SENSITIVE BUT UNCLASSIFIED:
EXAMINING THE USE OF ELECTRONIC INFORMATION SHARING SYSTEMS BY LAW ENFORCEMENT AGENCIES IN THE UNITED STATES

By

Jack Drew

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Criminal Justice — Doctor of Philosophy

2015

ABSTRACT

SENSITIVE BUT UNCLASSIFIED:
EXAMINING THE USE OF ELECTRONIC INFORMATION SHARING SYSTEMS
BY LAW ENFORCEMENT AGENCIES IN THE UNITED STATES

By

Jack Drew

The Information Sharing Environment is a nationwide initiative intended to support public safety in the post-9/11 era. Within its architecture, electronic communications systems enable law enforcement agencies across government to share Sensitive But Unclassified information that can prevent or mitigate threats to citizens and critical infrastructure. However, few scholars have studied these systems. This study synthesized interdisciplinary research to identify what factors influence agency use of electronic information sharing systems, and to explore the linkage between system use and flows of law enforcement intelligence. A survey methodology was used to collect data from two samples of law enforcement personnel attending intelligence trainings. Of 335 responses from individuals who were employed at 147 local, county, or state agencies in the United States, quantitative analyses centered on 45 agencies to investigate the use of five federal networks.

The findings highlight extensive use of sharing systems by small and large agencies, with those at the state level appearing to be most active. Regular access to these systems does not necessarily result in more frequent exchanges of intelligence products. Technical-rational and institutional factors do not appear to explain variation in system use. The discussion presents possible interpretations of these findings along with their implications for policymakers, agency leaders, and sharing system administrators. Among these are the adequacy of self-learning as a source of systems training and the role of system champions at lower levels of authority. One

limitation of the study is the sensitivity of law enforcement intelligence practices and the willingness of law enforcement to report on them. For theoretical and methodological reasons, future researchers may consider a different study design to explore the contextual use of law enforcement systems for sharing information and intelligence.

ACKNOWLEDGEMENTS

Completion of this report has only been possible with the support of others. I wish to humbly express my gratitude to committee members who have provided valuable feedback at times when they undoubtedly had other pressing commitments. Dr. Steve Chermak, Dr. David Carter, Dr. Jeremy Wilson, and Dr. Dan Bronstein have all worked to help me produce a better piece of research. Thank you.

Dr. Chermak influenced my thinking from the very first semester when he taught "CJ904 Criminal Justice Organizations and Processes." At a time when I was struggling to adjust to the pace of the doctoral program, his class helped me to connect with our discipline. Indeed, this research owes much to the string-to-the-wall exercise he used as a call for more criminal justice theory, class discussions of contingency, resource dependency, and institutional perspectives, and his openness to viewing concepts from different vantage points. As a dissertation chairperson he remained patient with my progress (which must have seemed glacial at times) and he constantly exuded positivity. When I expressed doubts, his response was always emphatic: you can do this! He encouraged me to keep moving forward while also gently reminding me that it's a privilege to learn in a college setting — a message, I am ashamed to admit, I sometimes forgot.

Several members of the School's faculty have also contributed to my professional and personal development. In particular, Dr. Christina DeJong served as a teaching mentor and advised me throughout my graduate studies. Instructors for the Homeland Security program — Dr. Phil Schertzing, Dr. Robyn Mace, and Professor Rad Jones — persuasively argued the need to explore this area of growing research. Critically, Dr. Ed McGarrell made it possible for me to work with Dr. Chermak and Dr. Carter on a national study of law enforcement intelligence

practices sponsored by the National Institute of Justice. This in turn led to an opportunity to work on the START project.

Dr. Jeremy Carter also worked on the START project and was unstinting in his support and advice for carrying both the project and my research through to completion. Dr. Nick Corsaro and Dawn Chang shared separate, but equally helpful methodological insights. Dr. Andrew Dawson provided feedback and urged me recalibrate my views about the research process ("We aspire to build the Taj Mahal but it's probably more realistic to think we will, at best, produce a few clay bricks"). Dr. Mara Ranville proofread different drafts.

University rules have the capacity to bewilder, but Melissa Christle guided me through the official procedures during my final candidacy. I appreciated her calm manner and quick responses as deadlines loomed.

To colleagues in the program, friends, and relatives who asked about my work and offered support, thank you. Even brief inquiries about my progress and well-being meant a lot.

Last, but by no means least, I want to acknowledge my wife. Mary has been unwavering in her support throughout my time in the program and repeatedly said, "You will get through this." She never got cross when I chose to study instead of spending time with her and she provided many useful suggestions at critical junctures. Put simply, her generosity of spirit has made it possible for me to share this work. I love you!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1: Introduction

In the aftermath of the attacks that took place on September 11, 2001, legislators and government officials took steps to deter, prevent, and mitigate against future terrorist attacks. These efforts have reformed the way government workers, in conjunction with the private sector, share information so that it is clear who has this information, how to ask for it and how to share details. In particular, a key recommendation of the National Commission on Terrorist Attacks Upon the United States called for the president to "coordinate the resolution of the legal, policy, and technical issues across agencies to create a 'trusted information network' " (*The 9/11 Commission Report*, 2004, p.418). The network that has subsequently arisen is the Information Sharing Environment and its architecture enables law enforcement workers to exchange information in a timely and responsible manner, and as a result respond to natural and man-made threats. Nevertheless, there have only been a handful of empirical studies that examine how law enforcement agencies share information. Scholars have asked practitioners about sharing behaviors but there remains a need to understand how sharing takes place, especially with respect to networked information sharing systems and the factors that shape the decision to adopt these technologies.

This study seeks to fill this gap with a systematic examination of law enforcement workers' use of online systems to access and share information they suspect has a criminal nexus or represents noncriminal threats to public safety. Previous research has asked if there are too many systems, whether they are interoperable, and if workers have access to them. The intent here is to understand what these systems contribute to law enforcement intelligence and to develop an explanation for the variation in their use.

Background

On any given day officials must contend with a variety of threats to public safety. Extreme weather patterns and attacks involving shootings, bombings, the use of chemical, biological, nuclear, and radiological weapons of mass destruction, aircraft hijackings, and cyber warfare can cause mass disruptions and harm to people and their property (*Creating a Trusted Network*, 2003). Prevention and mitigation against these threats involves officials gathering information that facilitates agile and proactive decision-making (Duecy, 2006; Louie & Von Eckartsberg, 2006; *National Strategy for Information Sharing and Safeguarding*, 2012). However, since no single organization is likely to have enough information to produce a complete assessment for emerging threats, it is vital that representatives from different organizations are able to share information so analyses include a wide range of sources and efficient allocations of limited resources are possible (Baird & Barksdale, 2006; Burke, 2009; Carter, 2009; Valledor, 2010).

The Information Sharing Environment (ISE) transcends local, state, and federal levels of government by integrating information streams from the intelligence, foreign affairs, defense, homeland security, and law enforcement communities (*Information Sharing Environment Implementation Plan*, 2006; *Information Sharing Environment: Definition of the Results*, 2008). In the case of the law enforcement community, the entrance points to the ISE are electronic information sharing systems that are accessible via the Internet to sworn officers, as well as nonsworn specialists, with the authority to use them. These systems support multidirectional flows of Sensitive But Unclassified information[1] between state, local, and tribal law enforcement

[1] Sensitive But Unclassified information refers to critical information that does not meet standards for classification and does not require officers to hold a security clearance in order to access it. However, in the absence of national guidelines, agencies have previously developed

(SLTLE) agencies, emergency operations centers, major urban area, state, or regional intelligence fusion centers, federal agencies, and the private sector (*Information Sharing Environment Implementation Plan*, 2006).

Promotion of a partnership between these various stakeholders implies a shared responsibility for protecting communities and raising awareness about threats (Davis et al., 2004; *Implementing 9/11 Commission Recommendations*, 2011). Nevertheless, SLTLE officers are especially well positioned to collect, act on, and relay information about suspects and crimes (*The 9/11 Commission Report*, 2004; Carter, 2009; *Creating a Trusted Network*, 2003; Ericson & Haggerty, 1997; GIWG, 2003). Two arguments support this view. First, as of September 2008, there were approximately 120,000 full-time law enforcement officers with arrest powers employed by federal agencies (Reaves, 2012). In contrast, the number of full-time, sworn personnel working for state and local law enforcement agencies was 765,000 (Reaves, 2011a), more than six times the number of their federal counterparts. Second, exposure to new information occurs when officers investigate citizen complaints, attend crime scenes, interview witnesses, perform traffic stops, speak with community leaders, and handle reports (Graphia-Joyal, 2012; Henry, 2002). These activities, coupled with a trained eye for unusual situations and suspicious individuals that stand out in familiar territory (Graphia-Joyal, 2012), result in officers gathering information to identify and manage risks (Ericson & Haggerty, 1997).

In short, SLTLE officers make a vital contribution to the ISE and electronic information sharing systems, in the form of web portals and other software facilitating the communication and management of distributed data, provide the technical means to engage these frontline

---

their own rules for identifying and protecting Sensitive But Unclassified information. At the time of writing and in line with steps to standardize treatment of this information, a designation of Controlled Unclassified Information (CUI) is being phased in to replace the Sensitive But Unclassified label (Carter, 2009; *Memorandum*, 2008).

workers (Akbulut-Bailey, 2011; *Creating a Trusted Network*, 2003). However, the architecture and guidelines that support the ISE have taken time to develop and obstacles to effective information sharing remain.

The Information Sharing Environment. During the past twelve years there have been many initiatives designed to improve information sharing across and between all levels of government, foreign allies and the private sector, but at each stage there has been support for electronic sharing systems. For instance, The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 was the first legislation designed to expand the power of law enforcement agencies with respect to counterterrorism; in particular, Title VII Section 401 called for the creation and operation of "secure information sharing systems to enhance the investigation and prosecution abilities of participating enforcement agencies in addressing multijurisdictional terrorist conspiracies and activities." Likewise, the Homeland Security Act of 2002 required sharing systems to facilitate information exchange between and across federal, state, and local governments; Section 1001 also required protection of "information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" through the provision of data integrity, confidentiality, availability, and user authentication.

In early 2002, law enforcement representatives from all levels of government convened at the International Association of Chiefs of Police Criminal Intelligence Sharing Summit and agreed to work towards a national intelligence plan by creating the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG). After consultations with state, local, and tribal law enforcement workers, this group released the National Criminal Intelligence Sharing Plan in 2003. The 28 recommendations outlined in the Plan serve as minimum standards

to guide law enforcement agencies with the development of an intelligence function and active participation in national information sharing efforts. To this end, Recommendation 21 called for the creation of a "nationwide sensitive but unclassified communications backbone [that] shall support fully functional, bidirectional information sharing capabilities that maximize the reuse of existing local, state, tribal, regional, and federal infrastructure investments" (GIWG, 2003, p.19).

A year later Congress passed further legislation that mandated the establishment of the ISE. Section 1016(b)(1)(A) of the Intelligence Reform and Terrorism Prevention Act of 2004 stated the President shall "create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties," along with an organizational plan and rules to manage it. The Act also specified functional characteristics the ISE should have in order to facilitate information sharing, again reiterating the need to connect existing information systems in a secure manner for the purposes of assisting ongoing analyses and investigations.

