data in the systems analyzed. The purpose of the research will be to evaluate the research data for the purpose of discovering the elements and factors involved in the design, development, implementation, and use of the social intranet system in the organizations studied to determine the viability of ESSPs in a police

environment. The research will be centered on the portions of the system that enable information and knowledge sharing. In addition, the relationship of these elements to the facilitation of collaboration will be reviewed.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EMERGENT SOCIAL SOFTWARE PLATFORMS

While many legacy computer systems simply automated and further codified old business practices and organizational structures, Emergent Social Software Platforms (ESSPs) offer the potential to help move police agencies to new age in communication.

ESSP is a term used to describe the websites that incorporate Web 2.0 tools. ESSP can be better understood by breaking it down into its three elements: emergent, social software, and platform. Emergent describes the patterns and structures created by interaction of the user's over time. The emergent nature is fostered by the use of voluntary and open systems that do not use traditional hierarchical structures.[73] "Emergent" focuses on the nonlinear aspects of a system that includes "adaptive, dynamic, goal-seeking, self-preserving, and sometimes evolutionary behavior."[74] Social software refers to the tools that allow direct interaction between users to include making initial connections and being able to create and participate in online communities. Platforms are another way of referring to the web sites that provide an environment for the social software interaction to take place. Unlike some communications mediums, such as telephone and email, the interaction between users is visible to other users and made available for future reference. [75] "Social intranet" is an alternate term used to describe ESSPs that are used in an internal secure environment.

An ESSP would be classified as a self-organizing complex system due to the lack of (stringent) central control and simple rules of operation. These qualities allow for complex collective behavior and the ability to adapt over time.[76] The benefit of ESSPs as

---

[73] Andrew McAfee, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges,* Harvard Business School Press, 2009), 69.

[74] Meadows, *Thinking in Systems: A Primer*, Kindle location 364 of 4207.

[75] McAfee, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*, 69.

[76] Melanie Mitchell, "Complexity a Guided Tour," Oxford University Press, Kindle location 312 of 7309.

a complex system is their increased ability to capture and store large amounts of information and to make it available in an easily used format.[77]

Enterprise 2.0 is a term used to describe the application of ESSP in a business environment. Unlike the term of Government 2.0, which focuses almost solely on government agencies and their use of Web 2.0 to connect with the public, Enterprise 2.0 emphasizes the use of Web 2.0 to improve internal collaboration and communication in addition to its use to improving customer and other outside engagement. Enterprise 2.0 is also associated with flattening hierarchies, harnessing the knowledge and experience of employees, and empowering employees to become an active participant in developing organizational strategy.

Though Enterprise 2.0 may be primarily associated with technology, at its core, it is policy. Policy is closely intertwined with culture. Any move towards the use of Enterprise 2.0 tools must also involved changes in policy and culture. As shown in Table 1, Enterprise 2.0 denotes a shift from hierarchical and rigid operations to a culture that values networking, collaboration, and flexibility. Information access becomes personalized and available from multi sources, regardless of hierarchical structures. Decision making is pushed down to those with immediate access to the changing needs and demands of the organization. However, to understand the cultural changes facilitated by, and part of, Enterprise 2.0, a basic understanding of Enterprise 2.0 technology in the traditional sense is needed.

[77] Melanie Mitchell, "Complexity a Guided Tour," Oxford University Press, Kindle location 728 of 7309.

Dimension	Enterprise 1.0	Enterprise 2.0
Operating model	• Hierarchical • Rigid	• Networked • Collaborative • Flexible
New models of service delivery	• One-size-fits-all • Monopoly • Single channel	• Personalized • Choice-based • Multi-channel
Performance-driven	• Input-oriented • Closed	• Outcome-driven • Transparent
Decision making	• Spectator	• Participative

Table 1. Enterprise 1.0 and 2.0 Comparison (adapted from *Change Your World*)[78]

Enterprise 2.0 is closely tied with Web 2.0 technologies but is distinguished by its application in an enterprise environment. Emergent social software platforms (ESSPs) are designed to facilitate communication and collaboration among users, as well as to capture user knowledge and harness the potential of connections between people, systems and data.[79] According to Andrew McAfee, an Associate Director for the MIT Center for Business Intelligence, Enterprise 2.0 is the use of these ESSPs by an organization to pursue its goals. These platforms can be used to within companies or expanded to include other companies, customers, and users. Characteristics of an ESSP include the ability for users to collaborate through the use of online technology in which interactions that are visible by the entire community. "Emergent" refers to the tendency of these platforms to form patterns and structures through uses of the system that may not have originally been anticipated. These systems are usually freeform in nature meaning that their use is not required, and the data input may come in many different forms. They also do not follow typical formal hierarchical structures.[80] It's anticipated that Enterprise 2.0 tools will

78 Macmillan, Medd and Hughes, *Change Your World or the World Will Change You*, 9.

79 *The Social Enterprise: Using Social Enterprise Applications to Enable the Next Wave of Knowledge Worker Productivity*, Oracle, 2008), 6.

80 Andrew McAfee, "Shattering the Myths about Enterprise 2.0," *Harvard Business Review* 87, no. 11 (2009), 1.

reduce the use of email and other outdated applications that do not allow for transparency or the wide spread sharing of information. Replacing these outdated applications with asynchronous Web 2.0 tools can increase productivity, efficiency, and the flow of information.[81]

Key elements of the ESSP concept include allowing users the freedom to create and modify content without the controls and conditions usually associated with formal information systems. ESSPs facilitate the capture and location of information, harness collective intelligence and wisdom, allow for frequent updates of information, and allow for the creation of a knowledge database.[82]

One element typically associated with ESSPs is the lack of anonymity. Unlike many Web 2.0 tools used in the public arena, which allow for anonymous interaction with the system, ESSPs typically require identification of the contributor—doing so helps avoid some of the problems that come with anonymity in the online world. Some anonymous users may vandalize wikis by deleting information or by entering false or derogatory comments. Anonymous responses to blogs may be unnecessarily rude or otherwise inappropriate. In the public arena, administrators or other users may quickly resolve these issues.[83] With an ESSP, requiring a log on that includes the contributor's identity circumvents these problems.

Unlike traditional media such as television, newspaper, and most intranets, Web 2.0 technologies are dependent on and benefit from user participation and content generation. ESSPs offer a path to transform intranets in becoming as versatile and malleable to a user's needs and business interests as the Internet is today. [84] The following section will go into more depth on the most common of these tools.

---

81 Anria Sophia van Zyl, "The Impact of Social Networking 2.0 on Organizations," *Electronic Library, the* 27, no. 6 (2009), 906, 911.

82 Andrew McAfee, *Shattering the Myths about Enterprise 2.0*, 2.

83 Don Tapscott and Anthony D. Williams, *Wikinomics: How Mass Collaboration Changes Everything* (New York, NY [u.a.]: Portfolio/Penguin, 2010), 73.

84 *The Social Enterprise: Using Social Enterprise Applications to Enable the Next Wave of Knowledge Worker Productivity*, 6.

A. WEB 2.0/ESSP COMPONENTS

1. Profile/Portal Pages

Profile, or portal, pages are a common component of social networking sites including Facebook, Google+, LinkedIn, and others. Profile pages are web pages that are focused on the individual user. These pages allow the user to post comments for viewing by others. The pages also allow the user to share photos, videos and other files, as well as to provide contact information.[85] These pages automatically update to include new bookmarks, track changes, and highlight new postings.[86]. Profile pages provide a means for users to identify and contact users that may have specialized knowledge, work on a project, or share an interest in a certain topic. The CIA is using a similar technology to help connect members of the intelligence community including outside agencies such as the FBI and NSA.[87]

2. Really Simple Syndication (RSS)

RSS provides an easy means for keeping up with changes in sites of interest by providing an update whenever a change is made. The user controls the frequency of the updates. RSS updates, called feeds, are accessed through software aggregators that monitor the sites for changes and then display a link and sometimes a short summary of the item of information. Freed from the various source web pages, users are able to view multiple RSS feeds on a single page displaying what has been referred to as the "collective mind."[88] Through this aggregation, RSS can greatly reduce time a user spends checking both internal and external sites for changes.[89]

---

[85] Kaplan and Haenlein, *Users of the World, Unite! the Challenges and Opportunities of Social Media*, 59–68, 63.

[86] *The Social Enterprise: Using Social Enterprise Applications to Enable the Next Wave of Knowledge Worker Productivity*, 5.

[87] Sharon Gaudin, "THE GRILL: Andrew McAfee," *Computerworld* 44, no. 7 (April 5, 2010, 12–14.

[88] Dick Stenmark, "Web 2.0 in the Business Environment: The New Intranet or a Passing Hype?" 2008).

[89] Andrew McAfee, "Enterprise 2.0: The Dawn of Emergent Collaboration," *Engineering Management Review, IEEE* 34, no. 3 (2006), 25.

3. Wikis

As popularized by the nonprofit website, Wikipedia, wikis are an online collaborative system for creating and editing a web pages content. It was designed as an online meeting place. Any user is permitted to create a new page or edit an existing one. Like most of the Web 2.0 elements, wikis are web based and accessible through a browser. Finding information is done through searches due to the vertical structure of wikis. In addition, relevant pages may be linked together making it easy to find information on a related topic.

One of the strengths, and perceived weaknesses, of a wiki is the lack of editorial oversight or approval of items being posted. The accuracy of the information provided in a wiki is based on input and alterations resulting in the emergence of a degree of consensus from users. A discussion page is available for ongoing discussion about disputed material and potential changes needed.

Compared to email, wikis support higher communication efficiency not limited by silo like information exchanges between small groups of individuals. A primary benefit is the ability for information captured in the wikis centralized and shared system to evolve, expand and improve over time through the involvement of multiple employees, experts, and users.[90] Giving users access to the latest versions of documents, as provided in a wiki format, contributes to understanding and increases knowledge through user input including edits, annotations, and links.[91]

4. Blogs/Micro-blogs

Blogs are simply a web page where the author may post his or her writings for the world to see. Users are able to respond to the article to provided feedback or begin a conversation with the author and other readers. In an internal police environment, blog postings could be used to start a dialogue about successful crime reduction efforts,

---

[90] San Murugesan, "Understanding Web 2.0," *IT Professional* 9, no. 4 (2007), 36.

[91] van Zyl, *The Impact of Social Networking 2.0 on Organizations*, 912.

training, administrative issues, or on any number of other areas. Unlike wikis, blogs are usually managed by a single use. Many companies use blogs to inform customers and employees alike.[92]

Micro-blogs, such as Twitter and Facebook, allow users to send a short amount of text (usually 140 characters or less) to other users. These messages can be sent and retrieved from a variety of different devices and software. Micro-blog postings, unless sent as a direct message, are available to any user. A user may subscribe to, or follow, other users postings, otherwise known as a "stream," or search other micro-blog postings. As compared to blogs, micro-blogs are more casual in nature.[93]

5. Social Bookmarking/Tagging

Tags are user-selected words that can be added to a document, image, post, or other online element to help categorize information by creating a personal taxonomy. McAfee prefers the term *folksonomy* to describe this process. Folksonomy emphasizes the involvement of users and the fluid, ongoing categorization of information.[94]

Often these bookmarks or tags are represented in a visual form that resembles a cloud. The words within the cloud are depicted in various sizes or colors of font to help the user gage the frequency of its use. The cloud allows for easy identification and selection of popular terms.[95] Tag clouds also allow users to draw inferences about relationships within sets of unstructured data.[96] Tagging and social bookmarking allow users to categorize information in the manner that it is valued by the user, as opposed to traditional categorization methods that are preset and cannot be easily altered. The tags are visible to all users allowing them to benefit from previous user's categorization

---

[92] Kaplan and Haenlein, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, 59–68, 63.

[93] Kate Starbird et al., "Chatter on the Red: What Hazards Threat Reveals About the Social Life of Microblogged Information" ACM}, 2010).

[94] McAfee, *Enterprise 2.0: The Dawn of Emergent Collaboration*, 25.

[95] *The Social Enterprise: Using Social Enterprise Applications to Enable the Next Wave of Knowledge Worker Productivity*, 8.

[96] Murugesan, *Understanding Web 2.0*, 37.

efforts. Tags and social bookmarking are also a way for employees to track internet sites that they find useful and share these sites with others.[97] With the addition of tags, information may be more easily searched and accessed.

B. HIERARCHY

Hierarchies, such as those existing in law enforcement agencies, are insufficient for the sharing and transfer of information. Hierarchical structures support and encourage the maintenance information silos through the use of predefined categories. Unstructured information that does fit into these categories disrupts established information channels and will flow to unregulated and possibly nonsecure networks.[98] One research study found that "30% of office workers in the USA and 42% of UK office workers admitted to discussing work-related issues via social media applications."[99] In a police environment dealing with sensitive information, a secure alternative is essential.

Drapeau and Wells note that Web 2.0 software offers the potential for users to create what they term as "heterarchies," which empower users to form decentralized groups that can provide an alternate to the traditional hierarchical communication silos. Benefits of creating a means to facilitate horizontal information sharing, while still supporting vertical systems, include "encourag(ing) open discussion, community building, and efficiencies of scale."[100] The move to horizontal, open exchange of information can generate fear from staff as the communication hierarchy breaks down. As stated by Emile Attunes, the Web Director for NASA's Goddard Space Center, "You're supposed to let anyone talk to anyone else, and that can be a little scary for

---

97 McAfee, *Enterprise 2.0: The Dawn of Emergent Collaboration*, 25.

98 Ines Mergel, "The Use of Social Media to Dissolve Knowledge Silos in Government," in *The Future of Public Administration, Public Management, and Public Service Around the World*, eds. R. O'Leary, Kim S. and D. VanSlyke, 2011), 178.

99 van Zyl, *The Impact of Social Networking 2.0 on Organizations*, 906.

100 Drapeau and Wells, *Social Software and National Security an Initial Net Assessment*, 7.

people who prefer to have a chain of communication go in a particular way."[101] Changing communication expectations will take changes in policy, ongoing support from upper staff, and time.

C. WEB 2.0 AND ESSP IMPACT ON INFORMATION SHARING AND COLLABORATION

Web 2.0 and its application through the use of ESSPs in Enterprise 2.0 environments has allowed the knowledge management of many organizations to move beyond a centralized, relatively static, storage mechanism for knowledge towards an interactive and conversational endeavor.[102] Web 2.0 technologies help to create knowledge networks, which facilitate conversational knowledge management by allowing information to be updated at any time by any user that has new information that may be relevant.[103] Rather than providing static information that starts becoming outdated the day after publication, information storage mechanisms in these networks allow the continuous updating of information.

Another of the key benefits of technology is that it increases the reach of and the speed in which information can be transferred.[104] By extending the reach beyond formal communication networks, and the employee's own immediate coworkers and social circles (within the work environment), the rate of information sharing can be increased.[105] Though the extended networks provided by social media may be weaker, the exposure to new ideas is crucial to transferring knowledge.[106] Increased sharing

---

101 "Social Networking Takes Flight at NASA," http://www.ciozone.com/index.php/Case-Studies/Social-Networking-Takes-Flight-at-NASA.html.

102 Lee and Lan, *From Web 2.0 to Conversational Knowledge Management: Towards Collaborative Intelligence*, 47–62, 49.

103 Ibid., 52.

104 Davenport and Prusak, *Working Knowledge: How Organizations Manage what they Know*, 125.

105 Alavi and Leidner, *Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues*, 107–136, 121.

106 Maxine Robertson, Jacky Swan and Sue Newell, "The Role of Networks in the Diffusion of Technological Innovation," *Journal of Management Studies* 33, no. 3 (1996), 333–359.; Alavi and Leidner, *Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues*, 107–136.

heightens the probability that new information may be encountered due to the expansion of the personal network beyond the regular circles. The tendency is for small nonnetworked groups to possess similar information.

Information technology also provides a method to facilitate the extraction of information from individual users, and then structure it in such a way that makes it accessible to others.[107] Social software platforms can resemble a living process subject to change and adaptation occurring as quickly as changes in the world around the user. In these open systems, the user is able to respond more quickly to the information because each of them has unfiltered access and the ability to make direct use of it.[108] Platforms for micro-blogging, (e.g., Twitter), and tools like tagging help connect users to knowledge and empower users to help facilitate easy access for other users who might have an interest in the information.[109]

The core philosophy of Web 2.0, and the ESSPs that employ them, is that it allows the creation of an environment of dynamic knowledge and collective intelligence.[110] By expanding the reach of the information through the expansion of personal networks, each user is increasingly empowered to make more direct use of information and share the information they develop directly with other users. This moves the information closer to the officers and detectives in a position to make the best use of it, while still allowing direct access to strategic decision makers.[111]

By providing users a platform where a steady flow of dynamically changing information can be vertically shared, users are able to decide what part of the information

---

107 Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know.*

108 Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Portfolio, 2006), 35.

109 Drapeau and Wells, *Social Software and National Security an Initial Net Assessment*, 23.

110 Lee and Lan, *From Web 2.0 to Conversational Knowledge Management: Towards Collaborative Intelligence*, 47–62, 57.

111 Brafman and Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, 53.

is important and relevant to them.[112] Such open systems also have the benefit of creating an environment where users want to contribute.[113]

D. NETWORK ASPECTS

A positive aspect of Web 2.0 and ESSPs is the ability to enforce the strength and increase the number of links among employees within the police department, and eventually outside the department. This follows the model of social networking already in common use in the general public. Networks exist in all systems including police organizations, but current software technology infrastructure supports data and standardized information collection more than human interaction. Within police agencies, Human interaction, a prime catalyst for the development of new information and knowledge, is primarily limited to face-to-face interaction, telephone conversations and email. None of these is well suited to the capture and sharing of information and knowledge outside of the original participants. From a network perspective, the problem is that the number of links and nodes in systems limited to these communication technologies will have fewer degrees of connectedness. Communication growth will be limited by not taking advantage of new technologies such as Web 2.0 tools including blogging, micro-blogging, wikis, and others. By adopting Web 2.0 tools, the potential connectedness between users in an agency can be increased allowing for improved information and knowledge sharing.

The phrasing "potential connectedness" is used because Web 2.0 technologies do not come preassembled with users and content. While Web 2.0 technologies offer the potential to increase connectedness due to the relative ease of communicating with large numbers of people, but without content there is little reason for people to use these technologies. Of course, content is dependent on the input of users. This issue is referred to as a network effect. When this effect is present, the value of a system increases as more people use it. The value of an ESSP grows exponentially as the amount of data

---

[112] Drapeau and Wells, *Social Software and National Security an Initial Net Assessment*, 7.

[113] Brafman and Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, 75.

increases along with the number of persons using the system.[114] The growth process can be kick-started by establishing some initial structure within the ESSP. By establishing the initial starting point for employees, employees will have a base for further growth and development of the system.[115]

In addition, the relatively static existing digital infrastructure is not able to quickly adapt to the communication needs of users. The infrastructure is also limited in the data that be captured due to the software input mechanism that data to be entered via predesignated sets of information. In other words, a user may want to send a tweet to fellow users, but instead has to complete a form that includes required extraneous data in order for the short message to be entered into the system. Software changes needed to adapt to user needs are often costly. Failure to have systems that address the networking needs of offices can result in users taking the path of least resistance, which may be to not take any action at all.

E. BIG DATA

To a certain degree, ESSPs are structures created to help personnel address information overload. Though it varies by agency and role, police officers have access to huge data bases of information including records management systems, utility data, correctional data, driver's license information, vehicle records, and others. In an age where the amount of data is growing exponentially, organizations are often overwhelmed with astronomical amounts of data, often unstructured, that exceed the ability of their current analytical systems.[116] "Big data" is a term used to describe data when it exceeds the ability of organizations to effectively use it. Put another way, "big data" refers to "datasets whose size is beyond the ability of typical software tools to capture, store,

---

[114] Dion Hinchcliffe, "Why All the Fuss about Web 2.0," , no. Jan/Feb (2010).

[115] McAfee, *Enterprise 2.0: The Dawn of Emergent Collaboration*, 27.

[116] Thomas H. Davenport, Paul Barth, and Randy Bean, "How 'Big Data' is Different" *MIT Sloan Management Review* (Mon, 30 July 2012).

manage, and analyze it."[117] Big data is a subjective term, but when a user crashes their computer trying to analyze crime data, it can be said that they are dealing with big data.