In 2006, the President directed the Director of National Intelligence to submit a report to Congress that included the Implementation Plan for the Information Sharing Environment. This document provided a description of the ISE's conceptual design, its capabilities and resources, a deployment plan and a method for assessing implementation progress and outcomes (*Information Sharing Environment: Background and Authorities*, n.d.). The three year, two-phase implementation plan aimed to establish trusted partnerships by building, and then incrementally extending, utilities and services to support multidirectional information sharing. A vital aspect of this development is a shift towards inclusion of terrorism and "all-crimes and all-hazards" information since the latter "may not initially be recognized as terrorism information,

but may be information that could ultimately prove crucial in preventing, preparing for, or responding to terrorism" (*Information Sharing Environment Implementation Plan*, 2006, p.11).

To continue the move towards effective interagency sharing and cooperation, the President's National Information Sharing Strategy (2007) provided descriptions of the roles and responsibilities of state, local, and tribal entities. The document also reaffirmed the importance of leveraging "existing technical capabilities" (p.3) to develop working partnerships across government and with the private sector and foreign allies, and it recognized successful initiatives: the creation of the National Counterterrorism Center; support for emerging state and major urban area fusion centers that serve as "primary focal points" (p.20) for terrorism-related information; continuing state and local government participation in federally led joint terrorism task forces; and U.S. Department of Homeland Security efforts to consolidate various information sharing systems (*President's National Strategy on Information Sharing*, 2007). In 2012, the National Strategy for Information Sharing and Safeguarding added to this list the Nationwide Suspicious Activity Reporting Initiative, High Intensity Drug Trafficking Area program and Regional Information Sharing Systems centers. It also called for adoption of the National Information Exchange Model to enhance the interoperability of information sharing systems and discovery of information across different parts of government.

Obstacles to effective information sharing. Despite the intentions of legislators and supporters of the ISE, it does not follow that officers share knowledge with others and assessments of the efforts to increase information sharing tend to echo a similar finding: interagency sharing and cooperation have improved since 9/11 but further progress is necessary (Chermak, Carter, Carter, McGarrell, & Drew, 2013; Graphia-Joyal, 2012; *Homeland Security: Efforts to Improve Information Sharing*, 2003; *Implementing 9/11 Commission*

Recommendations, 2011; *Information Sharing: Progress Made and Challenges Remaining*, 2011). This is due to obstacles that impede effective information sharing and authorities must overcome in order to implement the ISE.

A key consideration is the fragmented organization of American policing. In line with Federalist ideals encapsulated in the United States Constitution, and the 10th Amendment in particular, the national and regional governments are responsible for different policing functions. States, counties, and municipalities exercise general police powers while the federal government is responsible for the maintenance of interstate commerce and protection of federal property. Local enforcement agencies therefore have limited authority and their personnel are held accountable to local stakeholders. This means the federal government cannot coerce SLTLE agencies to participate in the ISE (Henry, 2002); outside of federal government, information sharing is voluntary (GIWG, 2003) and a bottom-up approach prevails (Graphia-Joyal, 2012).

A decentralized structure essentially guards against overreach by individuals and groups in positions of authority. It also creates inefficiency (Foster, 2005). According to the 2008 Bureau of Justice Statistics' Census of State and Local Law Enforcement Agencies, in addition to the 50 primary state law enforcement agencies, there are 12,501 local police departments, 3,063 sheriff's offices, 1,733 special jurisdiction agencies, and 638 other agencies in the United States. Special jurisdiction agencies comprise tribal and campus police departments along with agencies responsible for the enforcement of environmental laws and the protection of natural resources including parks and recreation areas, and transportation-related jurisdictions such as mass transit systems, facilities at ports, bridge and tunnel structures. Other agencies cover small entities such as constable offices (Reaves, 2011a). Taken together, the sheer number of

independent, subfederal entities, each with separate identities, poses a serious challenge to the introduction of any new practice or policy (Crank & Langworthy, 1996; Hagan, 1989).

Fragmentation also impacts levels of meaningful cooperation. A sense of competition for limited resources and prestige promotes rivalries and the need to protect turf, especially at the federal level (White, 2004) where agencies are fewer but have national prominence and are subject to Congressional oversight, with the result that collaboration is diminished. Joint terrorism task forces illustrate the value of bringing workers from different agencies together (Casey, 2004; *Creating a Trusted Network*, 2003; Riley, Treverton, Wilson, & Davis, 2005), but there is also evidence to suggest local and federal friction about how information flows between them (Sheptycki, 2004). Fears that information could be misused and subsequently compromise ongoing criminal investigations persist (Brown, 2000; Graphia-Joyal, 2012). A countermeasure for building trust involves the use of security clearances to limit access to information on a need to know basis only, but delays surrounding individual background checks that precede the issue of clearances is another impediment (Carter, Chermak, McGarrell, Carter, & Drew, 2012; Henry, 2002; White, 2004).

The need to coordinate for the purposes of public safety extends beyond arrangements between law enforcement agencies to other parts of the criminal justice system and the private sector. Research suggests law enforcement agencies are sharing information with other entities across the justice system but, once again, there is scope to extend this activity (Carter et al., 2012; Hamm, 2007). Formal arrangements extending to nongovernmental entities tend to be unusual. Public-private partnerships are difficult to establish due to misunderstandings about the goals and capabilities of organizations from the other sector (Carter et al., 2012; *Enhancing the Law Enforcement Intelligence Capacity*, 2010; Graphia-Joyal, 2012) and they require a sustained

commitment from senior management (Carter, 2009; Jones, 2000). The fact that the National Infrastructure Protection Plan divides private industry into 17 categories with separate needs, combined with poorly coordinated requests (*Information Sharing Environment Implementation Plan*, 2006) and uncertainty about what level of commercial information should be shared with government (Carter, 2009) complicates relations.

Technology advances in computing power and storage provide the means for agency workers to develop their own structures for collecting, storing, and disseminating information (Chu, 2001; *Protecting America's Freedom in the Information Age*, 2002). Nevertheless, the introduction of computer technologies to support information sharing activities presents problems. First, investment in technology is a cost local agencies are responsible for (Carter et al., 2012), a nontrivial issue during a time of economic uncertainty when funding is limited and administrators face difficult budgetary choices, not least ones impacting the hiring and retention of personnel (Bhaskar & Zhang, 2007; Carter, 2009; Carter et al., 2012; Davis et al., 2010; Wilson & Heinonen, 2011). Development of an information systems infrastructure is expensive because funds must be found for systems security, maintenance, and upgrades after the initial purchases of equipment and software (Davis et al., 2010; Silverman, 2006). As systems age they take more effort to manage due to the integration of different vendor products and multiple databases with large amounts of information, and they require specialist knowledge to run (Duecy, 2006; *Protecting America's Freedom in the Information Age*, 2002). A failure to interconnect legacy systems is serious as the inability to transfer information within and beyond an agency renders them as silos (Sheptycki, 2004) and subverts the purpose of having information sharing systems in the first place.

Second, there is a risk police administrators will approach technological innovation as a remedy for overcoming problematic structures and processes (Ackroyd, Harper, Hughes, & Shapiro, 1992; Ratcliffe, 2008). In this situation a deterministic perspective presents technology as a cause of change and progress (Homburg, 2008), and it obscures the need to examine how an electronic information sharing system will fit with current practice (Wilson, 1989). Agencies vary by mission, stakeholders, workforce composition, technologies already in use, and perceptions of threats (Akbulut-Bailey, 2011; Davis et al., 2004) and it is important to determine whether workers have the necessary IT skills and direction from top management to utilize the new system (Akbulut-Bailey, 2011; Huysman & De Wit, 2002). Once implemented, evaluation of system performance is necessary (Silverman, 2006) and a lack of reliable metrics complicates the task of assessing an information technology's value (Manning, 2008).

Third, without careful planning and coordination of information collection, it is possible for front line officers to gather and submit overwhelming amounts of information (Brodeur & Dupont, 2006; Herman, 2001; Innes, Fielding, & Cope, 2005; Ratcliffe, 2008; Sheptycki, 2004). A sense of information overload causes officers to view information management activities, like entering data and verifying details, as too consuming to perform (Huysman & De Wit, 2002) and duplicate or erroneous information compromises analysts' efforts to produce timely and accurate intelligence products. Technology itself can assist with the detection of redundant information but searches take longer as the amount of stored information increases. Erroneous information erodes confidence in systems and leads workers to revert to interpersonal communication to acquire and share information (Brown & Brudney, 2003), and the use of paper systems (Ericson & Haggerty, 1997).

Fourth, with the introduction of a new technology comes uncertainty (Wilson, 1989). Resistance to this development is therefore a possibility, especially as information sharing conflicts with an occupational culture that protects information (*The 9/11 Commission Report*, 2004). This is mainly because of persistent fears that information could be misused and subsequently compromise ongoing criminal investigations (Brown, 2000; Graphia-Joyal, 2012), as well as careers (Manning, 2008). A safe option is simply to avoid divulging information with others. When officers do share information it is with individuals they trust. Informal networks of personal contacts develop with time and as professional opportunities arise, and they are not easily relinquished (Graphia-Joyal, 2012; Henry, 2002; Ratcliffe, 2008; Roberts & Roberts, 2007; Weiss, 1998). In essence, the move towards using electronic information sharing systems forces officers to rely upon formal networks and in so doing they lose control over information once they submit it the wider law enforcement community (Huysman & De Wit, 2002).

Fifth, many electronic information sharing systems remain operational in spite of calls to reduce or consolidate them. This creates uncertainty for officers at smaller departments who do not know what system to connect to while officers at larger agencies, and fusion centers specifically, must log into multiple systems to access new information (Dulin, 2009). The plethora of systems also complicates the provision of oversight and auditing, important tasks that reassure citizens only information with a criminal nexus is being stored and individual privacy rights are not being violated. 28 CFR Part 23 - Criminal Intelligence Systems Operating Policies are federal guidelines for SLTLE agencies collecting and storing noncriminal identifying information in criminal intelligence systems (Carter, 2009; Carter et al., 2012) and research indicates a high level of compliance among agencies (Carter et al., 2012). But unethical domestic intelligence practices in the past, especially during the 1950s and 1960s when agencies

kept dossiers on individuals due to their political activities, and lawsuits that followed in the 1970s and 1980s (Carter, 2009; Carter & Carter, 2009b), continue to highlight concerns about information management (Carter, 2009; Davis et al., 2004; Graphia-Joyal, 2012; Roberts, 2004). For this reason commentators highlight the importance of transparency within the ISE since trust between agencies, and the systems that connect them, sustains the information sharing mission (*Mobilizing Information to Prevent Terrorism*, 2006).

Statement of the Problem

Given these challenges, what factors shape the decision for SLTLE agencies to use electronic systems to collect and share information? Electronic information sharing systems are a vital component of the ISE because they support knowledge work and decision-making by bringing law enforcement officers together in a "central area, accessible anytime, anywhere" (Chu, 2000, p.35). In particular, they standardize information exchanges and support interorganizational collaboration (Davis et al., 2010; Yang & Maxwell, 2011) for the purposes of detecting serious crossjurisdictional threats to public safety (McGarrell, Freilich, & Chermak, 2007; Schlegel, 2000; Small & Taylor, 2006), in addition to emergency response planning (Davis et al., 2004).

However, previous research indicates there is variation in the implementation of these systems at the state and local level (Carter et al., 2012). A few studies identify the determinants of utilization within local law enforcement agencies (Akbulut, Kelle, Pawlowski, Schneider, & Looney, 2009; Akbulut-Bailey, 2011; Saviak, 2007; Skogan & Hartnett, 2005), but difference in theoretical underpinnings, sampling frames, times of data collection, and findings make it unclear what factors are most influential. If the goal of having every SLTLE agency participate in the ISE rings true (Carter, 2009), then there is still a need to understand the factors impacting

the uptake of a technology that enables agencies to transcend organizational boundaries (Dawes, Cresswell, & Pardo, 2009; Pardo, Gil-Garcia, & Burke, 2008) and build working partnerships within a decentralized system of law enforcement (McGarrell et al., 2007).

The shift of intelligence functions within government entities, and specifically fusion centers, away from a terrorism only focus toward "all crimes, all threats, all hazards" has been a significant development in counterterrorism. Chermak et al. (2013) state this trend is unsurprising as it ensures fusion centers operate efficiently by employing a flexible approach that supports national counterterrorism efforts while satisfying the needs of local stakeholders, recognizes the relationship between precursor crimes and terrorism threats, and reflects a growing interest in intelligence-led policing, an "inclusive development process" (Carter & Carter, 2009, p.316) that matches information gathering and analysis with agency goals, characteristics, and capabilities with jurisdictional needs.

Critics question whether this shift deviates from initial expectations for fusion centers for the purposes of securing funds for activities distinct from counterterrorism (Monahan & Palmer, 2009; Taylor & Russell, 2012). They also question whether the all-crimes, all-threats, all-hazards approach is sustainable since officers need to collect information for a wider array of threats (Taylor & Russell, 2012). Moreover, Davis et al. (2010) assert that a broader focus ultimately leads to a greater number of electronic information sharing systems that only store certain types of criminal or homeland security information. As a consequence, doubts remain about the capacity of electronic systems to yield information that is "more accurate, comprehensive, timely, and available on demand" (Brown & Brudney, 2003, p.32).

Purpose of the Research

The purpose of this study is to examine law enforcement agencies' use of electronic information sharing systems. In particular, the study addresses two questions:

1. Which technological, organizational, and environmental factors are most likely to influence agency use of sharing systems?
2. Is there an association between agencies' use of sharing systems and the exchange of law enforcement intelligence and information?

Data were collected from two groups of law enforcement personnel in order to fulfill the study goals. These groups had attended official trainings regarding intelligence practices and, along with an awareness of operational details and agency structures, they were thus well placed to provide information relevant to the current research. The data gathering technique was quantitative in nature and involved a self-administered questionnaire that study participants completed via a web-designed survey provider. The codified responses in turn facilitated tests of the proposed research framework, including validation or rejection of hypothesis statements about specified factors and their effect on the uptake of information sharing systems.

Research Contribution

This study adds to the body of interdisciplinary research explaining how information sharing across government helps to address public problems (Pardo et al., 2008). However, its focus on the use of electronic information sharing systems within law enforcement practice makes it unusual if not unique. It therefore has value because it updates previous knowledge about law enforcement's use of these electronic systems, it extends a theoretical framework for the purposes of explaining a law enforcement practice, and it addresses the issue of what an agency mission contributes to terrorism prevention and crime control.

Events surrounding 9/11 have had a significant effect upon police practices (Chermak et al., 2013) yet there is still a pressing need for empirical studies that clarify how law enforcement agencies are actively supporting the counterterrorism mission (Lum, Haberfeld, Fachner, & Lieberman, 2009). As such, academics will be interested in this study because it adds to the growing body of research on intelligence gathering in law enforcement, specifically through the application of theories relating to police organizational adaptation and the use of computer technologies. Policy makers may find this study useful when trying to understand what electronic information sharing systems contribute to the ISE; it may also guide assessments directed toward improvements of information systems and police databases in general. Senior managers at police agencies that have not yet accessed networks for sharing information may find it insightful when they seek to understand how agencies are already utilizing these electronic systems.

Organization of the Study

This study consists of five chapters. The purpose of this chapter was to establish the background of the study, its aims and significance. Chapter 2 builds on this foundation by focusing on empirical findings about law enforcement electronic information sharing systems. These findings are used, in conjunction with other research, to develop a testable model that explains law enforcement agencies' use of these systems. Chapter 3 presents the methodology for the study, and details the instrument design, process of participant selection, data collection, operationalization of concepts, and data analysis procedures. Chapter 4 reports the results of data analyses that address the research questions. Chapter 5 discusses the study findings and evaluates their significance, both in terms of theory and their implications for practice. The discussion also presents recommendations for further research and final conclusions about what

the findings contribute to our understanding of law enforcement electronic information sharing systems.

Chapter 2: Literature Review

This chapter presents scholarship relevant to the current study. It begins with a description of the search and inclusion criteria for sources. The review itself is broken into two sections: the first discusses police innovation and the second explores electronic systems used to share law enforcement information. The objective is to survey the current research and identify gaps this study will address (Denney & Tewksbury, 2013; Hart, 1998). More specifically, it highlights arguments and variables salient to agencies' use of electronic sharing systems.

Literature Search

Electronic searches of the ProQuest, Academic OneFile (InfoTrac), and Web of Science (Social Sciences Citation Index) academic databases, and Google Scholar, led to the discovery of relevant sources. Searches consisted of Boolean queries using combinations of the following key terms: law enforcement, police, justice, homeland security, government, interagency, information sharing, intelligence sharing, electronic, network, system, adoption, diffusion. Scrutiny of source references uncovered additional materials (Randolph, 2009); this step revealed title terms and keywords to use in new electronic searches.

The search yielded six empirical studies that specifically investigate law enforcement electronic information sharing. These include a conference paper (Lee & Rao, 2007), two dissertations (Akbulut, 2003; Saviak, 2007), and three peer-reviewed articles (Akbulut et al., 2009; Akbulut-Bailey, 2011; Skogan & Hartnett, 2005). All sources are written in English. The search also uncovered a body of research that is too large to fully address here. To advance the review, however, materials were included if they address the issue of organizational adaptation, police innovation, or police use of information technologies.

Understanding Police Innovation

Police agencies are constantly evolving their strategies and methods (King, 2000). Information management is a case in point. Since the introduction of computer-assisted systems of dispatching in the 1960s, police administrators have employed information systems to manage records, assign officers work, and evaluate performance (Manning, 1992). But the emergence of personal computers and networking has shifted officers' focus away from streamlining transactional work processes to the production of knowledge (Brown, 2000). The ability to rapidly transmit, store, retrieve, analyze, and display information from different sources now supports interagency collaboration (Chu, 2001) and underpins activities associated with generating all crimes, all threats, all hazards intelligence (Carter & Carter, 2009a).

Scholars have studied such developments through the theoretical lens of organizational innovation. The term innovation applies to many initiatives; it may refer to a plan, program, product, service, process technology, or work activity (Damanpour, 1991). However, Wolfe (1994) separates innovation studies into three categories, with each promoting a different research question, unit of analysis, and dependent variable. Diffusion of innovation studies center on patterns of adoption across time and/or space. With the use of survey and archival data, the objective is to reveal characteristics of an innovation that influence the rate of diffusion across a specific population. Process theory studies focus on the innovation process in order to explain how and why innovations are discovered, evolve, advance, and ultimately cease. This type of study therefore relies upon longitudinal research to capture the sequence of, and conditions for, distinct innovation stages. Innovativeness studies serve to identify organizational determinants for innovative behavior. This approach involves researchers adapting quantitative

measures from survey data to construct and test models that explain the extent of organizational innovation.

Police studies broadly conform to this classification. Weisburd et al. (2003) used survey data to yield self-reported measures of adoption and calculate diffusion rates of Compstat-like, management accountability programs among large agencies with 100 workers or more. Similarly, Weisburd and Lum (2005) used data from the Law Enforcement Management and Administrative Statistics (LEMAS) survey and the National Institute of Justice's Crime Mapping Research Center to establish a pattern of adoption of computerized crime mapping among a random sample of large police agencies. Both studies provide graphic illustrations of adoption distribution across time. Moreover, they present factors to explain differences in the adoption decision; a consistent theme is the extent to which an innovation represents significant organizational change and the role of agency mission as a trigger for adoption.

Process studies of police innovation are comparatively rare. Katz (2001) focused on the creation of a gang unit within a single agency and the reasons for this decision. A combination of in depth interviews with agency personnel, field observations, and a review of agency documents highlighted the influence exerted upon the agency by community stakeholders, or sovereigns. Organizational changes therefore stemmed from efforts to build relationships with community groups and maintain the institution's legitimacy. Korteland and Bekkers (2008) employed a case study methodology to reconstruct the diffusion and adoption process of a service delivery innovation, SMS-alert, among police agencies in the Netherlands. Analysis of data from documents and interviews with police personnel showed innovation diffusion often occurred when officers from different agencies met at events, such as site visits, to exchange knowledge and experience.

Police innovativeness studies address several developments within American agencies. These include the establishment of crime analysis units (Giblin, 2004, 2006) and practices associated with homeland security emergency preparedness (Burruss, Giblin, & Schafer, 2010; Giblin, Burruss, & Schafer, 2014; Haynes & Giblin, 2014; Schafer, Burruss, & Giblin, 2009), community policing (Burruss & Giblin, 2014; Schaefer Morabito, 2010), and intelligence-led policing (Carter, 2011). The foci here are the police organization as a unit of analysis and the implementation stage (Wolfe, 1994). Although exploratory studies may also use qualitative methods (Carter, 2011), data collection primarily involves cross-sectional survey responses from police sworn and nonsworn officers. Researchers numerically code these responses to investigate relationships between explanatory factors and organizational innovativeness. This dependent variable is usually an additive index of survey items that refers to the implementation of an innovation. Examples of explanatory variables include agency age, size in terms of the number of officers or residents served, funding, classification as an urban or rural jurisdiction, and proximity to metropolitan areas or other agencies (Carter, 2011).

Electronic Information Sharing Systems

Conceptualization. Differences in the conceptualization and definition of innovation have led to mixed research findings (King, 2000; Willis & Mastrofski, 2011). Some scholars have required an innovation to be new or "state-of-the-art" (King, 2000, p.305) while others suggest an innovation involves new tasks or existing tasks with "significant alteration" (Wilson, 1989, p.222). Mullen (1996) presents law enforcement computerization as a process that involves agencies modifying computer systems and applications that, in general, originate outside the field to meet their own needs. As such, the novelty is not the innovation per se but

rather the introduction of an existing product or process to fit a particular agency (Skogan & Frydl, 2004).

Researchers present sharing systems as new (Skogan & Hartnett, 2005) or improved (Lee & Rao, 2007) but they do not elaborate. An exception is Akbulut et al.'s (2009) distinction between information sharing, "[T]he volitional conveyance of information generated or obtained by one entity to another entity" (p.146) and electronic information sharing, "[I]nformation sharing that occurs via computing and communication technologies such as electronic mail, EDI, intranets, extranets, shared databases, etc." (p.147). They note electronic sharing streamlines information sharing because it makes communication more timely, accurate, and efficient.

The distinction between forms of information sharing is important because it presents the practice as multifaceted. Agencies may share information using nonelectronic means (e.g., face-to-face, via telephone or written report), electronic means that do not involve the use of a dedicated system (e.g., email), a government information sharing system, or a mixture of approaches (Akbulut et al., 2009). Moreover, it avoids the need to explain why one system supersedes older ones. This is difficult to determine for three reasons.

First, it is unclear how many law enforcement systems currently exist. A survey of law enforcement officials from 35 states identified 266 information sharing systems in use or in development, with 105 of these in operation at the state level and 42 at the federal level (*Information sharing systems*, 2006). Second, the use of law enforcement information systems is usually restricted to agency personnel who have applied for and been approved access rights, and publicly available information about these systems is limited. Third, whether a system is genuinely new, and thus adds to the number of available systems, or is instead reformed is not always clear. For instance, the Department of Homeland Security launched the Homeland

Security Information Network (HSIN) in February 2004, yet prior to then it was a pilot program known as the Joint Regional Information Exchange System (JRIES) between local and state law enforcement and the U.S. Department of Defense (Relyea & Seifert, 2005).