With the increase of data storage capacity and the number of data sources, along with improvements in software technology, big data has become a multi-billion dollar business in just less than a decade. [118] The growth of data is increasing by as much as 50 percent a year. The ability of software to glean information from unstructured data, such as images, video, text messages, sensor data, financial sources, government documents, and innumerous other sources is also increasing. Artificial intelligence, such as natural-language processing, pattern recognition, and machine learning are rapidly improving, and thereby further increasing the value of big data.[119] Despite wide access to big data, government agencies have yet to take advantage of the potential of this data to improve performance. [120]

ESSPs are a method to put information into context to increase its value to users, but in the context of big data, ESSPs will also provide a new source for data. This new source may one day help administrators better understand the effectiveness of current processes and practices. As an emergent system, the data created by the use of ESSPs may provide insight that can improve police efficiency and effectiveness.

Data mining allows organizations to extract patterns from big data through various statistical methods and machine learning with database management.[121] Predictive policing is one application of predictive modeling that uses statistical models to make predictions on potential outcomes.[122] Predictive policing is being used by forward thinking police departments by analyzing data from business intelligence

---

[117] Edd Dumbill, *Big Data Now Current Perspectives from O'Reilly Radar*. ([S.l.]: O'Reilly Media, 2011), 115.; Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*.

[118] Quentin Hardy, "How Big Data Gets Real," NYTimes.com, http://bits.blogs.nytimes.com/2012/06/04/how-big-data-gets-real/.

[119] Steve Lohr, "The Age of Big Data," *New York Times*, November 11, 2012.

[120] Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, 37.

[121] Ibid., 28.

[122] Ibid.

systems to predict future trends. Business intelligence data is used for CompStat purposes to understand past criminal activity and performance data with a limited focus on forecasting future activity. The use of big data and improved analytical software allows for the focus on where crime will be tomorrow rather than where it was yesterday. Though the locations are the often the same, systems that use big data are able to make more accurate predictions that take into account a multitude of different factors. As the value of big data, data mining and predictive policing is recognized and adopted by more police agencies, these agencies will be able to increase productivity and efficiency in the same manner that commercial organizations are using it to increase sales and reduce costs. [123]

Data analysis for many departments is limited to structured information that is small enough to be analyzed using an Excel spreadsheet. Little information of value can be derived from this limited data and processing capability.[124] In determining the success of policing efforts, the traditional focus on been on easily measured data such as arrests, citations, and call response times. An officer effective at reducing the incidents of crime in their beat may have less impressive arrest numbers than other less effective officers. Inputs and outputs, such as the impact of efforts on actually reducing crime or collisions, have received little attention, though this is changing. Supervisors can improve their evaluations of officer performance through the increased use of data. Rather than simply examining arrest and citation data, supervisors using data such as crime rates, area averages, past performance, and other factors will be able to give more accurate and constructive evaluations. Improved evaluations methods will also improve the ability of agencies to reward effective performance, evaluate policies and strategies. By using data in this way, law enforcement agencies can better reward performance and evaluate policies.[125]

---

[123] Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, 12.

[124] Kevin Fogarty, "Big Data Plus Police Work: Good Partners?" Information Week, http://www.informationweek.com/software/business-intelligence/big-data-plus-police-work-good-partners/240004290.

[125] Alex Olesker, "Big Data Solutions for Law Enforcement," CTO Labs, http://ctolabs.com/wp-content/uploads/2012/06/120627HadoopForLawEnforcement.pdf

Good leaders recognize that the quality of management decisions is limited by the data on which they are based. By increasing the quality and amount of data, management will be better position to accurately measure performance. [126] The analysis of big data allows administrators to use less tangible inputs and outputs to improve productivity, innovation, and growth. [127]

In the article, "How 'Big Data' Is Different,"," Thomas Davenport noted that "a key tenant of big data is that the world and the data that describe it are constantly changing, and organizations that can recognize the changes and react quickly and intelligently will have the upper hand."[128] In policing, the upper hand is not on the commercial competitor, but on the criminal element. The analysis of big data can help officers find violent crime hot spots in the community and predict crimes more accurately than ever before. [129] Using data sources that did not exist ten years ago may provide additional opportunities for policing. Real time traffic data, GPS data, and personal location data can improve emergency services response times. Dispatchers can quickly identify the location of callers, identify the nearest officer, and provide the shortest response path. [130] Data can also be used to improve service that can save lives, reduce crime, and improve community relations.[131] To improve performance and efficiency, departments will increasingly need to integrate information from multiple data sources. These sources could include corrections data regarding the release of convicted felons, probation and parole data, license plate reader data, traffic engineering data, etc.[132]

---

126 Thomas C. Redman, Data Driven: Profiting from Your most Important Business Asset (Boston, Mass.: Harvard Business Press, 2008), 98.

127 Erik Brynjolfsson and Adam Saunders, *Wired for Innovation: How Information Technology is Reshaping the Economy* (Cambridge, Mass.: MIT Press, 2010), 4.

128 Davenport, Barth, and Bean, *How 'Big Data' is Different.*

129 Fogarty, *Big Data Plus Police Work: Good Partners?*

130 Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, 91.

131 Olesker, *Big Data Solutions for Law Enforcement*, 4.

132 Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, 12.

One challenge for innovators in policing is the nature of government as contrasted with commercial organizations. Governmental organizations do not have the competitive drive that commercial organizations must have to survive and thrive. As the private sector takes advantage of current technology and innovations, public sector productivity falls further behind. The concept of big data is alien to many government organizations that have yet to take full advantage of data that is already readily accessible to them.[133]

In addition, government organizations often have legacy systems that are incompatible with current standards, which make the integration of data and the use of advanced analytical methods more difficult, if not impossible, with current systems. In many cases, the information is not in a digital format adding yet another barrier.[134] Another issue is the lack of personnel that have the skills needed for advanced analytics. Even with the analyzed data, government reward systems do not necessarily encourage the use of this data to improve decision making.[135]

Privacy advocates have been vocal in their concerns over the concept of big data. Examples abound in objections to the use of big data by commercial organizations. Google has received criticism for using data from user emails to target advertising. Facebook has faced objections from entire governments that decry the use of facial recognition technology.[136] These same concerns are faced by governmental organizations that seek to use big data to improve public services.[137] When using big data, police agencies must carefully balance privacy rights with the need to protect and serve the public. As big data sources and analytical capabilities increase, the ethical decisions regarding the extent to which data should be used will move to the forefront of policing.

---

133 Jacques Bughin, Michael Chui, and James Manyika, "Clouds, Big Data, and Smart Assets: Ten Tech-Enabled Business Trends to Watch," *McKinsey Quarterly* 56 (2010), 8.

134 Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, 107.

135 Ibid., 108.

136 Fogarty, *Big Data Plus Police Work: Good Partners?*

137 Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, 108.

As with commercial organizations, it will be incumbent on police leadership to help citizens understand the benefits and potential risks associated with the use, or lack of use, of big data.[138]

The New York Police Department is already using big data from license-plate readers to track the location of vehicles. Their system integrates 911 calls, crime reports, radiation detectors, outside intelligence sources and other sources to improve efficiency and productivity.[139] A study of Santa Cruz predictive policing efforts using big data found that it predicted 20 to 95 percent more crimes than traditional CompStat practices. The Richmond (VA) Police Department has also used data on store, bar, housing, and ATM locations to help identify factors driving crime.[140]

The collection and analysis of data from calls for service, police reports, video and audio of video, and audio by police agencies may also be used to make police departments more proactive and accountable to the public. The large amounts of data gathered will not only be used to target crime but will also enable organizations to reduce administrative and operational waste and deficiencies while improving customer service.[141]

In policing, as with business, analysis based on big data will increasingly be used to improve decision making. Experience and intuition will be supplanted by analytical methods that are scientifically testable and verifiable. One study of business found that "data-driven decision making" achieved productivity gains that were five to six percent higher than other factors could explain."[142] It is not unreasonable to expect the same results in policing. Today's police leaders must improve their own understanding of the

---

138 Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, 12.

139 "NYPD and Microsoft Create a Next Generation Law Enforcement Big Data Solution," http://ctovision.com/2012/08/nypd-and-microsoft-create-a-next-generation-law-enforcement-big-data-solution/.

140 Olesker, *Big Data Solutions for Law Enforcement*, 4.

141 Ibid., 2.

142 Lohr, *The Age of Big Data*.

potential value of big data and analytics in policing. Culture and processes will need to be changed to increase the use of big data to improve decision making and the resulting action.[143]

[143] Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, 12.

V. INTELLIGENCE

This chapter is focused on the definition and nature of intelligence, and how the laws and regulations that regulate information and intelligence sharing impact collaboration. Whenever considering information sharing technologies and processes in policing, legal and privacy concerns are critically important policy issues. Moving the concept of social media beyond its initial use as public relations and communications tool requires careful consideration of these issues.

Law enforcement intelligence operations enable more effective proactive policing by allowing officers to intervene more effectively in on-going criminal operations and to locate and stop criminal activity.[144] Whether or not an ESSP used for sharing of information on crime and criminal offenders should be classified as an intelligence system is a question likely to quickly arise. Answering this question incorrectly could severely impact and limit efforts at information sharing due to the legal and privacy issues that are specific to intelligence systems. Unfortunately, many agencies do not understand what intelligence is or how to properly manage it.[145] Without a clear understanding of intelligence and the multitude of related issues, agencies will soon find themselves unable to effectively operate within the modern information environment. They will also be ill-prepared to address many issues that reduce their ability to collect, store, and share information and intelligence. The inclusion of individual officers who work in the community is critical to the intelligence function of any agency. Without the full participation of the officers on the beat, as well as those in specialty units, intelligence operations will be limited in their ability to return beneficial intelligence to these officers.[146]

---

144 *Criminal Intelligence: Concepts and Issues Paper*, 2003rd ed. (Alexandria, VA: IACP National Law Enforcement Policy Center, 1998), 6.

145 Marilyn B. Peterson, *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, DC: Bureau of Justice Assistance, 2005), 3.

146 *Criminal Intelligence: Concepts and Issues Paper*, 11.

A. INTELLIGENCE DEFINED

An interesting aspect of intelligence is that it may include data, information, and/or knowledge. Most agencies have policies and procedures for the handling of each of these. But intelligence handling has its own set of rules and regulations based on federal law. An item of data or information has different handling requirements than an item of intelligence. The misclassification of certain types of information as intelligence will result in limiting the number of people being granted access to it and has the potential to significantly shape how information is shared and collaborated on with new technologies. Conversely, mishandling intelligence can result in infringement on individual rights, violations of federal law, and criminal cases being compromised. While there may be a tendency to over-classify information and limit sharing to err on the side of caution, ineffective use of available information can carry with it a cost. One only needs to remember the ineffective handling of information prior to the events of 9/11 to understand the potential harm. While not effectively handling information and intelligence may not result in anything so dramatic, one can safely say that it will result in a loss of potential efficiency and associated costs, and increased victimization. While these factors may be difficult to quantify, the costs are very real.

All intelligence is not equal. National security intelligence should not be confused with criminal intelligence. Neither should be confused with information, but the terms "intelligence" and "information" often are confused with one another and used interchangeably. The term "information" is often used broadly and encompasses intelligence. Just as there is a need to distinguish between the terms of data, information and knowledge, it is also important to distinguish between information and intelligence. Intelligence products have different guidelines, rules and regulations that govern their use and that do not necessarily apply to information. According to Carter, "…intelligence is erroneously viewed as pieces of information about people, places or events that can be

used to provide insight about criminality or crime threats." To the contrary, information does not become intelligence until it is analyzed.[147] The line between the two can be indistinct and the subject of disagreement.

The International Association of Chiefs of Police (IACP) noted that although intelligence in its most basic form is information, not all information is intelligence. Basic information including data, regardless of its source, is not intelligence until it undergoes an analytical process that determines its value for tactical and strategic purposes. Simply going through this process does not mean that the information will become intelligence. The term intelligence is used generically within law enforcement agencies.[148] This creates confusion and limits the understanding of and appropriate application of both information and intelligence.

As opposed to the traditional definition of information, facts about something or someone, information within the context of intelligence can be defined as "pieces of raw, unanalyzed data that identifies persons, organizations, evidence, events, or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event."[149] Some examples of information include: criminal histories, offense reporting records, and vehicle registrations. Examples that may be mistakenly considered intelligence could include observations made by officers, surveillance teams, or citizens.[150]

The Association of Law Enforcement Intelligence Units (LEIU) produced a set of guidelines for the handling of criminal intelligence. The guidelines state: "The bulk of the data an intelligence unit receives consists of unverified allegations or information. Evaluating the information's source and content indicates to future users the information's

---

147 David L. Carter and United States, Dept. of Justice. Office of Community Oriented Policing Services, "Law Enforcement Intelligence a Guide for State, Local, and Tribal Law Enforcement Agencies," U.S. Dept. of Justice, Office of Community Oriented Policing Services, 11, ; *Criminal Intelligence: Concepts and Issues Paper*, 13.

148 Ibid., 3.

149 Carter and United States, Dept. of Justice. Office of Community Oriented Policing Services, *Law Enforcement Intelligence a Guide for State, Local, and Tribal Law Enforcement Agencies*, 11.

150 Ibid., 12.

worth and usefulness. Circulating information that may not have been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to the agency's operations and contrary to the individual's right to privacy."[151]

Neither this statement nor any other part of the guidelines created by LEIU clearly distinguishes information from intelligence. It may be that LEIU guidelines are attempting to simply emphasis the care that should be taken with any information or intelligence that is distributed. Regardless, statements such as the one above promote concerns that a thorough analysis must be performed before any information can be shared. This would tend to limit the sharing of information and may be too stringent of a guideline for some types of rough data and information that may need to be released. There remains a tendency to restrict the sharing of information rather than encouraging the sharing of it with others who can offer a new perspective.[152] Even unevaluated information, where the source reliability is unknown, can be of potential use when combined with other information. Due to the close relationship between information and intelligence, analyst, police officers, and police staff must recognize that though the terms are sometimes used interchangeably, they are not synonyms and must be evaluated individually.

B. DECONSTRUCTING INTELLIGENCE

Understanding the difference between information and intelligence is only part of the equation. Intelligence intrinsically has multiple meanings and areas of application. It can be broken down into two broad classes. The first class is referred to as the "discipline of intelligence." Within this class there are actually three types of intelligence including law enforcement or criminal intelligence, homeland enforcement intelligence, and national enforcement intelligence.[153]

---

[151] *Criminal Intelligence File Guidelines* (Washington, DC: U.S. Dept. of Justice, Office of Justice Programs, 2002), 6.

[152] Jerry H. Ratcliffe and Police Foundation, "Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders," *No.: ISBN 1-884614-21-3* (2007), 7.

[153] Carter and United States, Dept. of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence a Guide for State, Local and Tribal Law Enforcement Agencies*, 11.

The second class is referred to as the "application of intelligence." This type of intelligence addresses knowledge related to a specific crime type. This might include situational awareness of gang activity across the region or the latest information on drug trafficking practices in northern Mexico.[154] This class is often referred to as intelligence products.

1. Criminal Intelligence

One definition of criminal enforcement intelligence is "the product of an analytic process that provides an integrated perspective to disparate information about crime trends, crime and security threats, and conditions associated with criminality."[155] The IACP defines criminal intelligence as "a combination of credible information with quality analysis- information that has been evaluated and used to draw conclusions."[156] In their model policy, the IACP provides an alternate definition: "information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity."[157] In both definitions provided by the IACP, information is treated as an element of intelligence and presumably should be handled under the same set of standards applicable to intelligence. Though the IACP acknowledges the difference between information and intelligence, the definitions don't provide for a clear distinction, which again allows for confusion. This is of particular concern because it may be a contributing factor in the reluctance of law enforcement to share information. When information misclassified as intelligence is shared, higher security standards that apply to intelligence must accordingly have a limiting effect on the willingness of stakeholders to share it.

Criminal intelligence can be broken down into three subsets: tactical, operational, and strategic. Tactical is considered the most common form of intelligence in law

---

[154] Carter and United States, Dept. of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence a Guide for State, Local and Tribal Law Enforcement Agencies*, 10–11.

[155] Ibid., 12.

[156] United States, Office of Justice Programs, *The National Criminal Intelligence Sharing Plan: Solutions and Approaches for a Cohesive Plan to Improve our Nation's Ability to Share Criminal Intelligence.* ([Washington, D.C.]: Office of Justice Programs, U.S. Dept. of Justice, 2003), 3.

[157] *Criminal Intelligence: Concepts and Issues Paper*, 3.

enforcement today.[158] This type of intelligence can be directly applied to individual cases, suspects, and criminal acts. An example of this may be an analysis of a string of armed robberies that identifies a likely suspect based on the method of operations, the likely next target, and a time the suspect is likely to strike next. This type of intelligence appeals to the field officer because it allows for the quick development of a plan of attack to address the object of the intelligence.[159] Despite the view of how abundant this form of intelligence is, it is still highly underused. Quality tactical intelligence involving the identification of patterns and other connections is difficult to produce due to the large geographical area that is often involved, the mobility of offenders, and the large number of potential suspects.

Most of the "tactical intelligence" presented would better be classified as what could be termed "tactical information." If you were to ask a police officer what tactical intelligence was, they would likely base it their definition on what is needed to conduct a search warrant: house plans, neighborhood layout, communications, suspect information, and threats involved. Other types of tactical information would include the locations of crimes, suspects believed to be actively committing criminal acts, and active arrests warrant. Analysis may or may not be an element of tactical information. A variety of information sources that could be used to help develop tactical or other levels of intelligence are not integrated with current information systems. Though there needs to be a focus on broader levels of intelligence, there also remains a room for a great deal of improvement in the area of tactical intelligence.

Operational intelligence as a distinct level of intelligence is fairly new to the intelligence lexicon. This level of intelligence falls between the tactical and strategic levels and encompasses certain elements of both. The purpose of operational intelligence is to provide support to area commanders in aiding the planning of crime reduction

---

158 *Criminal Intelligence: Concepts and Issues Paper*, 3.

159 Jerry H. Ratcliffe, "The Structure of Strategic Thinking," *Strategic Thinking in Criminal Intelligence* (2004), 1–10.

activity and resource allocation.[160] Operational intelligence is a step above tactical intelligence and may encompass tactical intelligence as a tool in its implementation.

The third level of criminal intelligence is strategic intelligence. This level is focused on patterns of criminal behavior; the functioning of the criminal environment and related trends.[161] It is intended to be more proactive and used for planning of future operations. Strategic intelligence may be used to guide the creation of long-term goals and objectives for the department as well as staffing.[162] Good strategic criminal intelligence guides not only law enforcement, but also other entities that have an impact on crime in the community, such as homeless organizations, city planners, and community leaders.

In the book *Crime Analysis,* the authors distinguish between "intelligence analysis" and "crime analysis." The authors state that the purpose of intelligence analysis is to a focus on organized crime to include auto theft rings, fraudulent credit card operations, land swindles, and other criminal organizations. This definition would appear to cover terrorism groups as well. The purpose of crime analysis is to link elements such as suspect description and modus operandi with a series of offenses.[163] Other works don't make the distinction between organized crime intelligence and other criminal intelligence. This creates an odd loop. Gottlieb, et al, later notes that intelligence is the product of analysis. Analysis is the process to develop intelligence. With this in mind, the term "intelligence analysis" would be the analysis of the products of analysis. A better way of approaching this would be to classify the analysis of organized crime and other types of crime both under the umbrella of criminal intelligence. It is recognized that a

---

160 Jerry H. Ratcliffe, "The Structure of Strategic Thinking," *Strategic Thinking in Criminal Intelligence* (2004), 1–10.

161 Ratcliffe and Police Foundation, *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*, 50; *Criminal Intelligence: Concepts and Issues Paper*, 3.

162 *Intelligence-Led Policing: The New Intelligence Architecture*, (Washington, DC: Bureau of Justice Assistance, 2005), 10.

163 Steven Gottlieb, Sheldon Arenberg, and Raj Singh, "Crime Analysis: from First Report to Final Arrest," *No.: ISBN 0-9634773-0-7* (1994), 616, 27.

unit or analyst may be made responsible for focusing on either area. This issue is more important than it might seem at first glance. The Gottlieb book serves as the basis for many police crime analysis programs and is taught throughout the nation.