Nevertheless, it is necessary to revise this interpretation to highlight electronic sharing activities that enable information flows between SLTLE agencies and federal law enforcement, as well as the private sector. These activities include submitting queries to and receiving responses from databases at local, state, regional, and federal levels of government; pushing and pulling information about subjects or ongoing investigations from one agency to another; publishing information about individuals, investigations, events, and agency actions; and subscribing to receive notifications about individuals, investigations, and events (*Concept for operations*, 2003; Roberts, 2004).

Push-and-pull technologies enable agency officials to regulate what kinds of electronic information agencies receive (Rocheleau, 2006). For example, an agency may subscribe to a distribution list for certain types of information and an electronic system will automatically push notifications to registered recipients. This helps to control the amount of information agencies receive since a notification may only make reference to the existence of shared information, but a registered agency worker will need to log into the system to review the information itself. This approach also prevents sensitive details being automatically transmitted across an unsecured medium like email.

Consequently, electronic systems integrate Sensitive But Unclassified information and intelligence across governments. Information consists of pieces of "raw, unanalyzed data that identify persons, organizations, evidence, events or illustrates processes that indicate the

incidence of a criminal event or witnesses or evidence of a criminal event" (Carter, 2009, p.11)[2]. Examples of information include criminal records, tips, and suspicious activity reports. Intelligence is "the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature" (GIWG, 2003, p.27). Law enforcement intelligence outputs, or products, vary depending upon their intended audience but common examples include documents, alerts, bulletins, and threat or risk assessments (Carter, 2009).

In sum, an electronic information sharing system may be defined as a collection of digital, networked services that facilitates the sharing of information and intelligence between law enforcement agencies and relevant partners in a secure manner (Akbulut et al., 2009; Akbulut-Bailey, 2011; Carter, 2009; *Mobilizing Information to Prevent Terrorism*, 2006). As a policing innovation, implementation of a sharing system is likely to involve an assessment of what information officers need to collect, development of procedures for reporting data within the agency and with outside partners, and an adjustment in work tasks (Akbulut et al., 2009; Carter, 2009).

Exploration of systems adoption. In a nationwide investigation of law enforcement intelligence practices, Carter et al. (2012) presented the findings of a web-based survey administered to 2,025 SLTLE intelligence workers. In particular, they highlighted how many respondents indicated their agency were registered members of law enforcement systems built to support interagency information sharing. Of the 414 survey respondents, and in descending order, 82.5 percent said their agencies had access to the Federal Bureau of Investigation's Law Enforcement Online (LEO), 63.4 percent to the U.S. Department of Justice's Regional

[2] See Appendix A for listed definitions.

Information Sharing Systems Network (RISS.Net), 39.7 percent to HSIN, 20.6 percent to FBINET, and 15.0 percent to the Automated Trusted Information Exchange (ATIX). Although it does not include multivariate analyses, the study is important because it identifies and reports agency adoption of major sharing systems. As a benchmark against which to compare subsequent research results, the findings point out considerable variation in uptake among agencies. While LEO appears to have gained widespread acceptance, less than half of the respondents reported agency adoption for three of the systems.

Previous Research Models

In the first study of electronic information sharing by law enforcement agencies, Akbulut (2003) used responses from 136 local and county police departments in the state of Louisiana to test a predictive model comprised of technological, organizational, and environmental variables. The study results suggest five factors explain information sharing by local agencies: perceived risks for the agency due to inaccurate information, sharing complexity, material costs of participation, available technological resources and expertise, and external forms of encouragement or pressure.

Akbulut-Bailey (2011) subsequently conducted a secondary analysis of these data to extend this model to nine factors that explained 54.9 percent of variation in local agency participation in electronic information sharing. Technological factors included sharing benefits and sharing complexity; organizational factors included top management support, IT capability, financial resources, and agency size; and environmental factors included the level of trust between local and state agencies, the threat to program autonomy, and state exertion of power (Akbulut-Bailey, 2011).

These studies are important for two reasons. First, they demonstrate the value of the technology-organization-environment (TOE) framework (Tornatzky & Fleischer, 1990) for explaining technical innovation in a state-local electronic information sharing context. This is consistent across both studies despite the inclusion of different variables in the revised model. Secondly, the studies' findings mirror conclusions from research on interorganizational information sharing. Dawes (1996) found state workers' perceptions of the benefits and risks associated with the use of program information created in other government agencies are likely to shape agency expectations of, and willingness to participate in, future cooperative initiatives. Benefits of sharing include the ability to solve problems, build relationships, and discover new information; electronic technologies extend these benefits because digitized information is easy to duplicate, manipulate, and share (Chen et al., 2002). Risks consist of external demands for information leading to a drain of agency resources and restrictions on professional discretion stemming from misinterpretations of shared information (Dawes, 1996; Gil-Garcia, Schneider, Pardo, & Cresswell, 2005).

Similarly, the alignment of organizational mission, resources, and processes has considerable bearing on interagency sharing efforts (Yang & Maxwell, 2011). Here support from agency leaders is likely to prove decisive since information sharing involves communication of the need for the practice in relation to agency goals, setting roles, finding resources for equipment acquisition and staffing, and signaling the need for officers to actively participate (Gil-Garcia, Chengalur-Smith, & Duchessi, 2007; Yang & Maxwell, 2011). Conversely, an absence of commitment from the top of the organization serves to lower expectations among the rank-and-file and the failure to allocate adequate technical resources,

including training, represents a barrier to sharing with other organizations (Akbulut et al., 2009; Akbulut-Bailey, 2011; Yang & Maxwell, 2011).

However, the extent to which it is possible to generalize from Akbulut's research is questionable since it focused on electronic sharing between local and state agencies within a single state. It follows that the findings about external factors are strongly conditioned by respondents' relationship with state government, but the sampling frame does not permit comparisons between states. Moreover, the studies do not explicitly focus on law enforcement intelligence or systems that facilitate intelligence exchanges[3]. Akbulut's (2003) research predates information sharing tools currently available, as well as the emergence of fusion centers (Chermak et al., 2013). The ISE is a sharing context that extends beyond state law enforcement and includes other local law enforcement and government agencies, state attorneys and government agencies, state and regional intelligence fusion centers, and federal entities (Carter, 2009; Carter & Carter, 2009a; Carter et al., 2012; Chermak et al., 2013). We would therefore anticipate different environmental factors influencing the use of systems that convey Sensitive But Unclassified information and intelligence.

For example, Skogan and Hartnett's (2005) examination of partner agencies use of a centralized repository of criminal history information, the Chicago Police Department's Data Warehouse system, found agency managers' search of their external environment for ideas about police practices also influences technological innovation. A feature of the study was the decision to distinguish between system adoption and use because respondents may report their agencies have adopted an innovation, but agency personnel do not actually implement it (Chermak et al.,

[3] Akbulut (2003) conducted interviews with local and state highway safety officials as part of a case study examining the use of the Louisiana Uniform Motor Vehicle Crash Reporting System.

2013; Skogan & Hartnett, 2005). According to this view, inclusion of two dependent variables — one for adoption or innovativeness, and a second scale measure for utilization — facilitates an investigation of how deeply engrained an innovation is within agency practices.

With access to user records from the Data Warehouse itself, the authors therefore generated two separate multivariate models to distinguish between adoption and use. The first model highlighted officers' professional or cosmopolitan networks, officers with a college education, and agency experience of investigative databases as causal factors of system adoption. The second model indicated the number of officers per 10,000 residents and months of system experience, or early adoption, and explained system use. Based upon these results, Skogan and Hartnett (2005) concluded different set of factors explain technological innovation and use.

Saviak (2007) sought to re-evaluate these findings in his investigation of law enforcement information sharing networks by local agencies in three states. Survey responses from 384 local police executives in California, Georgia, and New York facilitated tests of eight explanatory variables and their relationship with separate measures of adoption and utilization. The research findings, while controlling for respondent experience, education, age, and agency budget, indicate leadership commitment and trialability were significant factors when explaining variance in agencies' adoption of information sharing networks. In contrast, relative advantage, complexity, and autonomy were significant determinants of agencies' network utilization. These results therefore lend support to the view that different variables explain the adoption and use of electronic information sharing systems. Likewise, they also suggest benefits associated with sharing systems influence their use but not adoption. It follows that the adoption decision rests less with technical-rational reasons and more with the agency leader's vision for the technology and the fit with agency priorities.

The study also included unanticipated results. For example, regression analyses indicated trialability had a negative, rather than a positive, effect on network adoption and thus agencies whose personnel had an opportunity to test information sharing networks prior to making an adoption decision were less likely to ultimately sign on. Likewise, system use was found to be negatively related to the retention of agency autonomy: respondents who believed their agency was not constrained by requirements and changes intended to promote information sharing were less likely to use sharing networks. Follow up interviews with study participants failed to provide reasons for these findings.

Overall, the current research on electronic information sharing by police agencies has generated mixed findings and it is difficult to conclude what factors best explain the agencies' adoption of sharing systems. Variation in the theoretical models driving the research, and concepts and their operationalization make the task of comparing variables across studies a challenge. This pattern suggests scholars' understanding of electronic systems use is incomplete. For instance, there is a notable absence of factors relating to law enforcement intelligence which raises three concerns. First, the lack of findings concerning actions to uphold civil rights protections in relation to sharing systems use is surprising and existing models fail to account for agencies' efforts to formalize intelligence activities. Second, researchers have yet to also explain how interactions with their external environment enable agencies to learn about the desirability and use of systems designed specifically to increase information exchanges across the ISE. Third, more generally but no less importantly, current studies do not explain how law enforcement intelligence products are linked to the use of these systems.

This study addresses these gaps by testing a theoretical framework that contains variables previously found to be important in police innovation, and additional constructs reflecting

structural and institutional aspects of police organizations. Consistent with literature that views policing and homeland security contexts as dynamic and subject to change (Burruss et al., 2010; Chermak et al., 2013), an underlying assumption is agencies' external environment shapes patterns of utilization with respect to a specific law enforcement technology designed to help minimize safety threats.

Theoretical Framework

A scientific theory is a statement that explains the relationships between observable phenomena (Stinchcombe, 1968). Theory is central to the research process because it shapes the questions being asked, the methods of data collection and analysis. Critically, a comparison of arguments with observations allows researchers to make an assessment of the theory and existing policies (Kraska, 2004). With this thought in mind, the current study uses the technology-organization-environment framework (Tornatzky & Fleischer, 1990), the diffusion of innovations theory (Rogers, 2003), and institutional theory (DiMaggio & Powell, 1983) to derive factors of law enforcement electronic information sharing systems' use. A brief description of each theory follows along with reasons for its inclusion.

Technology-Organization-Environment framework. As its name implies, the TOE framework considers three contexts that shape the process of technological innovation, and specifically implementation, within an organization. The technological context refers to characteristics of available technologies and the existing technological infrastructure. The organizational context represents structures and processes within an organization that enable or constrict the uptake of a technology. The environmental context refers to external forces impacting an organization and also forces it can shape (Tornatzky & Fleischer, 1990).