2. National Security Intelligence

National security intelligence (NSI) is probably more in line with the public's perception of intelligence activities. NSI is focused on foreign threats to the United States. Carter defines it as "the collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors, as well as the maintenance of the United States' sovereign principles."[164] Most state and local police departments have limited involvement with NSI, which is primarily a federal function. The most likely connection would be through the Joint Terrorism Task Force. Officers involved with this level of intelligence typically will have Top Secret or Secret security clearances.[165] Since NSI agencies are not limited by constitutional restrictions that apply to criminal cases, the information developed may not be usable by agencies involved in criminal investigations. Liability can become an issue if information that was gathered in a manner inconsistent with constitutional standards is used as part of a criminal investigation. Even the collection or storage of information or intelligence inconsistent with these standards can result in liability under 42 USC 1983, Civil Action or Deprivation of Civil Rights.[166] This issue becomes more clouded as federal laws are passed to encourage the sharing of information between all levels of government. The full impact these laws will have on the intelligence community and criminal investigations may not be determined for years to come.

---

[164] Carter and United States Dept. of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence a Guide for State, Local, and Tribal Law Enforcement Agencies*, 15.

[165] Ibid., 17.

[166] Ibid.

3. Homeland Enforcement Intelligence

It is often said that 95 percent of law enforcement duties involve providing various community services, and five percent is actual enforcement of the law. Community services range from working traffic collisions to responding to natural disasters, such as tornadoes, ice storms, and floods. Homeland Enforcement intelligence, also known as "All Hazards Intelligence"," addresses hazards that are noncriminal but have the potential of disrupting public order. Carter defines All Hazards Intelligence as "the collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of the threat."[167]

Homeland enforcement intelligence is not clearly delineated in law or policy but is being increasing used in terms as the Department of Homeland Security seeks to improve on efforts to protect critical infrastructure.[168] The Homeland Security Act of 2002 stops short of defining homeland security intelligence, but it does define homeland security information as "information possessed by government agency related to the threat of terrorist activity, prevention…or would improve the response to a terrorist act."[169] This definition takes a different and much more limited focus than the one provided by Carter. A congressional research document provides yet another interpretation of homeland security intelligence. This definition includes intelligence designed to protect against the activities of drug traffickers, organized crime, and others having international support networks.[170] Regardless of the definition and interpretations in the literature, this terminology is not common in the law enforcement environment and is likely to change as it becomes more widely used.

---

[167] Carter and United States Dept. of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence a Guide for State, Local, and Tribal Law Enforcement Agencies*, 14.

[168] Ibid., 17.

[169] Department of Homeland Security and United States Congress, *Homeland Security Act of 2002.* (Washington, D.C. The Department, 2002).

[170] Mark A. Randol and Library of Congress, Congressional Research Service, "Homeland Security Intelligence Perceptions, Statutory Definitions and Approaches," Congressional Research Service, 10.

C. LEGAL AND PRIVACY ISSUES

The highest of responsibilities for law enforcement and other government officials is to protect the privacy and civil rights of citizens, while still providing protection from domestic and international threats to the community. An ESSP that is not properly implemented and managed runs the risk of intruding on the privacy and civil rights of citizens and can place officers and the department in a precarious situation, to say the least. It may be better to not have a system for sharing information, than to have one that allows for uncontested abuse, or that stands a high risk of compromise by hackers who could then manipulate or use information for their agenda.

Laws and regulations that apply to intelligence operations include the Privacy Act of 1974, Criminal Intelligence Systems Operating Policies- Title 28 of the U.S. Code of Federal Regulations, part 23 (28 CFR Part 23), and the E-Government Act of 2002, as well as the policies and procedures of state, local, and tribal agencies.[171] Developing a thorough understanding of the legality of intelligence operations is complicated by the fact that laws, statutes, and practices that govern information sharing vary considerably between all levels of government.[172] Each of these issues must be carefully reviewed and interpreted to ensure appropriate, legal, and ethical intelligence operations.

Simply identifying the laws and regulations that apply to information and intelligence sharing can be challenging. Trying to apply them to new media and ESSPs that did not exist when the laws were written further complicate efforts. Most of the resources provided by federal agencies are vague in describing the applicable laws. The NSIS states in their recommendations for privacy guidelines that agencies must "assess, document, and comply with all applicable laws and policies."[173] The Information Sharing Environment Implementation Plan states that the sharing of terrorism information must

---

171 "Information Sharing Environment-(ISE)-Suspicious Activity Reporting (SAR)--Evaluation Environment (EE) Segment Architecture," Office of the Program Manager for the Information Sharing Environment, 4.

172 Ibid., 19.

173 United States, White House Office, "National Strategy for Information Sharing Successes and Challenges in Improving Terrorism-Related Information Sharing." White House, 27.

be "in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[174] These recommendations, while well intentioned, provide only the broadest of guidance to law enforcement.

The regulation that predominates in the literature is 28 CFR Part 23. Peterson emphasizes the regulations role as a national standard that ensures the protection of privacy and civil rights.[175] The National Criminal Information Sharing Plan (NCISP) also recommends that all law enforcement agencies follow the guidelines set forth in 28 CFR Part 23.[176] Currently, only agencies that received funding from the Omnibus Crime Control Act of 1968 are required to conform to this regulation.[177] The recommendation from the NCISP states that 28 CFR Part 23 is a minimum standard that agencies need to follow in order to ensure the privacy and constitutional rights of individuals, groups, and organizations. As a result, many agencies use this regulation as a guideline regardless of any federal funding being received.[178] Before any ESSP can be implemented, it must be considered in the context of this regulation if agencies seek to abide by it.

1. Criminal Intelligence Systems Operating Policies (28 CFR Part 23)

CFR 28 part 23 provides guidance in five primary areas: submission and entry of criminal intelligence information, security, inquiry, dissemination, and the review-and-purge process.[179] The purpose of this regulation is "to assure that all criminal intelligence systems…are utilized in conformance with the privacy and constitutional rights of

---

174 Thomas E. McNamara, "Information Sharing Environment Implementation Plan," *US Information Sharing Environment* 1 (2006), 2010, 133.

175 Peterson, *Intelligence-Led Policing: The New Intelligence Architecture*, 20.

176 United States, Office of Justice Programs, *The National Criminal Intelligence Sharing Plan: Solutions and Approaches for a Cohesive Plan to Improve our Nation's Ability to Share Criminal Intelligence*, 14.

177 Peterson, *Intelligence-Led Policing: The New Intelligence Architecture*, 25.

178 United States, Office of Justice Programs, *The National Criminal Intelligence Sharing Plan: Solutions and Approaches for a Cohesive Plan to Improve our Nation's Ability to Share Criminal Intelligence*, 14.

179 Ibid.

individuals."[180] This is appealing to police agencies, since it creates a path guiding them through the complex issues surround privacy and constitutional rights and in doing so helps to provide liability protection.

Due to some similarities with how ESSPs may be used, it is important to understand exactly what the regulation is referring to when it states "criminal intelligence system." Based on the definitions presented earlier in this paper, it would apply to any system that is used for the collection, storing, and dissemination of intelligence products produced through the analysis of information. This regulation differs in that it defines it criminal intelligence system as "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, or analysis of *criminal intelligence information.*"[181] (Emphasis added) This definition adds more complexity to the meaning. The key words that have to be examined are "criminal intelligence information." If the regulation simply referred to criminal intelligence, the application of the regulation would be somewhat simplified. By bringing in the word "information"," room for confusion arises. However, the regulation further defines the term of criminal information system by stating that it includes "information systems that receive, store and disseminate information on individuals or organizations based on reasonable suspicion of their involvement in criminal activity are criminal intelligence systems under the regulation."

Distinct from the academic definitions of intelligence, the regulation's use of the term of "criminal intelligence information" refers to data that is relevant to the identification of criminal activity that can tied to an individual who or organization which is reasonably suspected of involvement in criminal activity, ***and*** that meets criminal intelligence system guidelines." (Emphasis added) This could be interpreted to include all records management systems that include criminal identification data. An ESSP that allows for the sharing of criminal activity tied to individuals could also be considered a criminal intelligence system.

---

[180] "Criminal Intelligence Systems Operating Policies," Code of Federal Regulations Title 28, Pt. 23, rev. 1993.

[181] "Criminal Intelligence Systems Operating Policies," Code of Federal Regulations Title 28, Pt. 23.3B, rev. 1993.

The regulation created enough confusion on its proper application that the issue had to be addressed in a 1993 revision to the regulation. The revision, with included commentary, clarified that the regulation does not apply to criminal history records management systems. It is also clarified that the regulation only applies to systems that are shared with agencies outside the department. The regulation is not intended to apply to information sharing within a single agency, or within a multi-jurisdictional task force that operates under a single entity. Though 28 CFR Part 23 is recognized as a model standard for the handling of intelligence information, it is not required for all intelligence systems. The regulation is specifically directed at (1) inter-agency exchange of criminal intelligence information, and (2) agencies with criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968.[182] The Institute for Intergovernmental Research (IIR) asserts that the regulation was not intended to apply to case management databases, tips and leads files, and other nonintelligence databases. IIR distinguishes between criminal intelligence databases, and databases designed to assist in managing activities and providing factual information on subjects. These databases often include uncorroborated information.[183] An ESSP would likely fall in the latter category meaning that 28 CFR Part 23 would not apply.

Broad definitions of criminal intelligence and related systems pose a significant challenge to any information sharing efforts between agencies. The regulation was written to curb the abuses of law enforcement agencies in the 1950s and 1960s. The last revision to 28 CFR Part 23 in 1993 was written prior to the wide usage of intranets or cloud computing. Today, it results in agencies being overly cautious in their interpretation of the regulation, and as a result, over-cautious in the handling of potentially useful criminal information and intelligence.[184] This is contrary to the direction of government policies since the events of 9/11 that encourage inter-agency information sharing.

---

[182] "Privacy Act of 1974," United States Code Title 5, Section. 442A,1974.; D. L. Carter, "The Law Enforcement Intelligence Function," *FBI Law Enforcement Bulletin* 74, no. 6 (2005), 4.

[183] Institute for Intergovernmental Research, "28CFR FAQ " https://www.iir.com/Home/28CFR_Program/28CFR_FAQ/.

[184] Jerry Ratcliffe, "What Is Intelligence-Led Policing?," http://jratcliffe.net/research/ilp.htm.

Though information sharing and collaboration systems may be successfully utilized within a single agency, systems that overlap agency boundaries will likely be controlled and limited by the regulation. Even though adherence to the regulation may not be required, many agencies will follow it as a means to limit civil liabilities resulting from the potential misuse of information and intelligence stored in these systems.

2. The Privacy Act of 1974 (5 U.S.C. § 442a)

The Privacy Act of 1974 does not govern state and local government agencies, but should also be considered when reviewing intelligence standards due to its use as a model for state government. The primary purpose of this act is to protect an individual's privacy rights. The act sets forth regulations for the storage and release of personal information. Records containing the personal information cannot be released without permission of the person who the information is about. Seven exceptions are delineated including one that allows the limited release of information by law enforcement to other government entities. [5 U.S.C. § 442a (b) (7)] In addition, law enforcement is not required to provide "investigatory material" to individuals whom the records pertain to, except in limited circumstances. [5 U.S.C. § 442a (k) (6)] Numerous guidelines that apply to law enforcement agencies are outlined in the act. The act makes it illegal to retain records regarding how any citizen exercises his or her first amendment rights unless pertinent to and within the scope of any authorized law enforcement activity [5 U.S.C. § 442a (e)(7)]

One intelligence concern identified in the act is that law enforcement agencies are not permitted to release records to nongovernmental entities. This precludes the sharing of some information within the public realm. Arrest information is considered public information and can be released, but more detailed reports regarding crimes cannot be released. Most requirements of the act are procedural and would have a limited impact on ESSPs.

3. Agency Guidelines

While both of these guidelines, along with other applicable federal law, may be well understood within an intelligence unit, a lack of formal information and intelligence policies or operating guidelines may impede the full integration of the intelligence

function into the department's culture. While intelligence gathering may have once been the purview of a limited number of officers and analysts in the intelligence section of the department, concepts such as CompStat and intelligence-led policing are pushing intelligence throughout the department. Every patrol officer, detective, and supervisor is encouraged to gather information that may be of intelligence value and to apply information from intelligence products as part of their daily activities.

Department practice when it comes to the sharing of intelligence is an important consideration. Though it may be easy to assume that limitations on information sharing is due to a law enforcement culture that is overly protective of its intelligence products, it is equally likely a result of a conservative, mildly at that, interpretation of relevant laws and regulations. While many federal information sharing and intelligence publications stress the need for sharing information with private sector entities, laws and regulations actually make such sharing appear to be illegal. This takes us back to the difference between information and intelligence. Clearly, it cannot be illegal to share all types of information, but it is the tendency of these laws and regulations to restrict information and intelligence sharing as opposed to encouraging it. 28 CFR Part 23(f)(1) specifically prohibits the sharing of information except to law enforcement authorities who agree to follow procedures regarding information receipt, security, and dissemination that are consistent with the regulation's principles. The only exception given is when sharing of the information is necessary to avoid imminent danger to life or property.

Though efforts have been made to improve information sharing, while still protecting citizen rights, the base standard of 28 CFR Part 23 has not been changed to reflect this effort and is still restricting such action. Another challenge is that the definitions of intelligence may be overly broad. By referring to all bulletins, data, and observations as intelligence, the term is devalued. Even after the intelligence sharing failures of 9/11, intelligence personnel are still concerned about violating law by the improper sharing of information. A common viewpoint is that it is better to err on the side of caution than to be federally prosecuted.

4. Planning for the Inevitable

The main point of an ESSP is to reduce information compartmentalization, so that information will be more readily available to those who can make the best use of it. As data, information, and knowledge is shared and used to improve collaborative efforts, the likelihood of it being compromised increases. An effective implementation strategy can help reduce these risks. The setting of overall goals and objectives for the authorized use of ESSPs established the groundwork for security. ESSPs are simply an extension of the employees using it. By clearly communicating organization values and expectations, abuse of these systems can be largely avoided. In a police environment, personnel often share sensitive information. Management must set guidelines on the types of information that may be shared over the ESSP to ensure proper security standards are followed and that citizen's privacy rights are respected consistent with law and organization regulations. Federal departments have produced numerous documents that can help guide agencies in the development of standard based on best practices. Setting these guidelines not only protects the agency from legal liabilities, but it also helps employees understand the implications of improper use of these systems, and how to best utilize them in a manner consistent with organization standards. Training for employees is also needed to ensure their understanding of potential threats to the system, and to provide processes that can be followed to reduce opening the system up to vulnerabilities.[185]

Following information sharing system environment guidelines will also reduce the consequences of malicious attacks and hacking by outside entities. Information technology departments must insure that appropriate security controls are used for all ESSP servers to reduce the threat of attacks. These security controls include firewalls, virus protection, and access controls in addition to physical security surrounding servers.

[185] Sara Estes Cohen and Shala Ann Byers, "Look before You Leap: Security Considerations in a Web 2.0 World," *IA Newsletter* 13, no. 2 (2010), 20.

Inevitably, despite the best of efforts incidents will occur where information is compromised, or where users inappropriately use the system. Management must anticipate and plan for these occurrences to ensure a quick response and mitigation of any damage done.

D. EMERGENT INTELLIGENCE

The core philosophy of Web 2.0, and the ESSPs that employ them, is that it allows the creation of an environment of dynamic knowledge and collective intelligence.[186] ESSPs can be envisioned as a virtual water cooler, around which employees can transfer information, while at the same time providing a platform for discovering what information they do not know, and even for creating new knowledge.[187] This is especially important in policing where there has not been a "water cooler." Officers do not work eight to five jobs where they have opportunities to share information. While there is some limited contact among officers during a shift, this limited contact does not often include opportunities for communication with those working other shifts and divisions. By increasing opportunities for intra-agency information sharing and collaboration, an ESSP successfully employed by police departments has a high potential of affecting the way in which we view intelligence.

As discussed earlier, there are many views on the nature and definition of intelligence. Most police "intelligence" comes to officers in the form of crime bulletins or officer safety bulletins that are classified for law enforcement use only. Though these bulletins may be thought of as intelligence products, a large number of them would be better classified as criminal information products due to the lack of analysis in producing the final product. The aspect of "analysis" is the commonly accepted distinction between

[186] Lee and Lan, *From Web 2.0 to Conversational Knowledge Management: Towards Collaborative Intelligence*, 47–62, 57.

[187] Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*, 90.

an information product and an intelligence product. One definition of analysis is " using the scientific approach to problem solving."[188]

For example, a specific burglar's personal data, arrest history, and methods of operation are simply information. Even if this information is sent out to officers because the suspect is believed to be actively committing crimes, it would still be considered criminal information. However, an analyst may pull data showing the dates and times for burglaries for the past month. Using this information, the analyst notes that the there was a decrease in burglaries during the five days the suspect was in jail over another case. The analyst would also be able to use predictive analysis to determine the day of week, time, and location the suspect is likely to strike next. As a result of the analysis done, the product would be considered criminal intelligence.

Keeping in mind the emergent element of ESSPs and the collaborative environment it creates, the use of ESSPs could further blur the lines between information and intelligence. When an analyst is responsible for the product, the point of analysis can be identified, and it is relatively easy to determine when information becomes intelligence, but when numerous officers become part of the process, it becomes less clear.

In a traditional hub and spoke network, an analyst gathers information from various resources and users. The analyst then creates a product and disseminates it. The analyst and author of the product is a single point from which limits on the information's distribution may be applied with the input of supervisors. In cases where the information or intelligence sensitivity is identified at its inception, ESSPs allow for restrictions on dissemination and whether or not users may make modifications. However, depending on the level of distribution permitted, restrictions limit or even prevent the collaborative/social aspect of the ESSP.

An ESSP flattens the network to where each user in the network has the potential to create, view and further develop information and shared intelligence. In those cases

---

[188] Carter and United States, Dept. of Justice. Office of Community Oriented Policing Services, *Law Enforcement Intelligence a Guide for State, Local, and Tribal Law Enforcement Agencies*, 9.

where an intelligence product is disseminated, the rules of handling can be made clear from the beginning. A question arises regarding when individual contributions to a blog, a wiki page, or other Web 2.0 tools become intelligence. This issue highlights the emergent nature of intelligence. Individual bits of information shaped by collaboration between users over time could be said to have the potential of becoming intelligence. Due to the different legal implications associated with information and intelligence, recognition of this issue and a path for addressing it is needed.[189]

Considering the above example with our hypothetical burglary suspect, but without the crime analysts input. Using an ESSP, an officer may post a blog asking for help in stopping a burglary series in the officer's beat. Another officer, more adept at using available crime data, puts together some data and posts a response that includes days of the week and times that the burglar is most likely to strike. Another officer recognizes a suspect description from one of the incidents and provides a possible suspect that the officer had arrested a couple of weeks ago. Looking further into it, the requesting officer finds that the suspect was in jail during a week when there were no burglaries in his area.

The information in this example is essentially unchanged from the earlier example. An argument could be made that the blog with the above provided information is now an intelligence product. The primary difference between the two was that in the first example a professional analyst did the work. As is the case with many departments, the analyst may even be a police officer filling that role. One author noted that "Crime analysis does not replace the field work and investigative skills of sworn personnel in a policy agency, but is designed to complement and add value to that work."[190] It may very well be that the definition that states information must include analysis to be considered intelligence is too broad of a definition, or at least that "analysis" is too widely applied. If "analysis" can be applied to any officer's investigation, it loses its descriptive value. As

---

189 Carter and United States, Dept. of Justice. Office of Community Oriented Policing Services, *Law Enforcement Intelligence a Guide for State, Local, and Tribal Law Enforcement Agencies*, 12.

190 Bruce Taylor, Rachel Boba, and Jeff Egge, *Integration of Crime Analysis into Patrol Work: A Guidebook*U.S. DOJ: COPS, 2011), 12.

police departments develop software that simplifies the process of analysis, clearer definitions for the term of analysis will be needed.

Though criminal intelligence has existed in law enforcement for over 100 years, it lay within the "murky backwaters of policing."[191] Applying intelligence definitions within a municipal police agency's daily operational environment may be outside the intentions of the writers of 28 CFR Part 23. This idea is supported by a policy clarification that stated the regulation was not intended to regulate criminal information records management systems. Regardless, if another officer finds out that the burglar may be committing the crimes to support an overseas terrorist organization, most would agree that the line between information and intelligence has been crossed.