Scholars have used TOE as an organizational-level theory to examine the adoption of information systems in different work settings and countries (Parker & Castleman, 2007, 2009). For example, the subject of recent studies has been private organizations' adoption of knowledge management systems (Ryan & Prybutok, 2001), e-commerce (Ghobakhloo, Arias-Aranda, & Benitez-Amado, 2011; Lip-Sam & Hock-Eam, 2011; MacLennan & Van Belle, 2014; Sila, 2013; Sila & Dobni, 2012; Van Huy, Rowe, Truex, Robinson, & Huynh, 2012; Zhu, Kraemer, & Xu, 2003), supply chain management technologies (Chong & Ooi, 2008; Pan & Jang, 2008; Ramdani, Chevers, & Williams, 2013; Ramdani, Kawalek, & Lorenzo, 2009; Venkatesh & Bala, 2012), and cloud computing (Alshamaila, Papagiannidis, & Li, 2013; Low, Chen, & Wu, 2011; Tweel, 2012). Its theoretical relevance stems from the ability to add constructs from additional theories to the TOE context groups. This has resulted in consistent support for the framework, although specific factors vary depending on the study in question (Fichman, 1992; Oliveira & Martins, 2011).

Critically, the inclusion of factors relating to perceptions, policies, and practices presents technological innovation as a social process rather than simply the introduction of hardware (Orlikowski, 1992). Policing scholars also highlight the need to avoid explanations that treat technology as an instrument (Ackroyd et al., 1992; Chan, 2001; Ericson & Haggerty, 1997; Manning, 2001) and they urge consideration of "social organizational matters in which the technology has its place" (Ackroyd et al., 1992, p.10). In short, TOE facilitates such an investigation.

Diffusion of Innovations theory. Diffusions of innovations (DOI) theory explains the process by which an innovation, "[A]n idea, practice, or object that is perceived as new by an individual or other unit of adoption" (Rogers, 2003, p.12), is adopted and then used by

"interrelated units that are engaged in joint problem solving to accomplish a common goal" (p.23). It is a complex theory because it accounts for different categories of adopters, communication channels, and time in order to show how and why an innovation spreads and at what rate (Oliveira & Martins, 2011). DOI grew from an agricultural study in the 1950s and it has subsequently served as a framework for researchers working in sociological, medical, communications, and business fields; Rogers (2003) estimated there have been over 5,200 studies using DOI since he first published his theory forty years earlier.

Studies of technology benefit from DOI because it differentiates between the initial decision to adopt an innovation and its actual use, since it is possible to adopt but then ignore the innovation (Koch, 2005). Moreover, DOI highlights five attributes that are central to the decision to accept and employ an innovation: (1) its relative advantage compared to the innovation preceding it; (2) its compatibility with adopters' needs and values; (3) its complexity, or the extent to which organizational members perceive the innovation as difficult to understand and use; (4) its trialability, or the extent to which it is possible to experiment with the innovation on a limited basis; and (5) its observability, or the extent to which others can see the results of an innovation (Rogers, 2003).

Scholars also argue DOI is theoretically compatible with TOE (Oliveira & Martins, 2011; Tweel, 2012). Thus, studies have combined these theories (Chong & Ooi, 2008; Low et al., 2011; Tweel, 2012) to develop more robust theoretical explanations that combine a recognizable classification of technological characteristics with organizational and environmental factors influencing adoption (Oliveira & Martins, 2011). In the case of electronic information sharing systems, Saviak (2007) found DOI explains in part why agencies adopt these systems. This is consistent with the body of research based upon DOI that suggests how workers perceive an

innovation's characteristics shapes the decision to adopt and utilize it (Kapoor, Dwivedi, & Williams, 2014; Koch, 2005; Moore & Benbasat, 1991). DOI attributes are therefore important to consider in a technological context.

Institutional theory. Institutional theory suggests the shape organizations take and the tasks they perform owes more to the influence of external interests than rationalizations about effectiveness or efficiency (DiMaggio & Powell, 1983; Meyer & Rowan, 1977; Meyer & Scott, 1992; Scott, 2008). The term institutionalization refers to "the processes by which social processes, obligations, or actualities come to take on a rule like status in social thought and action" (Meyer & Rowan, 1977, p.341). Institutional rules therefore shape the level of support for organizations since they explain why organizations exist and what their purpose is (Meyer & Scott, 1992). In response, organizations gather information about social expectations, evaluate available options, and make decisions that are likely to meet with approval from external stakeholders (Liu, Ke, Wei, Gu, & Chen, 2009). Thus conformity, or institutional isomorphism, involves organizations integrating elements that reflect external criteria instead of internal assessments of efficiency, but a reliance on external institutions also provides stability during periods of uncertainty (Meyer & Rowan, 1977).

DiMaggio and Powell (1983) build upon this explanation by describing how three types of external pressures elicit responses from organizations. Coercive isomorphism stems from formal or informal pressures by which organizations compel other dependent organizations. Legal, financial, and technical requirements are examples of coercive pressures that "may be felt as force, as persuasion, or as invitations to join in collusion" (p.150). Imitative or mimetic isomorphism involves organizations modeling their activities upon other organizations that appear to have had success addressing similar problems. Modeling may occur indirectly as

workers move between organizations, or result from formal attempts to borrow practices. Normative isomorphism arises from collective expectations within an institutional context about what is appropriate organizational behavior. The ways in which professionals "define the conditions and methods of their work" (p.152) influences these expectations and individuals become aware of them through sources of training and as their careers progress.

Institutional theory has received a mixed reception from scholars. Critics argue the theory includes assumptions about institutional myths and citizens' propensity to accept them that are difficult to establish (Zucker, 1987). Additionally, a conceptual framework must be testable, more than a simple description, and it should avoid tautological reasoning (Manning, 2008; Zucker, 1987). The latter concern is problematic since it is difficult to determine whether public demands trigger organizational responses or vice versa (Crank, 2003). On the other hand, proponents maintain institutional theory has matured greatly (Scott, 2008) and broadened to consider issues such as agency and different organizational responses to external pressures (Oliver, 1991). Moreover, policing scholars see institutional theory as a promising avenue of inquiry and they state that, as public sector organizations, law enforcement agencies are strongly influenced by institutional values regarding how criminal justice agencies should handle crime (Burruss & Giblin, 2014; Crank, 2003; Crank & Langworthy, 1992, 1996; Giblin, 2006; Giblin & Burruss, 2009; King, 2014; Maguire & Uchida, 2000; Willis, Mastrofski, & Weisburd, 2007). "By looking and acting right" (Crank & Langworthy, 1996, p.215) agencies receive legitimacy and access to resources that support their mission (Suchman, 1995). Studies examining the creation of specialized gang units (Katz, 2001) and crime analysis units (Giblin, 2004, 2006) lend support to the view that agencies are responsive to external demands and seek opportunities to pursue initiatives designed to ensure public safety (McGarrell et al., 2007).

However, to enhance our understanding of police organizations further, Maguire and Uchida (2000) encourage scholars to consider theoretical modifications to institutional theory and they suggest this will involve "artful blending of existing theories" (p.538). In this respect researchers examining technology innovation have already taken steps to incorporate components of institutional theory, most notably DiMaggio and Powell's (1983) isomorphic mechanisms, as environmental variables (Liu et al., 2009; Pan, Nam, Ogara, & Lee, 2013; Rizzi, Ponte, & Bonifacio, 2009; Zhang & Dhaliwal, 2009; Zorn, Flanagin, & Shoham, 2011) and in a few cases they have combined TOE with institutional theory (Gibbs & Kraemer, 2004; Soares-Aguiar & Palma-dos-Reis, 2008; Tweel, 2012). This approach accounts for organizational attempts at minimizing the uncertainty arising from the introduction of a new technology (Pan et al., 2013) and external pressures exerted by competitors and business partners (Oliveira & Martins, 2011). This study also uses institutional theory to represent environmental variables since previous research indicates government agencies have different and conflicting motivations for contributing to information sharing efforts (Dawes, 1996), especially in a post-9/11 environment. For SLTLE agencies there is a tension between meaningful participation in the ISE and the benefits, such as legitimacy and potential access to funding grants, associated with this activity, versus the challenge of having the technical infrastructure to successfully gather information and distribute it electronically. It is therefore necessary to assess institutional pressures, or cultural and nontechnical pressures, surrounding the use of electronic information sharing systems.

Research Hypotheses

Tornatzky and Fleischer's (1990) TOE framework highlights the role of context in the innovation process. They present technological innovation as "the situationally new

development and introduction of knowledge-derived tools, artifacts, and devices by which people extend and interact with their environment" (p.11). They argue innovation is a complex process, in part because of underlying assumptions: cultural norms and values condition technology use, and characteristics of a technology may be physical and social. But in their view innovation helps to renew social systems, and context, while not determining the outcome of technological change, both facilitates and constrains this process.

The TOE framework has remained virtually unchanged since its conception. Baker (2012) attributes a lack of development to its adaptability with scholars' placing different factors within the TOE contextual categories to reflect the innovation being studied. Consequently, they have treated alternate explanations, such as Roger's (2003) diffusion of innovations theory, as compatible and encapsulated complementary ideas within the TOE framework (Baker, 2012; Chong & Ooi, 2008; MacLennan & Van Belle, 2014; Sila & Dobni, 2012).

The current research follows a similar approach to derive and test a theoretical model for explaining law enforcement agencies' use of electronic systems to share information and intelligence. In addition to those explanatory variables prior research indicates are important, the following model includes factors drawn from the policing literature that address law enforcement intelligence and homeland security activities.

Technological context. The technological context refers to characteristics of available technologies and the existing technological infrastructure (MacLennan & Van Belle, 2014; Tornatzky & Fleischer, 1990). In a law enforcement intelligence context available technologies include electronic systems that agencies use to capture, manage, and share information (Brewster et al., 2014). However, the number of system components and their configuration are likely to vary by agency. A single computer with an Internet connection is sufficient to access federal

network web portals, while subfederal entities running systems that other agencies connect to require hardware and software components configured to service data management operations for multiple users.

Irrespective of the exact implementation, the current infrastructure presents practical limits on the extent of innovation while available technologies show what organizational adaptation is possible (Baker, 2012; Collins, 2003; Rogers, 2003). To understand the influence of new technology on organizational adoption and usage, and their fit with current technology, scholars have identified salient characteristics. In particular, Rogers' (1983, 2003) diffusion of innovation theory has provided a starting point for understanding an organization's technological context (Hameed & Counsell, 2014). Central to the theory is the assumption that perceptions of innovation characteristics, rather than "attributes as classified objectively by experts or change agents" (p.223), facilitate such an investigation. This study focuses upon two technological characteristics: perceived benefits and perceived disadvantages.

According to Rogers (2003), an important consideration is an innovation's relative advantage, "[T]he degree to which an innovation is perceived as being better than the idea it supersedes" (p.229). Empirical findings consistently show relative advantage to be a significant predictor of adoption (Chwelos, Benbasat, & Dexter, 2001; Cragg & King, 1993; Hameed & Counsell, 2014; Iacovou, Benbasat, & Dexter, 1995; Premkumar & Ramamurthy, 1995; Tornatzky & Klein, 1982) where workers are able to identify benefits associated with an innovation (Chau & Tam, 1997; Rogers, 2003).

Perceived benefits here refer to the potential gains law enforcement agencies derive from using electronic information sharing systems (Akbulut, 2003). An overarching benefit is access to information that may originate outside an agency but supports its internal planning, decision-

making, and resource allocation. Access to this information also facilitates agency outreach and the development of professional relations (Akbulut, 2003; Akbulut et al., 2009; Akbulut-Bailey, 2011; Dawes, 1996). Participant trust in law enforcement electronic systems rests upon the fact they are designed to restrict views of Sensitive But Unclassified information to authorized individuals only.[4] It is therefore hypothesized that:

H1: Perceived benefits will have a positive influence upon agency use of law enforcement information sharing systems.

Any decision to accept or reject a new technology will depend on an evaluation of the potential drawbacks, as well as expected benefits, associated with its adoption (Lin, 2014; Rogers, 2003). Perceived disadvantages refer to the problems associated with law enforcement agencies' use of electronic information sharing systems. Due to the very nature of the activity, information sharing is likely to involve the collection and handling of large amounts of raw data. Agency efforts will additionally center on searching databases (Northrup, Kraemer, & King, 1995) and servicing specific requests for information from other organizations (Ericson & Haggerty, 1997). A concern, therefore, is whether sharing information will lead to resource

[4] Registration criteria vary by network. The Law Enforcement Enterprise Portal (LEEP) provides access to several systems including Law Enforcement Online (LEO) and Regional Information Sharing Systems Network (RISS.Net), and it requires applicants to be employed by a local, state, tribal, or federal law enforcement agency (*Law Enforcement Enterprise Portal*, n.d.). Networks managed by the U.S. Department of Homeland Security tend to be slightly more inclusive because of an all-threats all-hazards focus. For instance, the Homeland Security Information Network (HSIN) is available to law enforcement personnel and private sector entities working to enhance homeland security (*Homeland Security Information Network*, n.d.).

drain (Dawes, 1996) and whether external demands placed upon an agency will negatively impact its ability to set priorities such that agency discretion is threatened (Dawes, 1996; Gil-Garcia et al., 2005). Furthermore, despite access restrictions aimed at building trust between participants, the mishandling of shared information can result in damaging disclosures that lead to a loss of status or civil lawsuits (Center for Technology in Government, 1999; Gil-Garcia et al., 2007; Yang & Maxwell, 2011; Zhang, Dawes, & Sarkis, 2005). It is therefore hypothesized that:

H2: Perceived disadvantages will have a negative influence upon agency use of law enforcement information sharing systems.

Organizational context. The organizational context refers to the structures and processes within an organization that enable or constrict the uptake of a technology (Tornatzky & Fleischer, 1990). Because organizations are complex, human-made entities (Swanson, 2005), a number of different characteristics will impact innovation including goals, authority structures, roles, rules, and patterns of formal and informal practice (Rogers, 2003). For this reason prior research has incorporated a range of descriptive measures centered upon decision-making and internal communication, size of the organizational unit, and available human and technical resources (Hameed, Counsell, & Swift, 2012; Tornatzky & Fleischer, 1990). However, within the law enforcement intelligence domain salient features include those that create "the environment for the cultivation and sharing of knowledge" (Brewster et al., 2014, p.9); while these features represent forms of internal support for personnel, they will also enable officers to reach out beyond the organization into the policing community for the purposes of promoting information exchange. This study focuses upon three organizational factors: organizational readiness, top management support, and formal linking structure.

Organizational readiness refers to the amount of financial and technological resources available to support an innovation (Iacovou et al., 1995). An agency will draw upon its financial resources to build and maintain an IT infrastructure for its information management needs. This entails the procurement of hardware and software in addition to hiring, retaining, and training officers (Nunn, 2001). A lack of financial resources therefore restricts these activities and is a barrier to sharing information electronically (Akbulut et al., 2009; Akbulut-Bailey, 2011; Gil-Garcia et al., 2007; Norris & Moon, 2005; Yang & Maxwell, 2011).

A practical concern is whether an agency has enough available IT resources and expertise to successfully introduce a networked information sharing system. Adopting agencies are more likely to have an adequate IT infrastructure and officers who have received training (Akbulut et al., 2009; Akbulut-Bailey, 2011), whereas a lack of resources and staff shortages act as an impediment (Akbulut et al., 2009; Yang & Maxwell, 2011). Greater readiness also reduces the level of perceived risk associated with the successful integration a new system (Akbulut et al., 2009; Premkumar & Ramamurthy, 1995; Wejnert, 2002). It is therefore hypothesized that:

H3: Organizational readiness will have a positive influence upon agency use of law enforcement information sharing systems.

Leaders play an important role in promoting or inhibiting organizational change (Wilson, 1989). They create the conditions that make innovation possible through planning, goal setting, finding resources to empower workers (Dulin, 2009; Mathis Beath, 1991; Tornatzky & Fleischer, 1990; Yang & Maxwell, 2011; Zhang & Dawes, 2006) and transmitting a message that the change is a priority (McGarrell et al., 2007). When the innovation deviates significantly from past practice, police leaders must influence workers' thinking with the hope that they adopt a new mindset (Ford, 2007). By demonstrating how a change aligns with organizational goals and

exhibiting a commitment to its implementation, leaders can overcome resistance from officers who are skeptical about the need for and permanence of the change (Ford, Weissbein, & Plamondon, 2003; Moore & Stephens, 1991; Skogan, 2008).

Recent studies of intelligence-led policing (ILP) highlight leadership as a facilitator of adoption. For example, an investigation of the New Zealand Police showed uptake was strongest where managers sought to encourage staff to perform ILP tasks and held them accountable to performance objectives (Darroch & Mazerolle, 2013). Similarly, Carter (2011) conducted bivariate and multivariate analyses with measurements of executive support for ILP, explicit rewards for information sharing, and perceptions of ILP as a priority. The results highlight a positive relationship between commitment and ILP adoption.

Although research findings for electronic information sharing also draw attention to leadership commitment as a salient factor, it is unclear whether it determines the adoption or use of electronic sharing technology. For instance, Saviak (2007) found a high level of commitment is a strong predictor of adoption but not system use, while Akbulut-Bailey (2011) concludes that support for, interest in, and importance of electronic information sharing communicated by top management led to its practice. This inconsistency may be due to measurement differences since respondents could interpret commitment as initial championship for an innovation (Rogers, 2003), while a construct for support that uses multiple items may imply ongoing leadership as implementation problems arise (Akbulut et al., 2009). It is therefore hypothesized that:

H4: Top management support will have a positive influence upon agency use of law enforcement information sharing systems.

Formal linking structures enable organizations to reduce uncertainty by developing an awareness of events occurring in the external environment and communicating them internally

(Tornatzky & Fleischer, 1990). To simplify managerial tasks and coordination, these bureaucratic structures involve personnel assignments and a distinct name for a specialist position or team (Galbraith, 1973; Tushman & Nadler, 1986). Formal structure also facilitates informal exchanges (McEvily, Soda, & Tortoriello, 2014) within and outside the organization; such boundary spanning activities inform and support processes such as planning, decision-making (Galbraith, 1973), and innovation (Baker, 2012).

An important linking structure within law enforcement agencies is the intelligence function. This is the activity responsible for any part of law enforcement intelligence, including collection, analysis, or distribution (Carter, 2009). A distinct function will consist of at least one sworn or nonsworn officer capable of understanding intelligence terminology, processes, and products (Carter, 2005; Carter & Schafer, 2007) who serves as a point of contact and acquires information relevant to the strategic and operational planning intended to disrupt criminal and terrorist threats (Carter, 2005). Consistent with the law enforcement intelligence mission, it is therefore hypothesized:

H5: Formal linking structure will have a positive influence upon agency use of law enforcement information sharing systems.

Police diffusion studies have shown the largest agencies are likely to be early adopters of computerized systems (Skogan & Hartnett, 2005; Weisburd & Lum, 2005; Weisburd, Mastrofski, McNally, Greenspan, & Willis, 2003). These organizations have more resources and more personnel than smaller agencies, and are more likely to have specialist structures to support a technological infrastructure (Skogan & Hartnett, 2005). A concern, therefore, is the extent to which agency size not only influences innovation but also other organizational variables such as specialist structures and, arguably, even responses to the institutional environment that

underscore the legitimacy of agency behaviors (Willis et al., 2007). As such it is necessary to control for the influence of agency size in multivariate models.

Environmental context. The environmental context refers to external forces impacting an organization and also forces it can shape (Tornatzky & Fleischer, 1990). This is a broad description and scholars have pursued different theoretical directions given the innovation under consideration. For example, based upon Tornatzky and Fleischer's (1990) original specification and its orientation towards private firms, research has examined the effect of industry characteristics and market structure (i.e., conditions and intensity of competition), technology support infrastructure (i.e., vendors), and government regulation upon organizational innovation. In contrast, law enforcement agencies are institutionalized organizations focused less on market competitors and efficiencies that drive profit-seeking activities than on constituent and member values (Crank, 2003). Police departments have an outward orientation and are selectively responsive to groups such as the media, politicians, funding organizations, unions, and citizens (Maguire, Shin, Zhao, & Hassell, 2003).

Previous studies of law enforcement electronic information sharing systems draw upon social exchange theory (Akbulut, 2003; Akbulut et al., 2009; Akbulut-Bailey, 2011; Saviak, 2007) to investigate the relationship between agencies and their external environment. According to this view exchanges of agency information rely on levels of trust between participants, the power agencies exert over one another in order to meet their own needs, and concerns about the preservation of autonomy (Akbulut, 2003; Dawes, 1996). On the other hand, police researchers contest the extent to which agencies operate as rational-legal hierarchies capable of establishing goals and administrative mechanisms to achieve these goals (Brown, 1981; Manning, 1992, 2001, 2008; Mastrofski, Ritti, & Hoffmaster, 1987; Skolnick, 1966;

Wilson, 1968). Moreover, recent work depicts a complex environment in which department goals, strategies, and actions serve to advance many, and at times conflicting, interests (Crank, 2003; Manning, 2008).

For this reason the introduction of technology into police operations may appear as a progression based upon projected efficiency gains while it actually restricts the ability of officers to fulfill their duties (Chan, Brereton, Legosz, & Doran, 2001; Chan, 2001). While maintenance of formal structures shows organizational actions are "desirable, proper, or appropriate" (Suchman, 1995, p.574), workers' activities may deviate from protocols simply to complete the work (Meyer & Rowan, 1977). In a police environment loosely coupled activities reflect a belief that what officers are doing is correct and the decision not to critically evaluate this core work enables leaders to attend to external groups (Crank, 2003).

In short, there is a need to account for technical innovation related with best practices for crime prevention and attempts to advance the organization's status with key stakeholders. Institutional theory facilitates such an investigation because it describes the role of external pressures and agency responses to them. Critically, it draws attention to formal and informal mechanisms that make it possible for officers to learn about a new practice, as well as the significance it holds for institutional groups. This study focuses upon four environmental factors: threat perception, coercive pressures, mimesis, and normative pressures.

Threat perception refers to the belief that a homeland security incident is likely to take place within an agency's jurisdiction (Davis et al., 2004). Survey research conducted since 2002 suggests agencies are more likely to engage in homeland security preparedness activities when agency decision makers perceive the likelihood of a terrorism event to be higher (Burruss et al., 2010; Davis et al., 2004; Giblin et al., 2014; Haynes & Giblin, 2014; Schafer et al., 2009).

Consistent with the finding that most agencies are unlikely to have experienced a terrorist incident in their jurisdiction (Davis et al., 2004), it is subjective judgments about risk that drive agency preparedness instead of objective assessments indicating such an event actually will occur (Haynes & Giblin, 2014; Roberts, Roberts, & Liedka, 2012). Moreover, the relationship between risk and preparedness does not extend to hazards despite preparatory measures assisting with law enforcement responses to natural and man-made emergencies (Giblin et al., 2014).