Police agencies strive to increase efficient police operations by applying the latest technologies. They also seek to stay within commonly accepted guidelines and must abide by applicable laws intended to protect the rights and privacy of individuals. Laws and regulations do not take into account the emergent properties that come with the use of many new technologies including ESSPs. These technologies will change the nature of how police work with information and intelligence. Laws and regulations must be updated to take these new capabilities into account, or they will continue to produce confusion in their application resulting in barriers and resistance to advancements in communication.

[191] Ratcliffe and Police Foundation, *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*, 14.

VI. IMPLEMENTATION OF A DISRUPTIVE INNOVATION

Salesmen of one type or another continuously bombard law enforcement leadership with the next new thing. Whether it is a new technology, such as license plate readers, or a policing concept, such as CompStat, the expectations often exceed the reality. In many cases, the problem may not be with the technology itself, but in the manner of implementing it. Though the need for an implementation plan is not a new idea, it is one that is often overlooked. If a project fails, it is likely due to one of three reasons, money, the technology, or leadership. Cases where a lack of money results in a projects failure are relatively easy to identify. But in cases where sufficient funding is available, yet the project still fails, identifying the culprit may prove to be more difficult. After all, often the leadership assigning blame is also responsible for the technologies implementation. It is far easier to blame an unfeeling technology than people. Of course, simply blaming leadership is too simple, of an answer. Failures in implementing new technologies may be a result of insufficient consideration of the social aspects, and an excessive focus on the technology itself.[192] Conversely, organizations that have been successful in implementing new technology have been recognized to include the impact of the technology on social relationships.[193] The true failure is in the implementation strategies used by leadership that do not take these factors into consideration, and in some cases, the lack of an implementation strategy.

This chapter will focus on developing an understanding of system issues, implementation processes, and necessary strategies needed to successfully integrate new processes and technologies into a department's culture and infrastructure. Any new technology is subject to failure, despite the best of strategies, but without a plan, the idea will most assuredly fail, regardless of the value of the technology.

---

192 Lehaney et al., *Beyond Knowledge Management*, 61.

193 Ibid., 66.

A. TECHNOLOGY ADOPTION CYCLE

Though the concepts of Enterprise 2.0 and ESSPs have been around since 2006[194], within police agency environments, they still remain in the earliest stage of adoption—referred to as the innovation stage.[195] "Innovation" is the first stage in the Technology Adoption Life Cycle (TALC). Police leaders seeking to adopt ESSPs for their agency should find value in understanding the TALC, which is a model that describes the rate in which consumers adopt new technology. TALC is described as a cycle because of the ever-returning tide of new innovations in technology. By understanding consumer adoption habits, leaders are in a better position to nurture the adoption of technologies within their own departments.

Figure 2 shows the other stages of the TALC: early adopters, early majority, late majority, and laggards. Getting innovators to sign onto a new technology is relatively easy because these innovators relish new technologies and will seek them out. They are valuable not because of their numbers, but because they become the evangelist that bring in the early adopters. Early adopters tend to be comfortable with new technology, but prefer to wait until they find a product that they find to be a strong match to their needs prior to adopting a new technology. Unlike some technologies that can be thrust upon employees, such as cameras in police cars, the use of ESSPs is highly dependent on voluntary user interaction. Though the user does not have to invest the monetary resources, their adoption of a new technology still requires a commitment of time, and a change of habits. Either of these factors can be as significant a factor in adoption as money.

It is in moving beyond the early adopter to the early majority stage that the potential for the successful adoption of a new technology is most vulnerable. The gap between the two stages can be described as a chasm.[196] As innovators and early adopters

---

194 McAfee, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*, 12.

195 Geoffrey A. Moore, *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers* (New York, NY: Harper Business Essentials, 2002), 5.

196 Ibid., 5.

take on a new technology, the hype often exceeds the actual benefits of the new technology. This results in disillusionment among users, which has the potential of killing off a new technology before the technology's salesmen and leaders are able to sell the early majority of users on the new technology.

The chasm between early adopters and the early majority is emphasized because of the exceptionally high potential for failure during the transition.[197] A crucial step needed for the successful adoption of a new technology is winning over the early majority. The early majority, while also comfortable with new technology, is pragmatic in their approach. They seek out recommendations from innovators and early adopters before they are willing invest in the new product. Even if an early majority adopts the new technology, there is still the potential for failure as the cycle moves to the late majority. The late majority recognizes the passing nature of many new technologies, and prefers to allow others to take the risks. Well-established technologies are the preference for this group. The last group is referred to as laggards.[198] These are the neo-luddites that will not accept new technologies until they are dragged kicking and screaming into the future. On my own department, I recall a number of officers that failed to see the value of computers in police cars and vigorously resisted using them. Ironically, once they were forced to use the new technology, they became some the biggest supporters. Fortunately, there are few laggards in leadership positions.

---

[197] Geoffrey A. Moore, *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers* (New York, NY: HarperBusiness Essentials, 2002), 20.

[198] Ibid., 14.

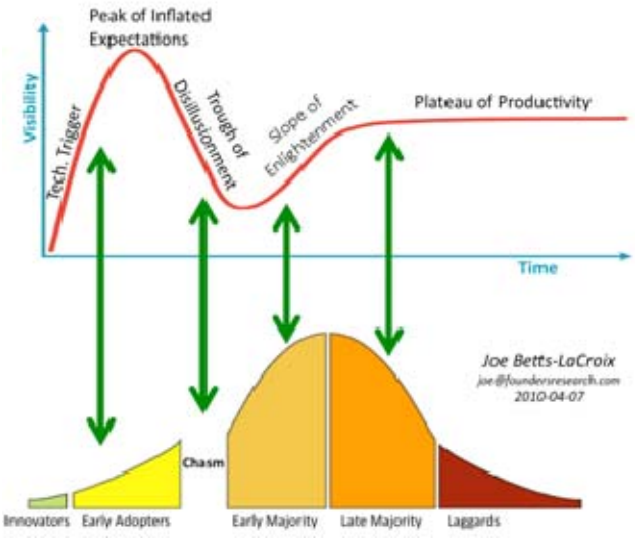

Figure 2. Hype Cycle/Technology Adoption Life Cycle[199]

B. DISRUPTIVE INNOVATIONS

Technological innovations can be divided between continuous and discontinuous innovations. Internal ESSPs, especially when integrated as part of the organizational culture, would fall under the category of a discontinuous innovation. A discontinuous innovation is technology that requires a change in behavior, or modification of other systems or products to fit with the new technology. [200]

The previous technological paradigm involved the automation of transactions, which emphasized management control, tightly controlled user interaction, and complex technological investments. Figure 3 shows the impact of the adoption of Web 2.0 tools on productivity over time. This figure illustrates that though a new technology may have short-term disadvantages, over time it will likely surpass older technologies.

Although the concept of ESSPs is a discontinuous innovation, the degree in which it is a disruptive one will be impacted by the manner of implementation and the technologies currently being used by individual agencies. The difference between a

199 Joe Betts-Lacroix, "Hype Chasm " *Evocator* (Wednesday, 7 April 2010).

200 Dan Yu and Chang Chieh Hang, "A Reflective Review of Disruptive Innovation Theory," *International Journal of Management Reviews* 12, no. 4 (2010), 435–452, 417.

continuous and discontinuous innovation is not a bright line but a continuum.[201] An agency with a static intranet, such is commonly used for document sharing and limited information dissemination, may find a shift to an ESSP a very discontinuous innovation due to the degree of cultural and technological change needed for implementation. However, a department that already values collaboration and that has some elements of an ESSP, such as a forum or blog, would experience less disruption when shifting to a full ESSP. For some progressive departments, the shift may even be considered a continuous innovation since an ESSP can be implemented incrementally. Unlike many other technologies, such as the disk drive market Christensen wrote about in *The Innovator's Dilemma*, an ESSP's Web 2.0 elements could be implemented in parts or as an entire system. However, for most departments, the move to an ESSP will be discontinuous innovation.

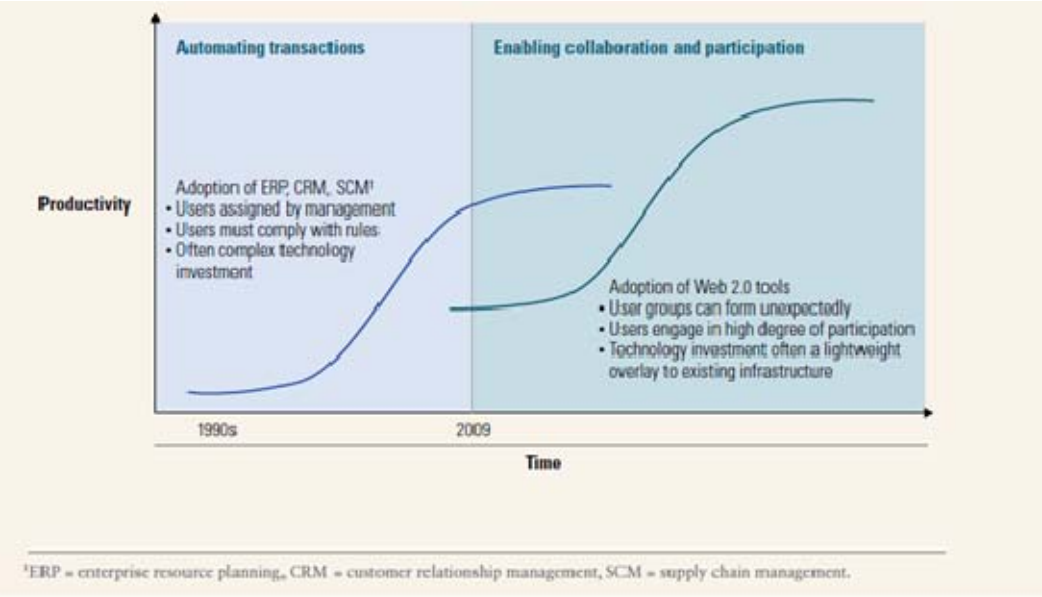

Figure 3. Web 2.0 Productivity Impact

201 Moore, *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customers*, 11.

Disruptive technologies are defined as tools that "impact existing social structures—ways of interacting, power relationships, and access to key resources."[202] An ESSP would also be considered a disruptive innovation due to its dramatic shift away from current information dissemination technologies that emphasize the management's viewpoint. Typical intranets do not emphasize collaboration and person-to-person information sharing. Posting of information is limited to staff, or a few select administrative personnel. Some more advanced intranets will allow commenting, but limited to topics preapproved by administrators. A social intranet applying Web 2.0 tools provides a platform that allows for dissenting views and debate. Rather than empowerment being a buzzword, it becomes a reality that some managers may find threatening.[203] ESSPs are a new paradigm in business technologies, so disruptions should be expected.

As a disruptive technology, the implementation of an ESSP may face significant resistance. Good management and best practices improve the quality for every level of change. However, the very decision-making and resource allocation processes that are key to success are the same processes that reject disruptive technologies because of management's reliance on old business processes and hierarchical communication structures.[204] Even with management support, employees within the organization are unlikely to adopt a new technology, especially a disruptive one, if it does not meet provide them a method that they recognize as a mean to fulfill individual and organization needs.[205] Recognizing the role of a new technology as a discontinuous and disruptive innovation can help management develop a successful plan for adoption.

---

202 Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Boston, Mass.: Harvard Business School Press, 1997).

203 McAfee, *Enterprise 2.0: The Dawn of Emergent Collaboration*, 26.

204 McAfee, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*, 162.

205 Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, 104.

C. ADOPTION CONSIDERATIONS

Technology implementation in the law enforcement arena tends to be of a sustentative nature. Changes through the use of sustaining technologies are incremental, which minimizes the impact they have on the overall culture.[206] These sustaining technologies allow for the continued operation of firmly stabilized systems within the department. Implementation of Web 2.0 technologies often will be disruptive to these embedded systems. Current social structures, technology structures (information feeds), individual role expectations, and agency policies are based on the legacy system.[207] Because of these factors, it is difficult to implement disruptive technologies within any current sociotechnical system.[208] In addition, managers may not recognize the potential benefit of these new systems due to risk aversion and entrenchment in the current system including established routines and training.[209] In order for any new proposal to receive even a modicum of support, these factors need to be incorporated at all levels of the implementation process.

Creating a receptive culture in a police environment must take into account all levels of personnel including officers, detectives, analyst, and staff. The sociological aspects must be considered as a critical factor in the adoption of any new technology or process. Regardless of the infrastructure used for collaboration, whether it through human –computer interfaces or person-to-person, the environment in which the infrastructure is implemented consists of personal social interaction.[210] Sociotechnical design provides a framework for such an analysis. Simply put, the sociotechnical process is defined as “a

---

206 Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, 11.

207 Frank W. Geels, “The Dynamics of Transitions in Socio-Technical Systems: A Multi-Level Analysis of the Transition Pathway from Horse-Drawn Carriages to Automobiles (1860–1930),” *Technology Analysis & Strategic Management* 17, no. 4 (12, 2005), 445–476, 441.

208 Ibid., 450.

209 Yu and Hang, *A Reflective Review of Disruptive Innovation Theory*, 435–452, 441.

210 Brian Whitworth, “Socio-Technical Systems,” *Encyclopedia of Human Computer Interaction* (2006), 533–541. doi:10/30/2006. http://brianwhitworth.com/hci-sts.pdf, 533.

way of implementing technology in the social environment."[211] Elements of sociotechnical systems include technology, regulation, user practices, and cultural meaning.[212] The sociotechnical approach recognizes the impact that current social networks and their varied objectives have on technical systems. Social and technology factors, along with economic and technological objectives, must all be taken into account.[213]

McAfee suggests four factors that contribute to the successful adoption of Enterprise 2.0: a receptive culture, common platform, an informal rollout, and, managerial support.[214]

Getting buy-in from employees is critical for the success of an Enterprise 2.0 style ESSP. ESSPs on the Internet can potentially draw from all Internet users. A successful business in this environment needs only a small percentage of users to contribute to the ESSP. This is fortunate, since it is only a small percentage of users that actively contribute to a ESSP. [215] This makes it critical for an agency developing an internally limited ESSP to draw in the broadest possible base of its employees as active users. Smaller agencies cannot succeed in establishing a successful ESSP without drawing in a higher percentage of contributing users than are found in publically accessible social media platforms. The number of participants and contributors to an ESSP is a key factor in sustainability.[216] To compensate, police agencies must understand employee resistance to new technology. McAfee surmises that many users are reluctant to adopt new technologies due to their personal understanding of, and comfort in, using established technologies. For an ESSP to be successfully adopted, agencies must be prepared for the

---

211 Lehaney et al., *Beyond Knowledge Management*, 61.

212 Geels, *The Dynamics of Transitions in Socio-Technical Systems: A Multi-Level Analysis of the Transition Pathway from Horse-Drawn Carriages to Automobiles (1860–1930)*, 445–476,446.

213 Lehaney et al., *Beyond Knowledge Management*, 43.

214 McAfee, *Enterprise 2.0: The Dawn of Emergent Collaboration*, 26.

215 McAfee, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*, 162.

216 Cummings, Massey, and Ramesh, *Proceedings of the 27th ACM International Conference on Design of Communication - SIGDOC '09; Web 2.0 Proclivity*, 258.

"long haul." Continuous support, demonstrations, and training will be needed for an extended period of time.[217] Leaders must recognize that in addition to learning new skills, employees are also learning new behaviors.

One method of getting buy-in from employees is through the cooperation of respected ESSP believers within the department. Using these leaders as internal cheerleaders and champions of the ESSP for coaching, training and encouraging, both in person and online, users can bring increased understanding of the benefits of the new technology.[218] Encouraging these early adopters helps build a base from which to address the early majorities concerns.

New ESSPs are most easily implemented when they do not replace an existing tool, but instead provide new functionality that is of benefit to the users. Facebook and Twitter are two examples of tools that did not seek to replace systems of communication, but provided entirely new methods. Enterprise 2.0 tools that are similar in nature to existing communication tools should be designed to work with those tools. Blogs, wikis, and RSS feeds often provide ways to incorporate the use of email for notifications and updates.[219] Without integration of current systems, a successful move to an ESSP is unlikely due to the nature of systems to endure continuous nondisruptive technologies, as long as current interconnections and purposes remain unchanged.[220]

With time, users should find that it is more efficient to adjust their work habits until a point is reached where the Enterprise 2.0 tools become the preferential format for communication. It is at this point that the ESSP has the biggest potential for dramatic increase as the result of a positive-feedback cycle.[221] As more users interact with the system, more value can be derived from the system.

---

[217] McAfee, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*, 171.

[218] Ibid., 175.

[219] Ibid., 177.

[220] Meadows, *Thinking in Systems: A Primer*, Kindle location 453 of 4207.

[221] Mitchell, *Complexity a Guided Tour*, Kindle location 4181 of 7309.

Leaders can facilitate this transition by identifying Web 2.0 alternatives to current processes, such as the use of a wiki for group discussions rather than email, or by posting a new policy proposal as a blog. Users can use tags rather than bookmarking favorite sites. Instead of storing documents in a personal folder, the documents could be stored in publically available document managers that index the files.[222] Eventually, Enterprise 2.0 tools may be fully integrated with current records management systems, personal and public document storage, and other databases. The higher the degree of integration with currently existing systems, the more potential there is for successfully improving the networking of information and employees.

McAfee, the author who coined the term Enterprise 2.0, suggest an informal rollout of new ESSPs. A formal rollout denotes new responsibilities rather than new abilities. Many employees perceive any expectation to use the new tools as an added responsibility on top of an already busy schedule.[223] The use of these systems should not be dictated, but supported by users that find value in the adoption of these tools.

Others suggest targeted deployment of new technologies to areas that are limited to smaller groups or units.[224] Starting the ESSP off with a small group of users will serve two purposes. First, it will create a group of supporters who have a vested interest in the success of the system due to their involvement. As they find value in the new system, they will serve as advocates for it. Management can evaluate the ways in which the technology is being used, and troubleshoot problems that arise. Successful aspects can be scaled up, while less successful ones can be modified to meet the needs of users.[225]. Limiting the initial rollout to small groups may also drive demand by increasing a sense of exclusivity around the program. A program being used by a robbery or homicide unit may result in an increased desire from other personnel to benefit from the same tools. In

---

[222] McAfee, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*, 110.

[223] McAfee A. P., *Shattering the Myths about Enterprise 2.0*, 4.

[224] Cummings, Massey, and Ramesh, *Proceedings of the 27th ACM International Conference on Design of Communication - SIGDOC '09; Web 2.0 Proclivity* , 262.

[225] Chui, Miller and Roberts, *Six Ways to Make Web 2.0 Work*, 64–75, 4.

addition, the starter group will create stock within the ESSP providing a base of information for users to build on. Additional stock can be taken from other informational sources that the ESSP is designed to supplant.

Contrary to the traditional dictation of specific processes by management, the way in which employees choose to use ESSPs to accomplish organizational goals will be made evident by their behavior.[226] Forcing users into a still developing system will likely result in their viewing of the system as of little value. By allowing innovators, enthusiastic users, and other leaders in the agency to lead the way, content can be developed while allowing others to explore and adopt the new tools as the perceived value increases. Even simply establishing policies regarding the use of ESSPs may restrict the emergent nature by anchoring and framing the system rather than allowing its development along lines that are of most benefit to users.

As with any significant change in technology, the first step for management should be the setting of goals. The goals of ESSPs are not inherent in their design. Though they increase the potential for information sharing and collaboration, these are not the goals of agencies, but they are simply a means of achieving goals. The goals of an ESSP within police agencies may include improving criminal information sharing to aid in the identification of crime trends and criminal suspects, so that the trends can be stopped, and suspects arrested and prosecuted. Another goal is the production of broad criminal intelligence that may or may not specifically address short-term objectives, but creates information to aid analyst in achieving a deeper understanding of crime issues. Additional information could be developed though the use of data mining techniques. Each agencies goal will vary. In keeping with the collaborative spirit of Enterprise 2.0, the goals and objectives should be determined by a consensus of the parties using the system.

In addition to developing clear goals, it is incumbent on leadership to send a clear message that employees' contributions to the ESSP are valued. Contributions to ESSPs benefit the whole of the organization, but may not correspond to current evaluation

---

[226] Meadows, *Thinking in Systems: A Primer* Kindle location 407 of 4207.

system's normal measurements of employee performance. Employees may find more reward and recognition in following established processes that support individual goals rather than adopting new processes and the values associated with Enterprise 2.0.

Intellipedia staff helped to encourage Intellipedia use and associated values by recognizing active contributors through awarding small items, such as a plastic shovel, or coffee mug with words of encouragement printed on them. The editor's supervisor was also sent a letter of appreciation in recognition of the contributions. Google gave away shirts and cash prizes as incentives. In addition to providing boosts to an employee's moral, the recognition also inspired more discussion about the technologies being used.[227]

Despite ESSPs being user driven, successful adoption requires the leadership of senior staff. A few simple words of encouragement or a response to a blog post by the chief can also go a long way in encouraging participation. Even better, the chief and other police leaders can blaze the path for employees' use of the system by using Enterprise 2.0 tools to reach out to employees and to gather needed information and input.

D. THE NEXT STEPS

Before specific steps for the implementation of an ESSP should even be considered, all levels of department leadership must foster an environment that encourages horizontal, as well as vertical communication and collaboration. Reducing barriers to the flow of information will be a challenging step for agencies where the control of information is a power base for many personnel. Reward systems based on the end results of efforts by individuals must be replaced with systems that recognize and reward an individual's participation and contributions to processes that lead to both successful and unsuccessful outcomes. Messages that an agency supports collaboration will be quickly dismissed, if an employee finds that their evaluation is still focused on

[227] McAfee, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*, 193.

individual production statistics. An ESSP will only magnify the collaborative atmosphere of a department. An agency weakly supporting collaboration will see this same attitude reflected in their ESSP. The ESSP will fail as a result.

Though the need for an ESSP to improve information sharing and collaboration may be clear to innovators, buy-in must come from the users of the system. A first step in implementing an ESSP is to form a committee of personnel selected based on their ability to handle change. These personnel should be known for their innovativeness and forward thinking attitudes. Specialty units that require a high level of communication with other units are a good place to start. The ESSP development should be based on the needs of these users.

An ESSP specification document is needed to outline the needs of users and detail the process of how the system will be implemented. Following the Defense Department mantra, "You should adopt before you buy and buy before you create," open source products should be used when possible. Absent open source options, off-the-shelf software should be purchased. Only if neither of these options is available should custom designed and built systems be considered.[228] Implementation of the software should be done incrementally when possible. This approach allows for modifications to the overall implementation plan as users needs are better understood, and paces the amount of adaptation needed by users..

Most importantly, managers should remember that ESSPs are complex adaptive systems, which will require the ability to make frequent updates and changes to meet the evolutionary needs of users, as they themselves adapt to the new system. This level of flexibility will require budgetary considerations to ensure that frequent changes are possible within financial constraints.

As the system is rolled out to the rest of the agency, staff contributions will be invaluable. Keeping in mind that information is power, by allowing all levels of

[228] Jason Miller, "Intellipedia Provides Lessons for FedSpace Initiative," FederalNewsRadio.com, http://www.federalnewsradio.com/?nid=697&sid=1949950.

personnel direct access to communication from leadership will provide a sense of empowerment to personnel and motivate further participation in the ESSP.

Taking these factors into consideration can help organizations to manage change successfully. The overall goal is to create systems that capitalize on the skills of individual employees, groups, and organization to create an environment conducive to collaboration and increased productivity. This also serves to breakdown traditional unit barriers to allow the organization to act as a single entity rather than a multitude of separate units.[229] If police departments wish to take advantage of the extensive knowledge within the organization, they must create a culture and environmental structure that encourages coordination including the sharing of information and collaboration.[230]

[229] Lehaney et al., *Beyond Knowledge Management*, 41.

[230] Ibid., 66.

VII. CURRENT PRACTICES AND CASE STUDIES

A. CURRENT PRACTICES (TULSA POLICE DEPARTMENT)

For the purpose of improving understanding of how ESSPs can be potentially used to improve sharing of and collaboration on information within a police environment, this chapter will address information flows within the Tulsa Police Department (TPD). Although the TPD may not reflect the current state of patrol and investigative level information sharing within municipal police departments, informal surveys of officers and staff with other police departments indicate that it has more similarities than differences.

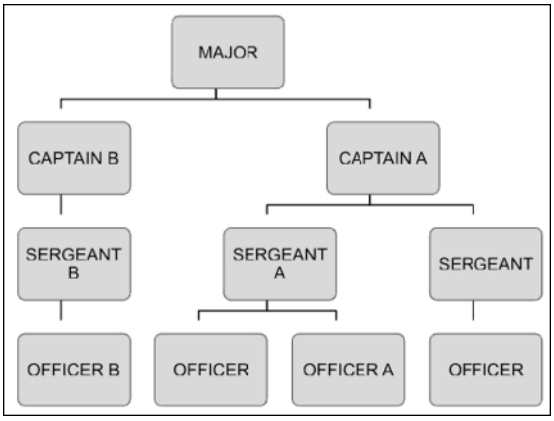

Figure 4. Hierarchical Information Flow

Another point to note is that software and other technological changes in law enforcement are rapidly changing. When the idea for this paper was initially being developed, no examples of the use of ESSPs within any municipal police department could be found in the literature. As of this writing, reports on of the use of ESSPs in no less than half a dozen police departments have been found. I fully expect that this number will increase at an exponential rate.

Figure 4 provides an example of the hierarchical flow of information within a typical police organization. In order for information to be transferred from Officer A to Officer B, it must first go through Sergeant A to Captain A, back to the Sergeant B and

then to Officer B. Though officers are permitted to communicate directly, due to shifts, days off, and personal relationships, the communication is likely to follow the pattern described. If direct communication does occur, it will likely be by phone or email.

One example of information flow in a typical police organization is shown in Figure 5. Using a crime bulletin as an example, Figure 5 depicts the pathway information may take to reach an officer. The crime bulletin created by an analyst is typically sent to division commanders, shift commanders, and other interested personnel. The bulletin may also be posted on the intranet. What often happens next is that the bulletin is forwarded by email to the squad supervisor by both the division commander and the shift commander. The squad supervisor and the officer may also obtain it through visiting the intranet. The squad supervisor then forwards it by email to the officer and will discuss it as squad meeting. In a process sometimes referred to as circular reporting, supervisors and officers commonly get multiple copies of the same bulletin. The process does not change due to occasions when needed information is not forwarded as expected, and the source not having access to all relevant parties. The general belief seems to be that it is better to get information multiple times than for it to not have reached those who might have a need for it.

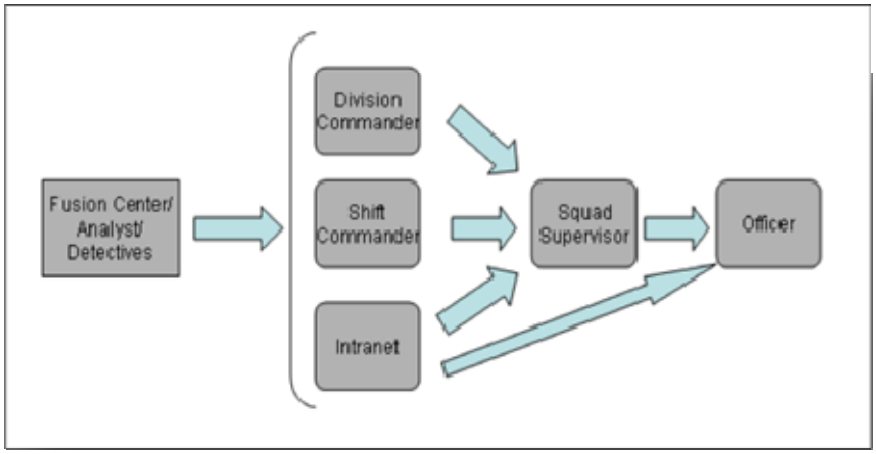

Figure 5. Criminal Information Dissemination

Figure 6 delineates how information in the form of feedback is returned to the sources described in Figure 5. While information can flow in the opposite direction, as shown in Figure 5, common practices show that it flows as depicted in Figure 6. Officers complete an incident report or suspicious activity report that then can be accessed by analyst and detectives for further investigation and analysis.

The main point in providing Figures 5 and 6 is to show the multiple layers in between the information source and destination points. Multiple layers increase the time it takes for the information to reach its destination and the likelihood that it will be duplicated (multiple copies to destination). In addition, the layers increase the likelihood that information may be lost or altered during the transfer process(es).

Figure 7 shows the transfer mechanisms used to transfer information from multiple sources to the intended recipients. Recipients desiring information on a particular topic may have to go to each source to insure that all relevant information is obtained. Even then, vital information may be missed if the right person is not consulted, if the right search is not conducted, or if multiple sources of information on the intranet are not checked. Integration of these various sources of information is limited due to the methods in which the information transferred. Documents that are emailed to officers have little potential value if the information contained is not put into context. Being informed that a person has been paroled for armed robbery is far less valuable than knowing that the person that the officer has stopped for a traffic violation is on parole for armed robbery. Context is essential to giving meaning to information so that it is of value of the officer.

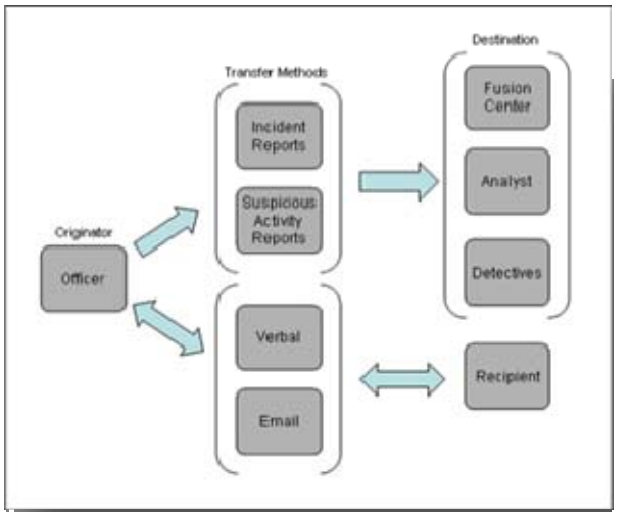

Figure 6. Information and Feedback Flow

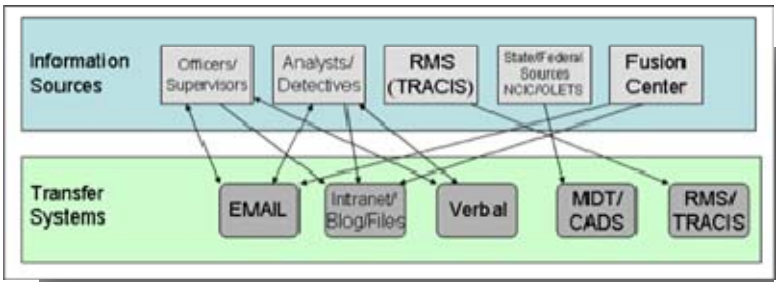

Figure 7. Information Transfer Methods

B. CASE STUDIES

Two cases that were found to be directly applicable to policing were identified: (1) the Redlands (California) Police Department, and (2) *Intelink*. The initial research plan was to research the use of emergent social software platforms (ESSPs) in secure internal police environments. Despite the wide public recognition of the value of social media, there were sparse examples of individual Web 2.0 tools being used in such a policing environment, and no documented examples of the use of ESSPS. While shaping the idea for this paper, a news story was found on the efforts of the Redlands (CA) Police Department (RPD) to use an ESSP in policing.

The RPD graciously granted this researcher access to their live CopBook site for study. Based on this access, a firsthand look at the site's structure, capabilities, and current use greatly informed this research. However, access to the site's individual groups was necessarily limited due to individual group approval processes, membership requirements, and security considerations. While the access provided was broad, these limitations were a factor in my overall perceptions of the site including participation levels, and content quantity and quality.

The second case study was of the Intelink system. Unlike the RPD's use of CopBook, Intelink is an intra-agency tool. As a sworn police officer, I have unclassified level access to Intelink. Intelink also had the research advantage of being well documented. The site also provides usage data and statistics. Even though it is not designed for internal information sharing on a field policing level, it is a leader in the use of Web 2.0 tools in a loosely, though increasingly, connected ESSP.

Not surprisingly, these systems are a work in progress. Research on complex adaptive systems, such as ESSPs, has long challenged researchers. In the case of ESSPs and social media, adaptations are rapidly occurring, which makes research in this area all the more challenging, and interesting.

1. Redlands California Police Department

a. Overview

The City of Redlands Police Department (RPD) is recognized as a leader in applying social media concepts in policing. An article in Law Officer Magazine noted that the RPD is "forging a new path that could become a model for law enforcement agencies across the country."[231] Redlands Police Chief Mark Garcia implemented an ESSP called CopBook with the goals of allowing instantaneous information sharing for

[231] "First Facebook, Now There's 'CopBook'," LawOfficer.com, http://www.lawofficer.com/article/news/first-facebook-now-theres-copb.

officers and providing a searchable repository of information. Chief Garcia sees CopBook as a means to maximize officers' ability to solve crime and provide effective service to the community.[232]

In 2010, The RPD partnered with the Effia Group to develop CopBook. CopBook was created with the Jive Platform. This was done under a grant from the Bureau of Justice Assistance to further develop the platform and evaluate its effectiveness. The project, which is still underway as of August 2012, includes the objectives of identifying good practices needed to drive internal adoption and determining the best way to integrate the public into the system while still maintaining appropriate and necessary security. The ultimate goal of the project is to provide a platform for knowledge mining within the agency, with other agencies, and with the public in a secure space to address crime and disorder issues.[233]

b. Web 2.0 Applications

CopBook allows officers and other authorized individuals to access information from a desktop, tablet computer, smart phone, or any other device with a web browser. Users can access CopBook from a smart phone application. As the name implies, CopBook shows clear inspiration from Facebook. This is an advantage in that any user comfortable with Facebook will have little difficulty in navigating CopBook. The overview page shown in Figure 8 includes recent activity, groups, available actions, and a section that shows top participants. Some actions that users are able to take include starting a discussion, posting documents, writing a blog, create a group, create a poll, create a task, send a private message, share videos and create a project. Users are also able to include tags along with information being posted, as well as see other tags being frequently used. The ability to search through the CopBook platform allows quick access to whatever information is being sought.

---

232 "First Facebook, Now There's 'CopBook'," LawOfficer.com, http://www.lawofficer.com/article/news/first-facebook-now-theres-copb.

233 Travis A. Taniguschi, *Using Social Business Software (SBS) to Enhance Public/Private Partnerships: A Collaborative Approach to Community Knowledge Mining*, ed. Jim Bueerman, 2011), 6.

Users also have the ability to suscribe to RSS Feeds. These feeds enable tracking of changes to individual pages. While changes are also shown on the overview page, the RSS feeds allow for tracking of particular pages of interest to the user. Users can access notifications of changes to these pages with a RSS aggregator, which is built into CopBook.

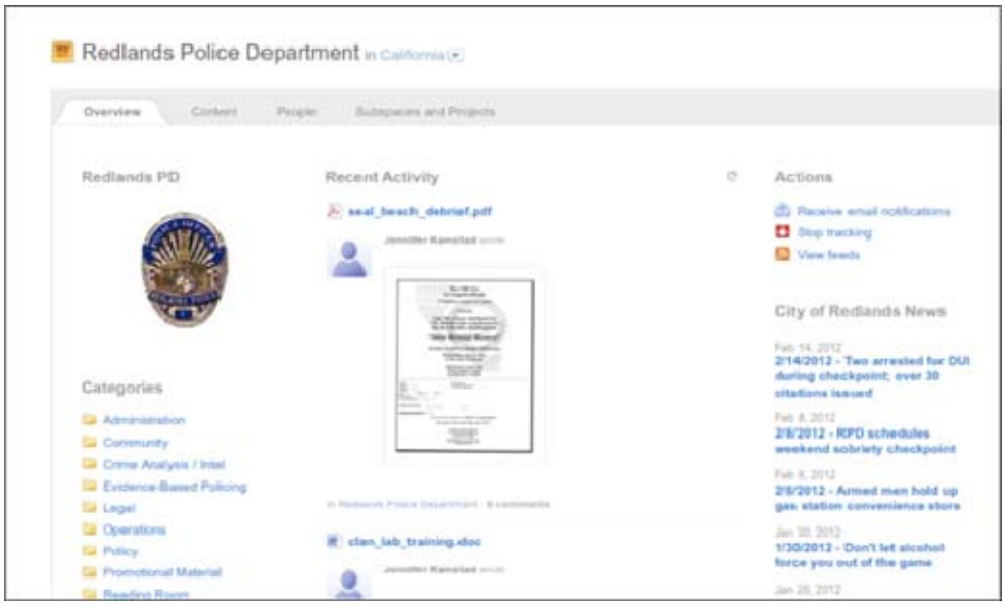

Figure 8. CopBook Overview Page

c. Structure

The structure of the RPD CopBook page is shown in Figure 9. The overview page serves as the user's home page. Tabs at the top allow the user to view content, people, and the subspace and projects pages.

The overview page content is organized into three columns. The first column allows for quick access to various information categories broken down by subject type. Category types include administration, evidence-based policing, legal, and promotional policy. Clicking on a category takes you to the contents page filtered to show the category selected. Also in this column are paths to discover new content based

on featured contact, tagging, and by top rated content as rated by users. The second column shows recent site activity based on the access levels of the user. This is also referred to as the user's stream. The third column allows the user to personalize and view notifications of site activity. This includes the ability for the user to receive email notifications of changes, change updates appearing in the recent activity column, or to change RSS feeds. The remainder of this column is dedicated to a City of Redlands RSS feed that shows the latest news.

The content page includes posted documents, blogs, polls, and discussions. The content can by filtered by category, user applied tags, or type. A search bar is another means for finding information. Users also have the ability to rate content with a "thumbs up" similar to Facebook, create bookmarks to items of interest, and to start and participate in discussions related to the documents. All users have the ability to post documents, create discussions, and even create polls. Items can be posted through the website, a mobile application, or even by email.

The people page shows a listing of the site's members. The listings include a picture of the member and show the number of people they are following and how many members are following them. Clicking on the photo, or name, links to the member's page set. The bio page allows viewers to see information the member has posted. Privacy settings allow each individual to customize the amount of information being shared. While name, email, rank, and expertise are required, including other information, such as an address, phone numbers, or a personal biography is optional. Members also have the ability to change their display photo, control notifications, and change other options. Additional tabs on the member's page allow for the viewer to see the member's involvement in the site including posted content, connections, and their places/spaces. The member can also create tasks, view bookmarks, and check private messages.

The final tab on the overview page links to a subspaces and projects page. This page allows members to view and participate in subspaces, or groups, that they have joined. For example, RPD is at a group level, while individual unit groups are at the subspace group, also referred to as social groups.

Projects are similar to groups in their organization but are task oriented rather than group oriented. Both areas allow for the creation of tasks and content specific to that group or project with the owner being able to set the level of access for other users. As with most other areas of the site, these pages can be tracked by email, project feeds, and recent activity tracking.

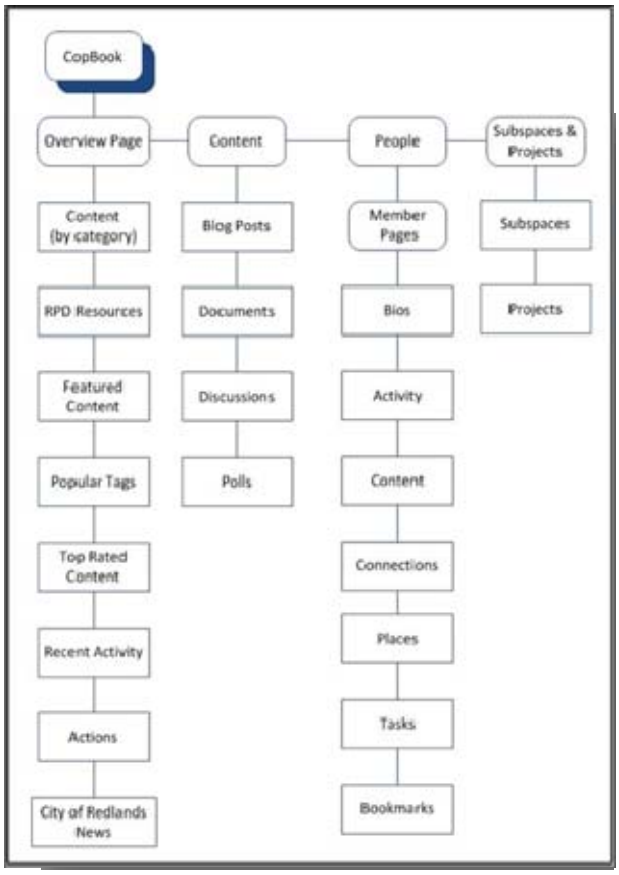

Figure 9. RPD/CopBook Basic Layout

d. Current Usage/Application

The RPD has brought along other area agencies onto the CopBook system. This includes the San Bernadino County Sheriff's office and the Rancho Cucomongo Police department. Numerous subspaces have been created including ones for the Emergency Operations Center, volunteers, investigations, and dispatch.