Preparedness activities include prevention and response planning, securing resources for training and equipment, establishing crossjurisdictional aid agreements, coordinating multiagency exercises, and organizing community outreach (Davis et al., 2004; Gerber, Cohen, Cannon, Patterson, & Stewart, 2005; Jones, 2000; Randol, 2012). They also encompass intelligence-related actions such as interacting with Joint Terrorism Task Forces (JTTFs), seeking advice about information collection and sharing from federal law enforcement agencies like the Federal Bureau of Investigation, and maintaining computerized intelligence files (Carter, 2009; Carter & Carter, 2009a; Davis et al., 2004; Roberts et al., 2012). In line with National Criminal Intelligence Sharing Plan (NCISP) recommendations, the use of electronic information sharing systems underpin these efforts since the systems are designed to facilitate exchanges of information and intelligence products that enable agencies to learn about and mitigate threats against public safety and critical infrastructure (GIWG, 2003). It is therefore hypothesized that:

H6: Threat perception will have a positive influence upon agency use of law enforcement information sharing systems.

Coercive pressures refer to formal and informal pressures that powerful organizations exert on dependent organizations. These pressures usually have a direct or indirect basis in law that specifies technical and/or financial requirements (DiMaggio & Powell, 1983; Meyer &

Rowan, 1977; Tolbert & Zucker, 1983; Zucker, 1983); in response dependent organizations modify aspects of their structures, rules, and practices so they conform to institutional expectations. For example, Crank and Rehm's (1994) case study of the Illinois State Police's drug interdiction program, Operation Valkyrie, illustrates how prior court rulings concerning police methods for identifying and intercepting drug couriers led to the introduction of a new strategy focusing on vehicles used for courier activity instead of courier profiles.

Likewise, civil lawsuits arising from officers' individual misconduct are another source of coercion. Under the Enforcement Act of 1871 42 U.S. Code Section 1983, any citizen of and within the jurisdiction of the United States can seek redress for the deprivation of their Constitutional rights (Cornell University Law School, n.d.). From a societal perspective, Section 1983 lawsuits serve to hold officers, agencies, and municipalities responsible for policing activities and establish "bounds of professional practice" (Kappeler, 2006, p.12). In effect the legal environment proscribes and prohibits institutional behavior (Giblin, 2004; Hinings & Greenwood, 1988; Meyer & Rowan, 1977) via orders for agencies to pay what can be significant dollar sums to citizens who win cases, or as the result of parties negotiating a settlement. Outcomes like these also damage officer morale and when publicized they present police conduct in a bad light (Kappeler, 2006).

Recent research indicates the rational deterrent effect of civil suits is limited due to the inability of agencies to access enough details about Section 1983 lawsuits to make informed decisions that result in corrective changes (Johnson, 2012; Schwartz, 2009). However, other work presents a slightly different view that emphasizes organizational proactivity: the prospect of civil suits leads law enforcement agencies to adopt new policies and practices that promote professionalization and reduce exposure to litigation (Vaughn, Cooper, & del Carmen, 2001;

Weiss, 1997). Where law enforcement intelligence is concerned the Criminal Intelligence Systems Operating Policies Federal Regulation (28 CFR Part 23) provides guidelines for handling criminal intelligence records while also upholding the constitutional rights of individuals (Carter, 2010). Although it is not a mandate, adherence to 28 CFR Part 23 protects against the likelihood of legal challenges to intelligence-driven processes (Carter, 2011) and it provides an important standard for the operation of multijurisdictional criminal intelligence systems, whether federally funded or not (GIWG, 2003). It is therefore hypothesized that:

H7: Coercive pressures will have a positive influence upon agency use of law enforcement information sharing systems.

Mimesis refers to an organization's imitation of others in response to uncertainty (DiMaggio & Powell, 1983). The modeling of practices successfully employed by other organizations is a viable option in the face of uncertain goals and untested technologies. Such modeling may arise coincidentally as employees move between organizations or more purposefully via informal communication channels (DiMaggio & Powell, 1983). For instance, telephone and email communication between police officers in different agencies facilitates peer emulation (Carter, 2011; Weiss, 1997, 1998). These actions are indicative of an occupation that values innovation (Crank & Langworthy, 1992; Meyer & Rowan, 1977); as a "potent contemporary myth" (Crank & Langworth, 1992, p.352), police agencies are able to demonstrate their attentiveness to problems that are important to institutional stakeholders, specifically through the use of modern methods for controlling crime (Bolman & Deal, 1991; Crank & Langworthy, 1992; Mastrofski & Uchida, 1996).

Prior studies have highlighted mimetic processes as a source of change within police departments. Crank and Rehm (1994) describe how, after the Illinois State Police released

information about its interdiction efforts in a national newsletter and at seminars, Operation Valkyrie served as a model for other agencies' programs. Similarly, Willis et al.'s (2007) retrospective analysis of Compstat implementation by three large municipal police departments reveals the intentional selection of the New York Police Department's variant. The realization that mimicry of an original program would enhance the legitimacy of borrowing agencies was not lost on participants despite the absence of objective assessments establishing Compstat's effectiveness for reducing violent crimes or crimes in general. Furthermore, survey findings draw attention to the relationship between agency attention paid to other innovative agencies and the adoption of crime analysis units (Giblin, 2004, 2006), community-oriented policing (Burruss & Giblin, 2014; Giblin & Burruss, 2009), and homeland security preparedness activities (Burruss et al., 2010). It is therefore hypothesized that:

H8: Mimesis will have a positive influence upon agency use of law enforcement information sharing systems.

DiMaggio and Powell (1983) argue normative isomorphic pressures arise mainly from professionalization. They therefore present professionalization as interchanges between members of an occupational group that establish work definitions and procedures. An ongoing social process, professionalization enables members to construct shared meanings for the work they perform (McClellan & Gustafson, 2012) and, by carrying out actions guided by similar beliefs, a pattern of normative isomorphism takes hold across the industry (DiMaggio, 1988; DiMaggio & Powell, 1983).

Two professional mechanisms in law enforcement are credentialing processes and training. Credentialing processes present standards that applicants must meet in order to be certified. Studies highlight a relationship, for instance, between voluntary participation in the

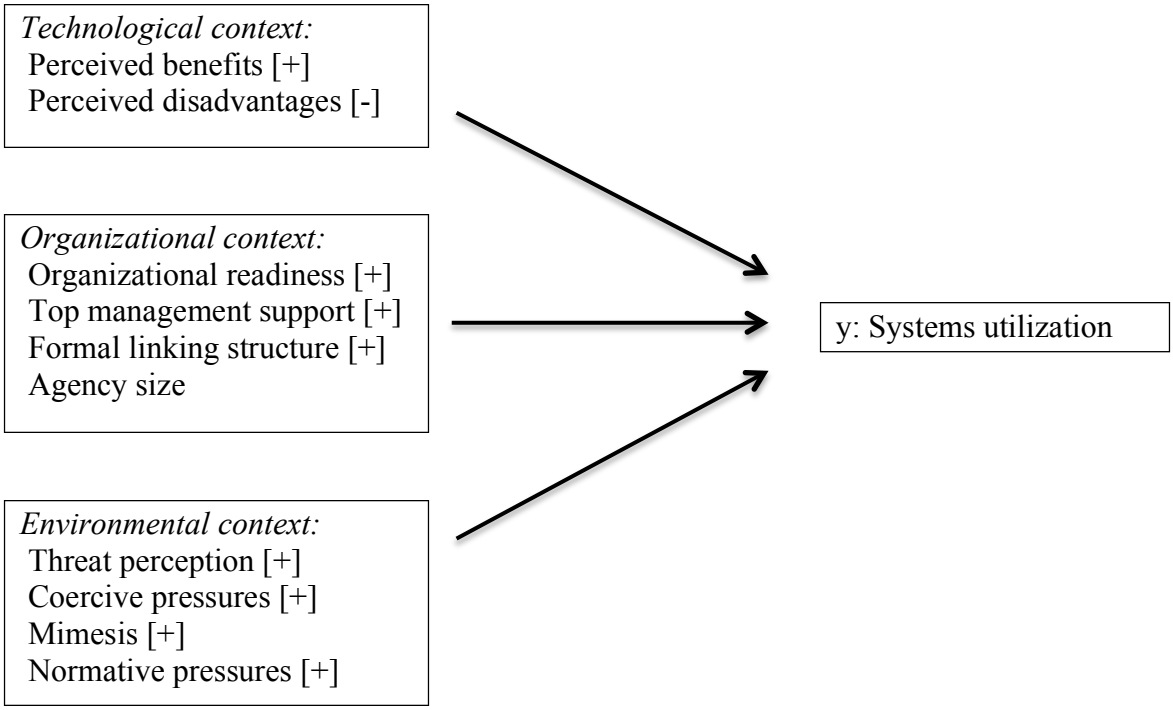
Commission on Law Enforcement Accreditation (CALEA) program and agency adoption of new innovations aimed at advancing public safety (Giblin, 2004, 2006; Skogan & Hartnett, 2005). Similarly, training facilitates knowledge diffusion and institutionalizes common vocabularies within a profession (DiMaggio & Powell, 1983). As a result practitioners sent by their agencies are taught key concepts and practices they can subsequently share with work colleagues (Burruss & Giblin, 2014; Burruss et al., 2010; Giblin, 2004; Giblin & Burruss, 2009; Skogan & Hartnett, 2005) and introduce to relational networks (Carter, 2011; Meyer & Rowan, 1977; Roy & Séguin, 2000; Weiss, 1997, 1998). This is an important process when the subject is relatively new and knowledge useful for practitioners has yet to be published; in the case of law enforcement intelligence, research indicates information made available at state and federal trainings has been a significant aid to the development of agencies' intelligence capacities (Carter, Carter, & Chermak, 2013; Chermak et al., 2013). It is therefore hypothesized that:

H9: Normative pressures will have a positive influence upon agency use of law enforcement information sharing systems.

Taken together, Figure 1 presents a model with the factors hypothesized to affect law agencies' use of electronic information sharing systems. The model depicts technological, organizational, and environmental factors acting in parallel and each of the variables exerting a direct influence on this activity. It should be noted that diffusion studies, by including longitudinal data to clarify the temporal order of events, indicate contextual factors are likely to "interact and reinforce each other in the course of the institutional process" (Roy and Séguin, 2000, p.464); an example from the policing literature is Crank and Rehm's (1994) argument that coercive forces preceded mimetic and normative pressures with respect to agencies' drug-interdiction efforts during the 1980s. As a consequence, and consistent with innovativeness

studies that rely on cross-sectional research designs to investigate organizational adaptation at a single point in time, the current study does not attempt to examine these interrelationships.

Figure 1: Proposed Model for Agency Use of Electronic Information Sharing Systems



Summary

Relatively few studies have examined the determinants of electronic systems use within police organizations. Confusingly, and perhaps inevitably because of the different research questions and a perceived demand within the academic community for original research instead of replication, this body of work emphasizes different constructs and different results. This pattern also holds for a very small subset of studies addressing the implementation of systems intended to facilitate information exchanges between law enforcement agencies. The findings of

these studies broadly suggest relative advantage and agency leadership are important factors when attempting to explain variation in police use of these systems.

A critical development has been recent research that highlights changes in the policing field with respect to law enforcement intelligence (Carter, 2011; Carter et al., 2012). Information sharing is a foundation of this enterprise so the review of prior research presented in this chapter serves primarily to identify variables relevant to the information exchange and promotion of the ISE. But what also emerges from a reading of this work is the tension between the rational expectations and symbolism associated with police information technologies. Manning (2014) explains it thus:

> The assumption of technological rationality, that technology has exclusively positive, systematic, predictable, and endearing consequences, is untenable. The craft of policing, as archaic as it may be, is predicated on managing the vagaries of the human condition...This means in turn that technologies are situationally contingent and relevant, rather than concretely obvious in their functions, meanings, and uses (pp.2502-3).