Statistics for the level of use by RPD employees were unavailable. The level of use will vary greatly by individual users due to group membership and activity that may not be viewed by other users. Based on this researcher's access level, the majority of content on the site are documents. Most of the documents are training announcements and training related documents. Blogs are the second most commonly used area of the site. Blog topics vary greatly. They include daily activity reports, news items, praise for good work, and various training topics. It appears that some items, such as the posting of daily activity reports in the blog section, did not catch on and are no longer being shared in this manner. The discussion area is being used primarily as a question and answer forum. Many of the questions are regarding the CopBook platform. Other topics discussed include training, as well as some limited discussion on crime concerns.

It appears that the CopBook systems saw some experimentation and usage by a limited number of users at the onset of the program. With time, the participation declined and contributions now appear to be primarily from system administrators and the training coordinator. Again, it should be noted that this researcher's access was limited and likely does not provide a complete picture of the usage levels.

e. Security and Legal Concerns

CopBook is based on the same platform used by the Directorate of National Intelligence (ODNI) and Defense Intelligence Agency (DIA) for the A-Space program. A-Space is a tool used by U.S. intelligence analysts at all security levels across U.S. intelligence agencies. Analysts use A-Space for real-time information sharing and collaboration on sensitive information.[234] The RPD is highly conscious of the legal concerns regarding any information sharing system. Due to the concerns, guidelines are being developed to ensure compliance with information sharing and intelligence

[234] Travis A. Taniguschi, *Using Social Business Software (SBS) to Enhance Public/Private Partnerships: A Collaborative Approach to Community Knowledge Mining*, ed. Jim Bueerman, 2011), 21.

standards. The mere fact that A-Space is being used by the federal intelligence community is a good indication that the CopBook structure, as a model for ESSPs, meets federal regulatory requirements.

Groups allow limited dissemination of information. Four security levels are available: open, members only, private, and secret. The “open” level allows for full access to group members and other users of CopBook. The member’s only level allows open access but limits posting and other direct participation to group members. With the private setting, only approved and invited group members have access to the site. The highest level of security controls access in the same manner as the private setting, but it also removes the group from the online directory. The private level is the most commonly applied security setting with 28 of the 29 subgroups operating at this level. One subgroup was members only.

The platform is externally hosted through the Sungard Corporation. The security provided protects secures the networks from both physical and digital internal and external threats. Physical security at the hosting facility includes an around the clock manned facility and monitoring, on-site security guards, dual authentication site access, and hardened server cabinets. For digital security, the system follows multiple levels of certification processes. Off-site data backup is also provided.

Data is securely transmitted through CopBook with the use of https. This is the same system used by online banking and commercial sites. An additional level of security can be added through the use of VPN when accessing the site from external sources. Within the CopBook platform, customizable user levels allow the user to control which elements of their profile can be viewed by other users. Information posted on the site can be controlled through the use of groups as described above. Information sharing with other agencies is strictly controlled. Only those users that have received explicit approval are permitted to view information from other departments.

f. Implementation

There is little documentation regarding the implementation process for CopBook. This is due to the experimental nature of the program. Determining good

practices for implementation is also one of the objectives for the overall program. One of the grant requirements is for the RPD to document the implementation process and provide a report to aid other agencies in the adoption of similar programs.

g. Future

CopBook has the potential of being integrated with existing records management systems and other databases. RPD has not yet taken the step to integrate other systems with CopBook, but is evaluating this as a possible future step.

RPD plans to eventually make CopBook available to community partners who will have the ability to capture, use, share, and increase their knowledge concerning crime issues. This is based on the recognition that the community has a different perspective from members of the police department on crime issues affecting the community. RPD intends to use this different perspective to help improve their own knowledge of the issues, and to improve decision making. A few of the community issues that RPD intends to use CopBook to facilitate discussion include homelessness, prisoner reentry, youth violence, and drug abuse.[235]

2. Intelink

a. Overview

Intelink, run by the Director of National Intelligence, is an information and intelligence-sharing tool used by the U.S. Intelligence Community. Created in 1994, Intelink has been recognized for promoting a shift from "need to know" to a "need to share" by, in part, providing a shared space in which analyst in the intelligence community can share intelligence and related information.[236] Intelink was established with the goal of providing a secure ESSP to allow for intelligence agencies to share and collaborate classified information. It was created with the understanding that to combat

---

[235] Travis A. Taniguschi, *Using Social Business Software (SBS) to Enhance Public/Private Partnerships: A Collaborative Approach to Community Knowledge Mining*, ed. Jim Bueerman, 2011), 9.

[236] "Intelink Basic Presentation," Intelligence Community Chief Information Officer, http://www.ndia.org/Divisions/Divisions/C4ISR/Documents/Breakfast Presentations/2010 Presentations/Intelink Basic presentation.pdf.

dynamic terrorist organizations, intelligence agencies must reduce information silos to increase their own ability to quickly address terrorist planning and actions.[237] Intelink systems are used for sharing intelligence and include tools to allow for collaboration, share media, and review raw intelligence.[238] Within the Intelink environment, blogs and Intellipedia enable analysts and divisions to establish a visible presence in the often closed and dispersed intelligence community.[239] Intelink access is open to federal, state, and local intelligence and law enforcement agencies. It is considered an internal social network but has a broader user base than some of the previously mentioned systems. Drapeau and Wells classify it as an internal networking tool due to its use being limited to the intelligence community.[240]

Intelink has multiple levels of security that allow users to access intelligence information that falls within their security clearance.[241] For the purposes of this paper, the controlled unclassified and FOUO level will be the focus. Called Intelink-U, this is the level of access typically given to law enforcement officials.

b. Web 2.0 Applications

Intelink includes Intellipedia and other social software tools including RSS feeds, social bookmarking, and photo and video sharing tools. Intellipedia, the intelligence community's version of Wikipedia, is the most widely known portion of Intelink.

Much like CopBook, Intelink has functionality that allows for the creation of blogs, document management, messaging, and multimedia sharing. Searches appear to

---

237 Frank DiGiammarino and Lena Trudeau, "Virtual Networks: An Opportunity for Government," *The Public Manager* (Spring 2008, 2008), 5.

238 Drapeau and Wells, *Social Software and National Security an Initial Net Assessment*, 8.

239 Nancy M. Dixon and Laura A. McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*, DIA Knowledge Laboratory, (2008), 9.

240 Drapeau and Wells, *Social Software and National Security an Initial Net Assessment*, 8.

241 Ibid., 8.

be based upon the application or area that hosts the search. The Intelink portal search function searches across multiple Intelink systems. A search in Intellipedia or the blog application is limited to that particular tool.

c. Structure

A key difference between CopBook and Intelink is the level of integration of the Web 2.0 applications. While CopBook functions as a single platform, Intelink acts as a portal to additional platforms. Figure 10 shows the basic layout of Intelink. As of May 2012, the overview page consists of an Intelink search bar and a series of icons that take you to the various applications, such as the blogs, bookmarks, eChirp, etc. A beta overview page is being tested. In addition to the above, the beta overview page includes additional methods of accessing data including a tag cloud, recent videos, quick links, and recent photos. The beta page, shown in Figure 11, is being actively changed and updated, so the final product may be significantly different. For example, one item that was added during the writing of this section was a section showing trending searches.

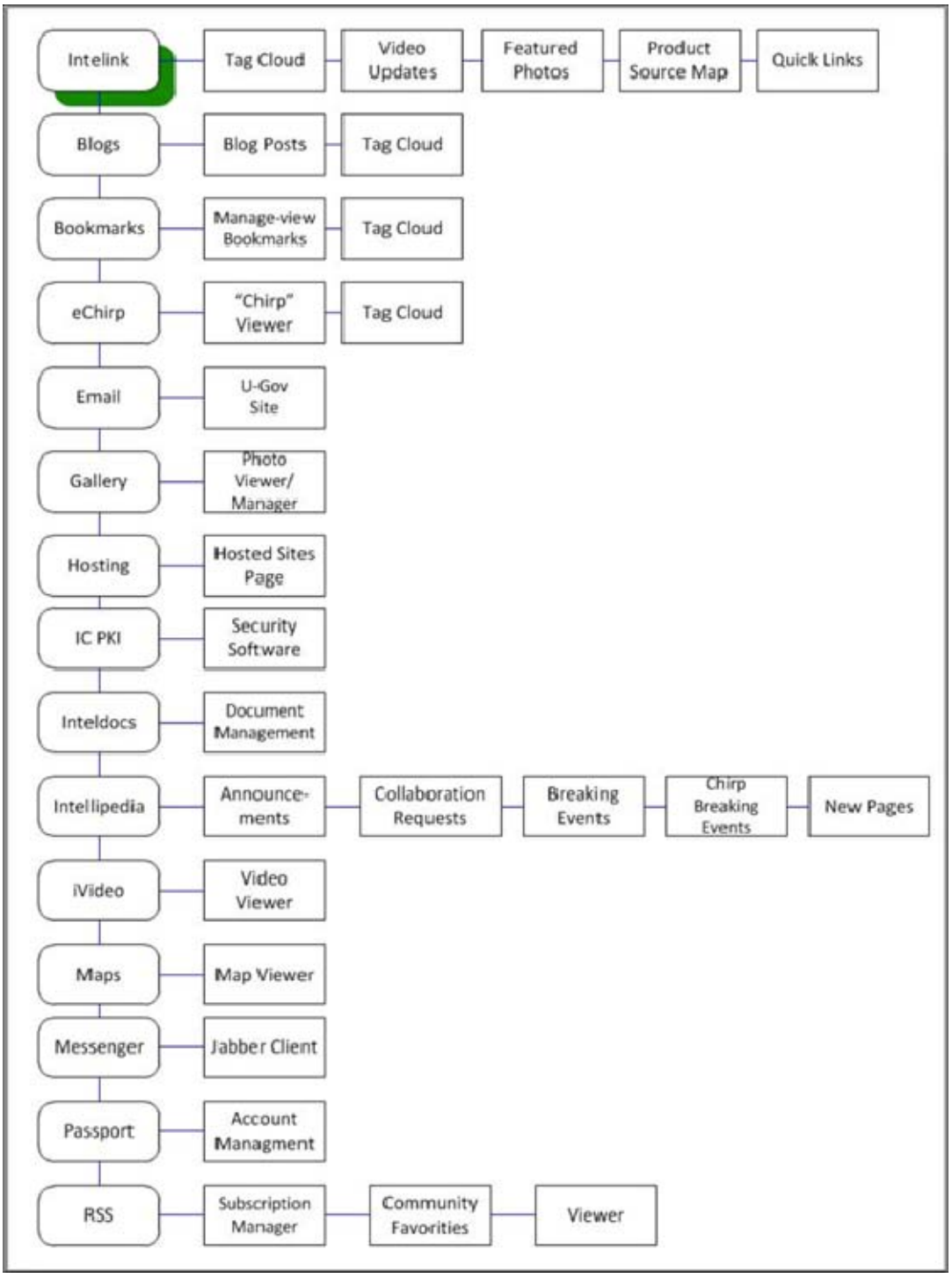

Figure 10. Intelink Basic Layout

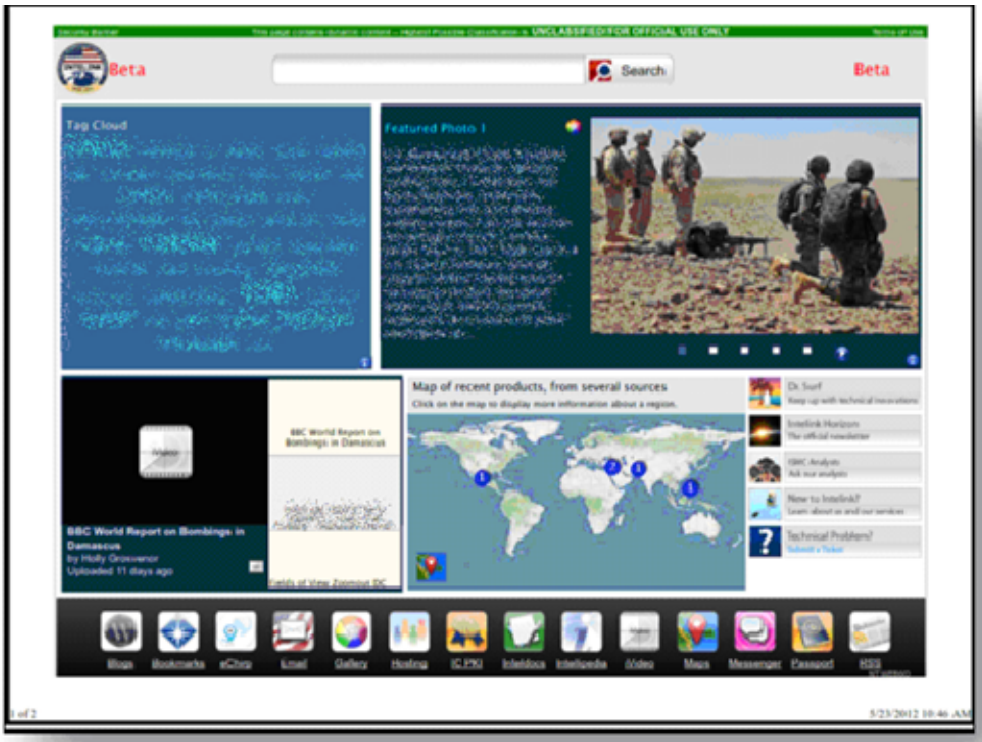

Figure 11. Intelink Beta Portal

From the overview, a number of Web 2.0 tools are accessible including: blogs, bookmarks, eChirp, email, gallery, Inteldocs, Intellipedia, video, maps, messenger, and an RSS aggregator. Each application appears to have been separately developed and has its own distinct appearance and identity.

Based on the commercially available Wordpress web software, blogs appear to be a popular tool within Intelink. A brief sampling of blogs showed five to ten or more posts a day, not including responses to the blog postings. Topics covered were often on Intelink itself but also covered the use of social media in intelligence, technological issues, and international incidents of social media usage. Users can add tags to their blogs to help users find areas of interest. Commonly used tags are displayed to the right of the blogs. Users can set up a profile within the Intelink blogs.

Bookmarks, also called Tagit, is a page that allows users to store book marks, tag pages, and manage previously stored items. It also allows users to view pages

that other users have bookmarked and tagged. Tagit provides listings of commonly used tags and recommendations for tags as shown in Figure 12. Users are even able to create RSS subscriptions based on tags of interest or even other users. Bookmarks can be created directly within the site, or by using a web browser bookmarklet that creates a bookmark from the current site.

Figure 12. Intelink Bookmark/Tagging

The application eChirp is the intelligence community's version of a micro-blogger similar in function to Twitter. It allows for a secure means of exchanging information between community members. Like Twitter, "chirps,"" or micro-blogs, can include a hashtag, which others can follow to track items of interest. For instance, if a user was to add a hashtag such as #CHDS, others interested in that topic could easily

search and track related posts. Chirps can be tracked using an RSS feed or through the eChirp page. Unlike Twitter, eChirp cannot be currently accessed through commercial devices such as tablets or smart phones.

Each user is provided 100MB of storage space in a section called Inteldocs. Inteldocs was created with Knowledge Tree, an open source product.[242] It provides a secure means to store, manage, and share secure documents within the Intelink system. Documents stored in Inteldocs may be findable within Intelink's search function. The default security setting allows access to all Intelink users, but the permission settings can easily be changed to restrict access.

Intellipedia is the intelligence community's wiki. Intellipedia was created using the same software as Wikipedia, Mediawiki. With an estimated 1.28 million pages and 188,467 contributors, Intellipedia is the most commonly used portion of Intelink.[243] Like any wiki, Intelink provides a platform for users to share and collaborate on various topics and issues that affect the larger community. The main page of Intellipedia, a wiki page itself, has areas for announcements, collaboration requests, breaking events, and new pages. Breaking events provides an example of integration with other Intelink tools. By adding a "#breaking" hashtag to an eChirp post, the "chirp" will appear on Intelink's main page in the breaking section. Code can also be added to wiki pages to appear in the breaking section of the main page Documents can be added to Intellipedia through the use of hyperlinks to the document's location, including ones stored in Inteldocs. As with the blog section of Intelink, users can set up a profile page that include personal biographical information. Information must be entered separately for each profile page. Intellipedia is often used for networking, intelligence product development, and the creation of organizational websites. By checking contributors to Intellipedia pages, users can easily identify other professionals with an interest in an area. [244]

---

[242] "Inteldocs," Intellipedia, https://www.leo.gov/https://www.intelink.gov/wiki/Inteldocs.

[243] *Intelink Basic Presentation*, 10.

[244] Dixon and McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*, 9.

Intelink Maps, powered by Google maps, will be familiar to users with experience using Google maps. In theory, Intelink maps provide the ability to visually search for intelligence information based on the topic or the sources geographical region. For example, the user can zoom into a geographical region and view intelligence documents generated in that region, or users can search for a topic and view documents based on the geographical location. The exact functionality of Intelink Maps could not be fully determined due to technical issues. At the time of this writing, searches could not be conducted.

Messenger allows for secure instant message/chat between Intelink users in all classification domains. Group chats are also possible with Messenger. Messenger was created with Jabber software, which uses XMPP, an open standard for instant messaging software. Unlike other elements of Intelink, Messenger does not operate within the browser and requires separate installation on a Windows desktop. Messenger cannot be run on any other operating systems.

The concepts behind email, the photo gallery, iVideo, and RSS aggregator are self-explanatory. The main difference between Intelink's versions and commercial versions is the higher level of security provided through Intelink's protected environment. The photo gallery and iVideo were not functioning at the time of this writing either due to user error or other technical difficulties. The RSS aggregator was in beta format and also had some functionality issues.

d. Current Usage/Application

Although usage statistics can be found for Intelink and some of its individual components, they may not provide a good indication of the extent of usage. In part, this is due to the wide variety of agencies and high number of individual users that potentially have access to Intelink. Another issue may be with the data itself. A 2009 CIA article stated that Intellipedia had over 100,000 government users and that over two million page edits had been made.[245] Today, the Intellipedia unclassified/FOUO statistics

[245] "Intellipedia Gurus Win 2009 Homeland Security Medal," Central Intelligence Agency, https://www.cia.gov/news-information/featured-story-archive/intellipedia-homeland-security-medal.html.

page shows that there are 59,051 registered users and 399 active users.[246] An active user is defined as one who has had activity in the past 30 days. While this may indicate a dropping off of the number of users since 2009, the statistics page currently shows that there has been a total of 1,171,557 page edits. The difference in reporting numbers is likely due to the levels of use within each security level of Intelink and Intellipedia. According to a 2010 article, the top secret portion of Intellipedia is the most active with more than 250,000 users and more than 74,000 contributors. The secret level had over 72,000 and the unclassified area had over 36,000.[247]

e. Security and Legal Concerns

Intelink-U operates on the DNI-U system. The DNI-U system is a secure internet accessible network that is used to connect intelligence agencies and various defense, law enforcement, homeland security and foreign relations activities. All data sent through DNI-U using commercial and public networks is encrypted.[248] Despite this, there are examples where agencies are not using Intelink due to security concerns. In a 2003 article on the CIA's website, an example was given that the CIA did not post some documents on Intelink due to the loss of control over dissemination once the documents were made available to the wider intelligence community. The CIA uses software called CIASource, which is linked to Intelink. Only those users that have been individually authorized via designated computers have access to data from within CIASource.[249] It is unclear if changes have been made since that time to address the CIA's concerns, but it is unlikely that any change would be made without a dramatic cultural shift in the handling of information and intelligence.

There may be less need to address physical security with Intelink as was needed with CopBook. Management in the process of evaluating software will likely look

---

246 "Statistics – Intellipedia," https://www.intelink.gov/wiki/Special:Statistics.

247 Miller, *Intellipedia Provides Lessons for FedSpace Initiative.*

248 "DNI-Unclassified," Intellipedia, https://www.leo.gov/https://www.intelink.gov/wiki/DNI-U#Briefings_on_Intelink-U_.2F_DNI-U.

249 Bruce Berkowitz, "Failing to Keep Up with the Information Revolution," *Studies in Intelligence* 47, no. 1 (2003).

less harshly on federally operated computer and software systems than they would with privately owned and hosted ones. Suffice to say, Intelink data centers have all the security measures one would expect of an intelligence system. These measures include: video surveillance, motion sensors, biometric access and exit sensors, on premises security, and other security protection.[250] The primary concerns with these systems are not for the possibility of systems being physically compromised, but for hacking and unauthorized use of software. The network security of Intelink is beyond the scope of this paper and this researcher's hope of understanding.

f. Future

Intelink is actively being improved upon. As mentioned earlier, a beta page is being developed to improve user access to items of importance. Other tools that are being considered and developed include the ability to mash-up data, the addition of geo-spacial capabilities, and the addition of widgets.[251]

A more significant issue facing Intelink is the advent of similar software across government domains. In the public arena, users are bombarded with options. It is not uncommon for a person to have a Facebook page, LinkedIn page, Google+ page, and Twitter account. The same situation is arising in the intelligence community. In addition to the secure systems already being used and developed by individual agencies, additional software is coming online. Govloop.gov and Fedspace.gov are just two examples of software that is overlapping with many areas that are in common with Intelink. While there are significant differences between the software applications, users may choose to limit their participation to one software platform.

As the use of Intelink and similar products become more common, the information being captured will become increasingly valuable. With the improvement of data mining techniques, software will be able to analyze a user's contributions to create a profile of the user's interest and expertise. Following in the steps of search engines such

---

[250] Randy C. Marks, "Intelink: The Intelligence Community's Classified Internet" Digital Government Society of North America, 2000).

[251] Miller, *Intellipedia Provides Lessons for FedSpace Initiative.*

as Google, searches may be narrowed to areas of importance to the user, saving time and money needed to sort through irrelevant data and helping to reduce information overload.[252]

C. ANALYSIS

1. Redlands Police Department

RPD should be recognized for having the vision for not only integrating social media into internal police operations, but also for looking beyond internal and external information sharing, to eventually include members of the community. Although Facebook and other social media platforms are being used to improve community relations, the RPD is taking this concept another step further. RPD plans to integrate the community into its problem solving and information networks to improve collaboration needed to address crime and the underlying issues that cause it.

RPD CopBook currently does not include a wiki for the capture of information. Information is captured primarily through the use of discussion groups, and documents. A subspace was created for a drug cartel. While this is allows for discussion and the sharing of documents on the cartel, it does not allow for the collation and organization of information, and collaboration that would be possible with the creation of a wiki. Though documents stored in the space can be edited and discussions can take place, documents do not provide the ease of editing and collaboration of a wiki. Each document must be downloaded, edited, and reuploaded. Each added step increases the complexity of making changes, and reducing the likelihood of participation. The current setup is more appropriate for discussing current and rapidly changing information but is less suitable as a long-term knowledge repository.

There are indications that new information silos are being created as traditional structures attempt find their place in a new system. Nearly all groups, including the ones for the police explorers and volunteers group are locked, therefore allowing only users preapproved by the group managers to access the information. While this may be

[252] Matthew S. Burton, "How the Web can Relieve our Information Glut and Get Us Talking to Each Other," *Studies in Intelligence* 49, no. 2 (2005), 60.

necessary for some areas dealing with particularly sensitive information, the overall effect will be that collaboration will continue to be limited through what amounts to a recreation of the hierarchical structure of traditional communication methods and systems.[253] Key elements of Enterprise 2.0 include trust and openness. Without these elements, information will continue to be sequestered thereby preventing the benefits that come from wide sharing and collaboration. These silos are undoubtedly created in the name of security and other concerns. However, it is incumbent on group managers to consider the risk of controlled, but broadened, information sharing, and to also consider the risk of *not* sharing. Though the cost of not doing something may be difficult to quantify, there are still costs involved. These costs are shown by increased inefficiencies, lost opportunities, reduced networking, and increased risk to officers that may have benefited from the sharing of particular information.

The structure for RPD CopBook is designed around documents, users, and groups rather than crime. Documents are put in one location, discussions in another, and crime bulletins are stored with training items. Organizational alignment of information with crime reduction efforts may be more appealing to officers who seek out tactical advantages to address crime issues.

A challenge that CopBook faces is a lack of integration with other RPD systems. CopBook runs parallel with current RPD systems. For officers already inundated with information from email, a variety of online sources of information, and criminal records systems, an additional source for information and opportunities for collaboration is less likely to be widely accepted, regardless of the potential value.

One level of integration that is being seen is in the area of document management. All training bulletins are being posted within CopBook. These include briefings on various police topics, as well as training announcements. Given the high level of interest in training, this integration with CopBook as opposed to using a separate document management system, should increase user traffic to the site thereby increasing user

[253] Mergel, *The Use of Social Media to Dissolve Knowledge Silos in Government*, 177, 179.

familiarity and encouraging further use. For widespread adoption of CopBook, further integration in addition to and beyond document management with current digital storage systems would help with user adoption.

Using private companies for the storing of sensitive data is always a concern. While many IT professionals seem to abhor off-site hosting of sensitive data, there is no indication that these systems are any less secure than internally hosted ones. RPD officials are comfortable with this hosting arrangement and have not experienced any problems as a result of it.

Extensive and regular use of CopBook for criminal information sharing and collaboration has yet to be fully realized. This may be in part due to lingering concerns over federal regulations guiding information and intelligence systems. The RPD is studying the application of these regulations to the CopBook system. It is apparent that concerns over the application of laws to ESSPs are impeding adoption of these ESSPs for use involving criminal intelligence.

Some minor human-computer interface issues still need further work. The company that created CopBook intends for it to be used by multiple police departments. The RPD is a group within the overall CopBook structure. This results in two selection areas in the top portion of the web page. One is a group of tabs and links for CopBook, the other for the RPD group. Depending on the selection made, clicking on the CopBook group may take the user outside of the RPD group. Then, selecting the “home” tab takes the user to the CopBook website rather than the RPD group. Some tools on the CopBook selection area are repeated in the RPD area. While redundancies sometimes can improve the ease of use, in this case it may result in confusion for some users. A single home page for RPD that is outside of the business side of the CopBook framework would be more streamlined and reduce confusion.

The language used to describe the user groupings within CopBook is not always clear. The terms group, sub-group, social group, and place can be confusing. The hierarchy used to organize these groups does not appear to be consistent with some “groups” at the group level, while other comparable groups are at the sub-group or social

group user. This may be clarified with training, but for a user without training, the structure clouds understanding of the site's organization and may make it more difficult to locate needed information or to connect with the right personnel.

The Redlands Police Department remains the leader in social media innovation in policing. The model being developed by RPD and CopBook currently sets the standard for departments across the United States. Though no one system will be suitable for all police agencies, RPD provides a solid starting point that should be considered by any police agencies working to implement ESSPs. Future efforts to expand its use will keep other agencies trying to catch up for years to come.

2. Intelink

Intelink is the gold standard for the use of Web 2.0 tools in an intelligence environment. Its use is changing the way the intelligence community views intelligence. A primary lesson learned is that changes to culture as dramatic as those necessarily involved with ESSPs take years to implement. Even with the success of Intelink, full implementation as a regular part of intelligence community processes will be an ongoing effort.

Many elements of Intelink are neither user friendly nor well-integrated. There are different methods to access Intelink including through other online portals, such as Law Enforcement Online (LEO.gov) and Open Source Center (Opensource.gov). To access Intelink directly, each computer used to access the system must be individually approved. However, accessing it through a portal allows access from additional computers. The use of a "passport" allows a different level of access. This researcher was not able to identify documents outlining the different methods of access and varying functionality based on the access method. For instance, a user can post a blog or an update to Intellipedia, if accessing Intelink through one of the other systems but cannot add a tag to an Intellipedia page. This may be due to ongoing development of the Intelink system, but exact reasons for the differences in functionality are not clear. What is clear is that the logon disparities complicate usage of Intelink and may decrease the adoption of the system by users frustrated with the complexities of simply accessing the system.

Intelink has been described as resembling "more of an oligarchy of agencies than a community of individuals with shared interests."[254] Rather than individuals working together across agency boundaries to create a common product, individual agencies are using Intelink as a means of disseminating their product. Agency logos are used to identify products under the pseudonym of "anonymous" rather than giving credit to individual writers. While in the intelligence field, some degree of anonymity may be necessary, the effect is that opportunities are being lost for analyst to connect with other analyst and agencies that may share areas of interest and knowledge, which could improve each other's intelligence products. Depersonalization of input into blogs, wikis and other social media by the use of agency branding, as opposed to individual attributions, results in fewer social connections being made, and lesser degrees of overall interaction.[255]

By impacting existing traditional information flows and the cultural power structures based on information control, Intelink has proven to be a tremendously disruptive technology.[256] The more Intelink is integrated with traditional practices, the more it impacts each of these areas. A criticism of Intelink and Intellipedia in particular, is that agencies are avoiding some of these effects by using it as a parallel system.[257] Intelligence agencies continue to maintain their own systems, even ones that heavily overlap with the functionality provided by Intelink. Other agencies are developing similar systems to ensure their own control over the system. Giving up control of information to other agencies, some with competing goals, is not in the nature of intelligence analysts and managers. Any duplication of effort, as would be required with parallel systems, can only result in resistance to using the secondary system. This duplication results in managers and analysts struggling to balance time spent contributing to Intellipedia with

---

[254] Burton, *How the Web Can Relieve our Information Glut and Get Us Talking to Each Other*, 55, 56.

[255] Ibid., 56.

[256] Dixon and McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency.*

[257] Joab Jackson, "Intellipedia Suffers Midlife Crisis -- Government Computer News " http://gcn.com/Articles/2009/02/18/Intellipedia.aspx.

time spent supporting competing systems and on traditional tasks. Some users are still debating whether Intellipedia contributes to or distracts from product development. [258] As long as agencies restrict its use to the dissemination of completed products, the full potential of Intellipedia as a collaborative system will not be reached.

As with CopBook, Intelink suffers from a lack of integration with other internal systems. In the case of Intelink, internal systems are the various Web 2.0 tools that make up the Intelink ESSP. The integration of tags and RSS feeds as part of the various functional areas is limited. Currently, Intelink requires manual creation of code allowing for RSS feeds from Intellipedia pages of interest. Each Web 2.0 tool has the feel of individually produced software. Integration between the different tools appears to be improving, but further development is needed so that movement between the tools is seamless with thorough interconnectedness.

Intelink is not accessible from mobile devices and smart phones. For office work, this may be sufficient. However, tools such as eChirp have very little value within an office environment. Twitter's ease of use for mobile users was one of the driving factors in its success. Don Burke, one of the co-founders of Intellipedia, was quoted as saying, "When you develop functions, it has to be mobile, in two years if you aren't mobile, you will be dead."[259] Security concerns may prevent mobilization of Intelink though it will be at the cost of lost contributions from mobile users.

Intelink is rapidly adapting to the needs of users and advances in technology. Intelink officials are working on many, if not all, of the issues identified. Intelink has established itself as an essential tool in the intelligence community. While Intelink is designed with the needs of the intelligence users in mind, police officials can learn from its designs and implementation. Intelink makes it abundantly clear that ESSPs can be used for intelligence and criminal information sharing and collaboration. The demand for Intelink as demonstrated by its success is a clear indicator of the need for a similar tool for police agencies to assist in crime reduction efforts.

---

[258] Dixon and McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency.*

[259] Miller, *Intellipedia Provides Lessons for FedSpace Initiative.*

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. RECOMMENDATIONS AND CONCLUSIONS

A. RECOMMENDATIONS

First and foremost, a department considering the use of an ESSP should not proceed without a full understanding of its potential impact on culture. Leaders should be willing to replace hierarchical communication patterns with highly interlinked networks of communication. No software will change these communication patters, only police leadership with the support of all personnel can do this. An adoption of an ESSP without the willingness to embrace true social media would be an ineffective use of resources. Ideally, this shift in culture, if not already in place, would be adopted before the ESSP investment is made.

The organization of the ESSP should be left to the users with only a skeleton to begin with. By lending control to the users and allowing them to address their communication needs, adoption will be more likely. As users find ways for the system to meet their needs, they will bring in more users. However, this should be done within the aforementioned open and networked culture. Simply recreating traditional information silos within a new system will not aid in full collaboration to address needs. The default setting should be for open access. Limited membership and access should be very limited and an exception to the norm.

The human-computer interface should be a top consideration when developing an ESSP. Part of the vast success of the Apple iPad was that “it just works.” This mindset should be kept in mind with an ESSP as well. Simple and clear user interfaces are especially important in the conservative environment of policing that includes many late adopters and laggards. If a new officer cannot set down at the new system and make sense of it, further design is needed. Though formal training will always offer benefits, first consider the training that Facebook, Twitter, and Google provided public users. If you are having trouble remembering, it is because training was not provided. Users helping users is the best instruction that can be given.

Crime reduction efforts are typically centered on a crime triangle that includes offenders, locations, and victims/targets. Patrol officer assignments are based on division, area, and shift. [260] As police agency's design or adopt their own ESSP, organization of information and resources should be based on how officers and detectives act to reduce crime. Rather than a breakdown based on administrative sorting of information, information should be broken down by this crime triangle and assignments. This would not be all together different from the RPD approach. Rather than have a "people" page for users, there would be a records page for suspects. Rather than a places page for groups, there would be a page for high crime areas and criminal targets. In addition, information between different areas should be linked whether by hyperlinks or tags. A suspect tied to a high crime area should have clear links between the different pages. Tags provide one method of doing this. Finally, there should be a page where an officer can quickly view all the activity related to their beat, shift, division, and department.[261] In short, the design should be based on the thinking and needs of officers and detectives. This isn't to say that there isn't a benefit in user or groups pages, but only that the design should be mission focused.

The development of an ESSP must be done with considerations of how it fits into current and planned information sharing systems. It cannot be set up as an independent system and still expect to see any level of success. Two levels of integration are needed with an ESSP. The first is internal. If the incremental approach is taken, as was the case with Intelink, the individual components should be tightly integrated with each other as they are implemented. Different human-computer interfaces for each WEB 2.0 component increases the learning curve for users. A lack of integration between the different components can reduce effectiveness and increase complexity by requiring users to go to each component individually to access information or by making it difficult to link information between the components. The added burden on users will negatively affect adoption.

---

[260] Tim Read, Nick Tilley, and Great Britain, Home Office, Policing and Reducing Crime Unit, *Not Rocket Science?: Problem-Solving and Crime Reduction* (London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, 2000), 38.

[261] These divisions vary by department. A beat and squad are geographical areas of responsibility.

The second level of integration needed is with other internal information systems. Rather than require the creation of a new user identification and password, the logon process should be integrated with currently existing ones. Basic user information within the ESSP should be populated from personnel databases. Privacy concerns of personnel can be addressed through the ability to limit the information being shared with other users. In addition, other digital information sources should be integrated as well. For those agencies that already have an intranet, the ESSP should eventually replace all the information sources within it. Criminal records management systems should be included in this integration. A suspect's record could emulate the biography pages within Wikipedia.[262] Though this may involve a higher level of software design, it is an achievable goal. The possibilities for integration are numerous. Map data could be linked to an officer's beat pages; dispatch histories could be linked to location pages. A goal in establishing an ESSP is for it to become *the* information source, not simply an additional one to add to the heap.

As they should, privacy and law remain a concern in this new environment. This research has focused on an internal agency level for the main purpose of ensuring a strong base for inter-agency spread information sharing. However, another reason for this focus is that federal regulations on the handling of criminal information and intelligence do not apply to states or municipality information system that is used for internal information sharing. An internal focus avoids many of the regulation concerns that come with broader information sharing. 29 CFR part 23 does not apply to criminal records information systems (CRIS) in any case. An ESSP should be viewed in much the same way as an advanced CRIS. By commonly accepted definitions, information is not intelligence until it has been analyzed. The emergent properties of an ESSP may require further consideration and research into what constitutes analysis, but for now, information sharing and collaboration should not be confused with analysis. For those cases in which law enforcement intelligence is shared within an ESSP, the same controls that are currently used should be applied within the ESSP.

[262] Wikipedia, http://en.wikipedia.org/wiki/Tim_Berners_Lee.

Finally, new ESSPs should be designed with mobility in mind. The RPD recognized this in advance and ensured that CopBook was accessible from any device or computer. Mobile applications further increase the usability of CopBook. This is essential for information and collaboration systems designed for a mobile employee. Systems designed for office-based employees may have some success without this mobility, but systems designed for a patrol officer will not.

B. CONCLUSIONS

The key to understanding Web 2.0 and ESSPs is that they are not about technology but about establishing a cultural environment that facilitates communication, collaboration, and information sharing. Another important element is the need for integration of data from different sources. Multiple databases and other information sources along with multiple logons and passwords only inhibit the free flow of information. The current status of formal information capture is hampering the sharing of information and collaborative efforts. While there is a need for formalities in official reports, there is also a strong need to find new ways to share and communicate information. Not only will the new information created within an ESSP be a valuable resource for investigations and problem solving. It will also provide a future source for data mining that will help us to better understand both employee and criminal processes and patterns

ESSPs can be viewed as a knowledge management and knowledge creation system. The primary point of adopting ESSPs is to increase the abundance and actionability of information. As a result, knowledge will also increase. An ESSP framework will allow for more efficient access to information and help the user to filter the information that is needed. In effect, the adoption of an ESSP is a major step towards creating a platform for living information and intelligence.

The implementation of an ESSP must not be viewed simply as the installation of a new tool. ESSPs are part of a larger system under the umbrella of Enterprise 2.0. When used to empower employees and reduce barriers to communication, it is the potential of revolutionizing an organization. The broader impact on an organization’s culture must be

considered when developing a plan for implementation. In addition to planning for the long haul, leaders must also plan for the bumps along the road, so they do not become barricades to progress. It is my belief that Enterprise 2.0 is here for the long term. The actions of police leaders are not needed for the eventual adoption of ESSPs but are necessary to ensure their timely adoption in a manner that brings success to the agency sooner than later.

Changing the culture of police agencies is another key factor in the successful implementation of an ESSP. Police leaders must recognize that no system based on the needs of the user can thrive without trust. Substantive increases in production are heavily reliant on establishing an environment where trust is a key value. In police culture, trust is not typically emphasized as a core value. Trust is a luxury most officers cannot afford when dealing with a significant percentage of people they interact with everyday. However, it is important to distinguish this from trust shared within the organization. In an open system, the CEO's trust in employees is essential for success.[263] Distrust within an organization will only impeded progress and create obstacles to the successful adoption of new innovations.[264]

Social media and ESSPs are breaking new ground in the areas of law, privacy, and security. To say the least, much has changed since 28 CFR Part 23 was adopted in 1993. Further clarification and changes to federal regulations will be needed to address the complex adaptive systems that are social media. However, none of these considerations are an excuse to avoid innovation. A-Space, Intelink, Redland Police Department's CopBook, and others are moving forward in this complex environment. Their successes should be our stepping-stones to future innovations.

Implementation is another way of saying "managing change." Managing this change depends more on addressing difficult organizational and cultural challenges than

---

[263] Brafman and Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, 67.

[264] Adrienne Werner, "The Potential Transformative Impact of Web 2.0 Technology on the Intelligence Community" (Homeland Security Studies, Naval Postgraduate School); Stephen M. R. Covey and Rebecca R. Merrill, *The Speed of Trust: The One Thing That Changes Everything* (New York: Free Press, 2008). Werner, 34.

it does purchasing new software or other technology. [265] The implementation of any ESSP has to be viewed as a long-term project with patience and persistence being key values. Wikipedia and Intellipedia, both now widely considered examples of success, took many years of active work before being fully embraced. Within a conservative police environment with entrenched cultures, no change of importance will take place overnight, or even in a single year. The implementation of an ESSP, as with any disruptive technology, will involve detours and setbacks. These should not be viewed as failures but only as steps toward success.[266]

It takes hard work and vision for an agency to innovate, but the potential reward is incalculable, especially in the context of the policing mission. Failing to innovate in policing, even to avoid risks, is an acceptance of the status quo. The tired mantra that we must find ways to do more with less has run its course. However, we must find ways to do more, with carefully considered changes to our communication hierarchy and through improved means of information sharing and collaboration. The post-9/11 emphasis on inter-agency information sharing and collaboration does little good if the same practices are not being applied within an agency.

It is past time for policing leaders to equip their personnel with the same tools that the general public has been benefiting from for a few years now. Just as police departments across the country adopted higher capacity and higher caliber weapons to better prepare officers against criminals who were already using the same weapons, police departments today must adopt tools for collaboration that are already being used by criminals including terrorist. Weapons are infrequently used in policing. Communication in its varying forms is used continuously. If a new gun can improve

---

[265] Tony Byrne, "Enterprise Social Software Technology," KMWorld, http://www.kmworld.com/Articles/Editorial/Feature/Enterprise-social-Software-technology--50453.aspx.

[266] Rodrigo Nieto-Gómez, "The Power of the Few: A Key Strategic Challenge for the Permanently Disrupted High-Tech Homeland Security Environment," *Homeland Security Affairs* 7, no. 18 (December 2011, 2011); Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail.*

police safety and effectiveness, a new paradigm-shifting communications tool has the potential to revolutionize policing and vastly improve the safety of the communities in which officers serve.

C. FUTURE RESEARCH

Motivated employees are a key to success for any organization. To ensure success, there is a need for incentive systems in enterprise social media.[267] The move away from standard measurements of success, such as arrests and citations, in policing has left a void for goal-oriented officers. Crime statistics are too broad of a measurement to be used alone. Police agencies and other government organizations are unable to provide financial rewards. Gamification has been suggested as a way to develop a reward system in a work environment. Gamification is defined as the application of game theory concepts and techniques to nongame activities.[268] The goal of gamification is to encourage desired behaviors through positive recognition given in a way the user finds entertaining—reward systems. Participants earn points or badges for participation or accomplishing certain tasks. The rewards are viewable by other players to encourage competition.[269] In an ESSP, badges could be earned for a certain number of blog posts, or for creating a group. Research into this area may help determine how game theory and gamification can be used to encourage behaviors and establish a reward system as part of successful ESSP.

Using big data analytics to determine patterns in crime and criminal behavior is another area ripe for study. Policing is building on the principles of CompStat, as it moves into the areas of intelligence led policing and predictive policing. Each of these is a method of dealing with the vast amounts of data currently available to police. Predictive policing is a result of big data analysis. As police agencies and other organizations

---

[267] Alavi and Leidner, *Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues*, 107–136, 126.

[268] "What is Gamification?" WhatIs.com, http://searchcloudapplications.techtarget.com/definition/gamification.

[269] Christina Torode, "Gamification Key to Launching New FedEx Social Collaboration Platform" (Monday, 13 August 2012).

develop improved methods for the analysis of big data, the term “big data” will eventually revert to the term “data.” In the meantime, the concept of “big data” should serve as a reminder of the need for police agencies to expand the use of data in determining the allocation of resources. With the public’s blessing, data should be taken from every available resource from weather data to census data, and beyond. Research into the implications and uses of big data to improve efficiency, productivity, transparency, and accountability will help guide the future of policing.

BIBLIOGRAPHY

"28CFR FAQ," accessed 4/23/2012, 2012, http://www.iir.com/28CFR_Program/~/Home/28CFR_Program/28CFR_FAQ/#q6.

Alavi, Maryan, and Dorothy E. Leidner. "Knowledge Management Systems: Issues, Challenges, and Benefits." *Communications of the AI*S 1, no. 2es (1999): 1.

———. "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues." *MIS Quarterl*y 25, no. 1 (2001): 107–136.

Andrus, D. Calvin. "Toward a Complex Adaptive Intelligence Community — Central Intelligence Agency " , accessed 9/29/2011. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Wik_and_ Blog_7.htm.

Arney, Margaret Brad Cohen, and Brad Medairy. "Impact of Advanced Collaborative Architectures on Intelligence Analysis," 2004.

Berg, Oscar. *Why Traditional Intranets Fail Today's Knowledge Workers*. The Content Economy. New York: Basic Books, 2010.

Berkowitz, Bruce. "Failing to Keep Up with the Information Revolution," *Studies in Intelligenc*e 47, no. 1 (2003).

Betts-Lacroix, Joe. "Hype Chasm," *Evocato*r (Wednesday, 7 April 2010).

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Portfolio, 2006.

Brynjolfsson, Erik, and Adam Saunders. *Wired for Innovation: How Information Technology is Reshaping the Economy*. Cambridge, Mass.: MIT Press, 2010.

Bughin, Jaques Michael Chui, and James Manyika. "Clouds, Big Data, and Smart Assets: Ten Tech-Enabled Business Trends to Watch." *McKinsey Quarterl*y 56, (2010).

Burton, Matthew S. "How the Web can Relieve our Information Glut and Get Us Talking to Each Other." *Studies in Intelligenc*e 49, no. 2 (2005): 55.

Byrne, Tony. "Enterprise Social Software Technology." KMWorld, accessed 5/7/2012, 2012, http://www.kmworld.com/Articles/Editorial/Feature/Enterprise-social-Software-technology--50453.aspx.

Carter, Dave L. "The Law Enforcement Intelligence Function." *FBI Law Enforcement Bulleti*n 74, no. 6 (2005): 1.

Carter, David L., and United States. Dept. of Justice. Office of Community Oriented Policing Services. “Law Enforcement Intelligence a Guide for State, Local, and Tribal Law Enforcement Agencies.” U.S. Dept. of Justice, Office of Community Oriented Policing Services.

Chau, Michael, Daniel Zeng, Homa Atabakhsh, and Hsinchun Chen. “Building an Infrastructure for Law Enforcement Information Sharing and Collaboration: Design Issues and Challenges.”

Chavez, T. Dave., Michael R. Pendleton, and Jim Bueerman. “Knowledge Management in Policing.” U.S. Dept. of Justice, Office of Community Oriented Policing Services.

Chen, Hsinchun, Daniel Zeng, Homa Atabakhsh, Wojciech Wyzga, and Jenny Schroeder. “COPLINK: Managing Law Enforcement Data and Knowledge.” *Communications- AC*M 46, (2003): 28–34.

Christensen, Clayton M. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fai*l. Boston, Mass.: Harvard Business School Press, 1997.

Chui, Michael, Andy Miller, and Roger P. Roberts. “Six Ways to make Web 2.0 Work.” *The McKinsey Quarterly*. no. 2 (2009): 64–75.

Cohen, Sara Estes, and Shala Ann Byers. “Look before You Leap: Security Considerations in a Web 2.0 World.” *IA Newslette*r 13, no. 2 (2010): 20.

Collier, Paul M. “Policing and the Intelligent Application of Knowledge.” *Public Money & Managemen*t 26, no. 2 (April 2006): 109–116.

Covey, Stephen M. R., and Rebecca R. Merrill. *The Speed of Trust: The One Thing that Changes Everythin*g. New York: Free Press, 2008.

Cummings, Jeff, Anne P. Massey, and V. Ramesh. “Proceedings of the 27th ACM International Conference on Design of Communication - SIGDOC '09; Web 2.0 Proclivity” 2009.

Criminal Intelligence File Guidelines. U.S. Dept. of Justice, Office of Justice Programs. Washington, DC: U.S. Dept. of Justice, Office of Justice Programs, 2002.

*Criminal Intelligence: Concepts and Issues Pape*r. 2003rd ed. Alexandria, VA: IACP National Law Enforcement Policy Center, 1998.

Davenport, Thomas H., Paul Barth, and Randy Bean. “How ‘Big Data’ is Different,” *MIT Sloan Management Revie*w (Monday, 30 July 2012).

Davenport, Thomas H., and Laurence Prusak. *Working Knowledge: How Organizations Manage what they Know*. Boston, Mass: Harvard Business School Press, 1998.

Department of Homeland Security, and United States. Congress. *Homeland Security Act of 2002*. Washington, D.C.: The Department, 2002.

"DNI-Unclassified." Intellipedia, accessed 5/27/2012, 2012, https://www.leo.gov/https://www.intelink.gov/wiki/DNI-U#Briefings_on_Intelink-U_.2F_DNI-U.

DiGiammarino, Frank, and Lena Trudeau. "Virtual Networks: An Opportunity for Government." *The Public Manage*r (Spring 2008): 5.

Dixon, Nancy M., and Laura A. McNamar*a. Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agenc*y: DIA Knowledge Laboratory, 2008.

Drapeau, Mark, and Linton Wells. "Social Software and National Security an Initial Net Assessment." Center for Technology and National Security Policy, National Defense University, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497525.

Dumbill, Edd. *Big Data Now Current Perspectives from O'Reilly Radar*. [S.l.]: O' Reilly Media, 2011.

"First Facebook, Now there's 'CopBook.'" LawOfficer.com, accessed 5/17/2012, http://www.lawofficer.com/article/news/first-facebook-now-theres-copb.

Fogarty, Kevin. "Big Data Plus Police Work: Good Partners?" Information Week, accessed 8/19/2012, http://www.informationweek.com/software/business-intelligence/big-data-plus-police-work-good-partners/240004290.

*Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Er*a. Washington, D.C.: Dept. of Justice, Office of Justice Programs, Bureau of Justice Assistance, 2006.

Gaudin, Sharon. "THE GRILL: Andrew McAfee." *Computerworld* 44, no. 7 (April 5, 2010, 12–14.

Geels, Frank W. "The Dynamics of Transitions in Socio-Technical Systems: A Multi-Level Analysis of the Transition Pathway from Horse-Drawn Carriages to Automobiles (1860–1930)." *Technology Analysis & Strategic Managemen*t 17, no. 4 (12, 2005): 445–476.

Gottlieb, Steven, Sheldon Arenberg, and Raj Singh. "Crime Analysis: From First Report to Final Arrest." *No.: ISBN 0-9634773-0-*7 (1994): 616.

Hardy, Quentin. "How Big Data Gets Real." NYTimes.com, accessed 8/17/2012, 2012, http://bits.blogs.nytimes.com/2012/06/04/how-big-data-gets-real/.

Hauck, Roslin Viprakasit. “Should they Share Or Not? an Investigation on the use of Communication and Knowledge Sharing Technology in a Police Organization.”The University of Arizona, 2005.

Hinchcliffe, Dion. “Why all the Fuss about Web 2.0.” Jan/Feb (2010).

“Information Sharing Environment-(ISE)-Suspicious Activity Reporting (SAR)--Evaluation Environment (EE) Segment Architecture.” Office of the Program Manager for the Information Sharing Environment.

Institute for Intergovernmental Research. “28CFR FAQ “ , accessed 5/6/2012, 2012, https://www.iir.com/Home/28CFR_Program/28CFR_FAQ/.

“Inteldocs.” Intellipedia, accessed 5/28/2012, 2012, https://www.leo.gov/https://www.intelink.gov/wiki/Inteldocs.

“Intelink Basic Presentation.” Intelligence Community Chief Information Officer, accessed 5/27/2012, 2012, http://www.ndia.org/Divisions/Divisions/C4ISR/Documents/Breakfast Presentations/2010 Presentations/Intelink Basic presentation.pdf.

*Intelligence-Led Policing: The New Intelligence Architectur*e. Washington, DC: Bureau of Justice Assistance, 2005.

“Intellipedia Gurus Win 2009 Homeland Security Medal.” Central Intelligence Agency, accessed 5/28/2012, 2012, https://www.cia.gov/news-information/featured-story-archive/intellipedia-homeland-security-medal.html.

Jackson, Joab. “Intellipedia Suffers Midlife Crisis -- Government Computer News “ , accessed 9/16/2011, http://gcn.com/Articles/2009/02/18/Intellipedia.aspx.

Janz, Brian D., and Pattarawan Prasarnphanich. “Understanding the Antecedents of Effective Knowledge Management: The Importance of a Knowledge-Centered Culture.” *Decision Science*s 34, no. 2 (2003): 351–384.

Kaplan, Andreas M., and Michael Haenlein. “Users of the World, Unite! the Challenges and Opportunities of Social Media.” *Business Horizon*s 53, no. 1 (2, 2010): 59–68.

*Knowledge Transfer Through Peopl*e. United States Strategic Command Knowledge Transfer Office, 2009b.

“Knowledge.” Dictionary.com, accessed 3/25/2012, 2012, http://dictionary.reference.com/browse/knowledge?s=t.

Kumaraswamy, Kowta Sita Nirmala, and Chitale C.M. “Collaborative Knowledge Sharing Strategy to Enhance Organizational Learning.” *J.Manage.Dev.Journal of Management Developmen*t 31, no. 3 (2012): 308–322.

Lee, Maria R., and Yi-Chen Lan. “From Web 2.0 to Conversational Knowledge Management: Towards Collaborative Intelligence.” *Journal of Entrepreneurship Researc*h 2, no. 2 (2007): 47–62.

Lehaney, Brian, Steve Clark, Elayne Coakes, and Gillian Jack. *Beyond Knowledge Managemen*t. Hershey, PA: Idea Group Pub., an imprint of Idea Group, 2004.

Lohr, Steve. “The Age of Big Data.” *New York Times* 11, (02/11/12).

Macmillan, Paul, Andrew Medd, and Peter Hughes. “Change Your World Or the World Will Change You” Deloitte, accessed 9/29/2011, 2011, http://www.deloitte.com/view/en_EC/ec/792ebd7690794210VgnVCM100000ba42f00aRCRD.htm.

Manyika, James Michael Chui, Brad Brown, Jaques Bughin, Richard Dobbs, Charles Roxburgh, and Anglea H. Byers. “Big Data: The Next Frontier for Innovation, Competition and Productivity.” *McKinsey Global Institute, May* (2011).

Marks, Randy C. “Intelink: The Intelligence Community's Classified Internet.”Digital Government Society of North America, 2000.

McAfee, Andrew. *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges* Harvard Business School Press, 2009.

———. “Enterprise 2.0: The Dawn of Emergent Collaboration.” *Engineering Management Review, IEEE* 34, no. 3 (2006): 38.

———. “Shattering the Myths about Enterprise 2.0.”*Harvard Business Review* 87, no. 11 (2009).

McNamara, T. E. “Information Sharing Environment Implementation Plan.” *US Information Sharing Environment* 1, (2006): 2010.

Meadows, Donella H., *Thinking in Systems: A Primer*. White River Junction, Vermont: Chelsea Green Publ., 2010.

Mergel, Ines. “The use of Social Media to Dissolve Knowledge Silos in Government.” In *The Future of Public Administration, Public Management, and Public Service Around the World.*, edited by O'Leary, R., Kim S., and D. VanSlyke, 177, 2011.

Miller, Jason. “Intellipedia Provides Lessons for FedSpace Initiative.” FederalNewsRadio.com, accessed 5/23/2012, http://www.federalnewsradio.com/?nid=697&sid=1949950.

Mitchell, Melanie. “Complexity a Guided Tour.” Oxford University Press.

Moore, Geoffrey A.,. *Crossing the Chasm: Marketing and Selling Disruptive Products to Mainstream Customer*s. New York, NY: Harper Business Essentials, 2002.

Murugesan, San. “Understanding Web 2.0.” *IT Professiona*l 9, no. 4 (2007): 34.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: Norton, 2004.

*National Criminal Intelligence Sharing Pla*n. U.S. Department of Justice, 2005.

National Security Strategy. Washington: White House, 2010.

Nieto-Gómez, Rodrigo. “The Power of the Few”: A Key Strategic Challenge for the Permanently Disrupted High-Tech Homeland Security Environment.” *Homeland Securitiy Affair*s 7, no. 18 (December 2011).

Nissen, Mark E. *Harnessing Knowledge Dynamics: Principled Organizational Knowing & Learnin*g. Hershey PA: IRM Press, 2006.

“NYPD and Microsoft Create a Next Generation Law Enforcement Big Data Solution.” accessed 8/20/2012, 2012, http://ctovision.com/2012/08/nypd-and-microsoft-create-a-next-generation-law-enforcement-big-data-solution/.

Olesker, Alex. “Big Data Solutions for Law Enforcement.” CTO Labs, accessed 8/19/12, http://ctolabs.com/wp-content/uploads/2012/06/120627HadoopForLawEnforcement.pdf.

O'Reilly, Tim. “What is Web 2.0?” O'Reilly Media, accessed 09/30/2011, 2011.

Peterson, Marilyn B. *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, DC: Bureau of Justice Assistance, 2005.

Randol, Mark A., and Library of Congress. Congressional Research Service. “Homeland Security Intelligence Perceptions, Statutory Definitions and Approaches.” Congressional Research Service.

Ratcliffe, Jerry H. “The Structure of Strategic Thinking.” *Strategic Thinking in Criminal Intelligenc*e (2004): 1–10.

Ratcliffe, Jerry H., and Police Foundation. “Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders.” *No.: ISBN 1-884614-21-*3 (2007): 50.

Ratcliffe, Jerry. “What is Intelligence-Led Policing?,” accessed 5/10/2012, http://jratcliffe.net/research/ilp.htm.

Read, Tim, Nick Tilley, and Great Britain. Home Office. Policing and Reducing Crime Unit. *Not Rocket Science?: Problem-Solving and Crime Reductio*n. London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, 2000.

Redman, Thomas C. *Data Driven: Profiting from Your most Important Business Asse*t. Boston, Mass.: Harvard Business Press, 2008.

Robertson, Maxine, Jacky Swan, and Sue Newell. “The Role of Networks in the Diffusion of Technological Innovation*.” *Journal of Management Studie*s 33, no. 3 (1996): 333–359.

*The Social Enterprise: Using Social Enterprise Applications to Enable the Next Wave of Knowledge Worker Productivit*y. Oracle White Paper. Oracle, 2008.

Starbird, Kate, Leysia Palen, Amanda L. Hughes, and Sarah Vieweg. “Chatter on the Red: What Hazards Threat Reveals about the Social Life of Microblogged Information.”ACM}, 2010.

Stenmark, Dick. “Web 2.0 in the Business Environment: The New Intranet or a Passing Hype?” 2008.

“Social Networking Takes Flight at NASA.” accessed 12/24/2011, 2011, http://www.ciozone.com/index.php/Case-Studies/Social-Networking-Takes-Flight-at-NASA.html.

“Statistics – Intellipedia.” accessed 5/28/2012, 2012, https://www.intelink.gov/wiki/Special:Statistics.

Taniguchi, Travis A. *Using Social Business Software (SBS) to Enhance Public/Private Partnerships: A Collaborative Approach to Community Knowledge Minin*g. BJA Solicitation: “Encouraging Innovation: Field-Initiated Programs FY 2011 Competitive Grant Announcment” Grants.Gov #BJA-2011-2946., edited by Jim Bueerman, 2011.

Tapscott, Don, and Anthony D. Williams. *Wikinomics: How Mass Collaboration Changes Everythin*g. New York, NY [u.a.]: Portfolio/Penguin, 2010.

Taylor, Bruce, Rachel Boba, and Jeff Egge. *Integration of Crime Analysis into Patrol Work: A Guideboo*k U.S. DOJ: COPS, 2011.

Torode, Christina. “Gamification Key to Launching New FedEx Social Collaboration Platform” (Monday, 13 August 2012).

United States. Office of Justice Programs. *The National Criminal Intelligence Sharing Plan: Solutions and Approaches for a Cohesive Plan to Improve our Nation's Ability to Share Criminal Intelligence*. [Washington, D.C.]: Office of Justice Programs, U.S. Dept. of Justice, 2003.

United States. White House Office. "National Strategy for Information Sharing Successes and Challenges in Improving Terrorism-Related Information Sharing." White House.

van Zyl, Anria Sophia. "The Impact of Social Networking 2.0 on Organizations." *Electronic Library, th*e 27, no. 6 (2009): 906.

Werner, Adrienne. "The Potential Transformative Impact of Web 2.0 Technology on the Intelligence Community." Homeland Security Studies, Naval Postgraduate School, 2008.

"What is Gamification?" WhatIs.com, accessed 8/20/2012, http://searchcloudapplications.techtarget.com/definition/gamification.

Whitworth, Brian. "Socio-Technical Systems." *Encyclopedia of Human Computer Interactio*n (2006): 533–541. doi:10/30/2006.

Wikipedia contributors. "Intellipedia." Wikipedia, accessed 09/29/2011, en.wikipedia.org/wiki/Intellipedia.

Yu, Dan and Chang Chieh Hang. "A Reflective Review of Disruptive Innovation Theory." *International Journal of Management Review*s 12, no. 4 (2010): 435–452.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California