And yet studies do suggest rational factors contribute to the introduction of information systems into agencies (Willis et al., 2007; Randol, 2013). It follows that instead of viewing rational and symbolic interpretations as mutually exclusive (Mastrofski, 1998; Wilson, 2006), this study proposes a model that integrates both perspectives. This is made possible by including organizational concepts that scholars deem central to technological innovation within police bureaucracies, along with those that reflect the role of institutional values in shaping agency learning and responses.

In keeping with a police innovativeness research agenda, the current study uses a cross-sectional design to specify and test relationship between technological, organizational, and

environmental variables and the use of electronic information sharing systems by law enforcement agencies. The next chapter therefore presents details of the design and administration of a measurement instrument to law enforcement professionals, and a plan for the analysis of study data collected.

Chapter 3: Methodology and Data

The previous chapter examined empirical findings relating to law enforcement electronic information sharing systems and contextual factors that affect their use. This chapter describes methods employed for the current study and the use of data collected as part of a project examining the intelligence practices of law enforcement agencies in the United States. These details are organized into six sections: selection of participants, instrument design, data collection, strategy for managing missing data, measurement, and data analysis plan.

Selection of Participants

The current study uses data collected as part of a project sponsored by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) and funded by the Department of Homeland Science and Technology Directorate's Office of University Programs, Center for the Study of Terrorism and Behavior (CSTAB) 2.13[5]. The purpose of this project was to understand (1) current information sharing and intelligence practices within law enforcement agencies, and (2) barriers to effective sharing of law enforcement information and intelligence. The anticipated outcome was the generation of knowledge about how agencies share information with a view to confronting terrorism following events on September 11, 2001 (Carter, Chermak, Carter, & Drew, 2014). With this objective in mind, a team of researchers from Michigan State University designed and distributed a self-administered survey to two samples of law enforcement intelligence professionals.

The first sample consisted of individuals who had participated in trainings conducted by the Memorial Institute for the Prevention of Terrorism (MIPT). Established as a nonprofit organization in 1995 following the bombing of the Alfred P. Murrah Federal Building in

[5] The Award Number for this research was 2012-ST-061-CS0001.

Oklahoma City, MIPT has primarily served as a point of reference for researchers, practitioners, and policymakers by collaborating on terrorism research projects and maintaining databases and archival materials containing information about terrorism (Ellis III, 2008). Additionally, significant numbers of police officers have participated in its trainings with support from the Department of Homeland Security (DHS), particularly workshops focusing on information sharing activities that promote law enforcement intelligence and counterterrorism activities. The research team therefore sought permission to conduct survey research within this group and MIPT offered to contact individuals registered for previous training programs with an invitation to participate in the study (Carter et al., 2014).

The second sample included individuals who participated in a training program organized and delivered by the School of Criminal Justice at Michigan State University (MSU). The program, the Law Enforcement Intelligence Toolbox, ran from 2005 to 2011 with the objective of increasing participants' knowledge of concepts and issues relating to the police intelligence function. As with the MIPT trainings, the provision of DHS funding to support these activities was contingent upon courses having standardized content and delivery (Carter et al., 2014). Total enrollment during the MSU program's lifetime was 4,723 officers from 2,102 agencies (Carter, 2011) with many of the officers being selected as representatives of their agencies' intelligence function (Carter et al., 2012).

The decision to approach this population reflects the view that the law enforcement intelligence field is highly specialized and subject to rapid change (Carter et al., 2012). Therefore, rather than generate a random sampling frame consisting of officers who would be unable to respond to questions relating to intelligence activities, a purposive sampling strategy was used to reach key personnel with the requisite knowledge and work experience to provide

accurate information (Kumar, Stern, & Anderson, 1993; Phillips, 1981). Key personnel here included individuals whose role and responsibilities had exposed them to law enforcement intelligence such that they understood issues relating to the development of an intelligence capacity and were aware of current intelligence requirements and processes.

It should be noted that the MIPT and MSU trainings were not exclusively offered to law enforcement personnel but were instead designed to inform a range of government workers including first responders from organizations such as fire departments, as well as government workers in nonlaw enforcement agencies still involved with homeland security planning or response activities. For this reason it was necessary to use a filtering strategy to verify attendees worked for law enforcement organizations. This targeted approach involves selection bias because there may have been workers who were eligible to train but could not attend, in particular when an agency could not afford workers to be absent. Nevertheless, the samples do consist of personnel with varying levels of professional experience, supervisory authority, and who are employed by agencies that serve different state, local, and tribal jurisdictions. The inclusion of key personnel therefore enhances the internal validity of the study measures, as well as external validity when assessing findings in terms of the population of law enforcement intelligence workers as a whole (Carter et al., 2014; Carter et al., 2012; Carter, 2011; Chermak et al., 2013).

Instrument Design

The START project used a survey methodology to gather data from study participants about their agencies' intelligence practices. Development of an instrument began with a review of recent research to identify important intelligence issues and then moved to drafting of survey items. These items asked for factual, attitudinal, and behavioral information about law

enforcement intelligence functions, perceptions of terrorist threats, agency preparedness, interagency interactions, and processes supporting information sharing. However, a feature of the survey vital to the current study was the incorporation of items used to measure technological, organizational, and environmental characteristics of participants' agencies, as well as their experiences with law enforcement electronic information sharing systems. Additional items asked respondents to indicate whether they were sworn or nonsworn personnel, and their role and tenure with the agency.

Care was taken during the design phase to ensure each question was relevant and comprehensible to readers by using simple sentences, avoiding excessive use of technical language, keeping questions as short as possible, and making the response task clear (Dillman, Smyth, & Melani Christian, 2009; Nardi, 2006). Furthermore, the research team sought feedback from state, local, and tribal law enforcement professionals who served as subject matter experts. This step was undertaken to identify problematic questions, but critically to increase the content validity of the survey items by increasing the content and coverage of questions. Lastly, the survey was submitted to the MSU Institutional Review Board, a body comprised of individuals both affiliated with and outside the University who follow federal, state, local, and university guidelines when assessing whether proposed research provides necessary ethical and safety protections for human subjects[6]. In its approved form, the instrument included 48 fixed-choice or open-ended questions organized by topic into 10 sections. A copy of the survey is shown in Appendix B.

[6] See http://hrpp.msu.edu/irb-office for more information.

Data Collection

Data collection for the START project involved the use of a web-based survey. The selection of this method rested upon concerns about the costs of mailing surveys and whether surveys would reach the desks of key informants via agencies' listed street addresses. Instead, the advantages of a web-based survey include reduced costs of administration, increased control over how questions are presented, convenience of response for participants, and the quick, reliable capture of responses as digital data (Gil-Garcia, Berg, Pardo, Burke, & Guler, 2009). Nevertheless, it is necessary to consider what access participants have to computers in order for them to participate in an online study (Dillman et al., 2009; Gil-Garcia et al., 2009). In this case the research team assumed respondents would have access to computers because study participants from both the MIPT and MSU samples had registered their email addresses at the respective trainings.

Preparation of the web-based survey involved the reproduction of the study instrument on the web site of a provider capable of securing respondent data[7]. The survey instructions, including details about the study and informed consent, and the questions were replicated online as a series of web pages. To simplify navigation questions were clearly numbered and the font, sizing, and color of survey text made consistent. The question text and responses for each item were displayed fully on the page they appeared, despite the amount of questions shown on each page being limited to minimize downward scrolling (Dillman et al., 2009; Fan & Yan, 2010). Lastly, in order to verify the web-based design was an exact copy of the original instrument and that responses were being captured correctly, members of the research team undertook the survey and inspected the recorded responses.

[7] The survey provider was http://www.surveymonkey.com.

Delivery of the survey began in September 2013 by sending invitation emails to the study participants. These emails included details of the study and its aims, a request for the participants to complete a self-administered web-based survey, and a URL the participants could use to access the online survey. The format of the emails was standardized but, to preserve the confidentiality of study participants, MIPT representatives took responsibility for sending emails to individuals who had attended their trainings while the research team transmitted emails to attendees at MSU trainings. This division of labor had two consequences. First, while the study team recorded automated notifications from mail servers to identify undelivered emails along with replies from participants who declined to participate, the MIPT representatives did not report taking the same steps. Thus the MSU sampling frame was adjusted to more accurately calculate response rates, but the MIPT sampling frame remained the same. Second, neither group assigned identifiers that would make it possible to track respondents. For analytical purposes it was therefore necessary to rely on respondents reliably reporting what agency they belonged to, such that it was possible to establish the identity of the organization.

Nonresponse error presents a serious challenge to research because too few responses inevitably prompt questions about whether respondents differ from nonrespondents in a way that is significant to the study (Billiet & Matsuo, 2012; Dillman et al., 2009; Rogelberg & Stanton, 2007). As a result, the ability of researchers to make inferences based upon a sample about the study population is diminished. Several factors may contribute to this situation including the characteristics of respondents (e.g., openness to survey participation, altruism) and the survey (e.g., length and salience), and advance contact with respondents (Anseel, Lievens, Schollaert, & Choragwicka, 2010; Cycyota & Harrison, 2006; Heberlein & Baumgartner, 1978). Due to their relative strengths and weaknesses, survey modes also affects response rates (Dillman & Melani

Christian, 2005). For instance, researchers using a web-based design must contend with it being an impersonal method of interviewing individuals and emails not blocked as junk messages that reach participants' attention are easy to delete (Fan & Yan, 2010; Shih & Fan, 2008). Prior research also suggests reasons for the nonparticipation of law enforcement intelligence professionals in an online survey were individuals no longer worked in the intelligence function, were unwilling or unable to invest the time required to complete the survey, declined to participate as they believed a colleague from the same organization had already responded, or were worried about the security implications of sharing information outside of the law enforcement community (Carter et al., 2012).

With these thoughts in mind, the research team took steps to promote the START survey and increase the number of study responses. These activities included instructions emphasizing the value of participation, thanking respondents in follow up emails, and demonstrating institutional support for the study. The latter item involved highlighting the level of professional interest attached to the study by featuring the START logo prominently on the online survey as well as statements about university involvement (Dillman et al., 2009; Fan & Yan, 2010).

11,103 emails with a link to the START online survey were sent to intelligence workers in the MIPT survey of whom 327 individuals (2.9%) responded. In the case of the MSU sample 869 emails were sent to intelligence workers and 190 individuals (21.9%) responded. The unit of analysis, however, was the agency so these responses were examined to determine how many distinct organizations the individuals represented for both samples. This process involved a comparison of target and respondent agencies, and adjustments consistent with the study goals. First, submissions were only included for analysis if the law enforcement agency could be clearly identified. Second, since federal agencies are mandated to share information across the

ISE and fusion centers rely on sharing networks to disseminate information, responses from these organizations were also dropped. Thus, the data for this study consists of 335 responses from individuals who were employed at 147 local, county, or state law enforcement agencies, with responses for nine agencies appearing in the MIPT and MSU samples.

Table 1: Respondent Characteristics (N=335)

	MIPT		MSU Toolbox	
	n	(%)	n	(%)
Sworn status				
Sworn	141	(67.1)	99	(79.2)
Nonsworn	69	(32.9)	26	(20.8)
Role				
Administrative manager	15	(7.5)	30	(25.4)
Supervisor	43	(21.4)	38	(32.2)
Investigator/Uniformed	79	(39.3)	31	(26.3)
Analyst	64	(31.8)	19	(16.1)
Tenure				
Less than 1 year	2	(1.0)	0	(0.0)
1-3 years	13	(6.2)	2	(1.6)
4-9 years	52	(24.8)	18	(14.4)
10-15 years	49	(23.3)	33	(26.4)
More than 15 years	94	(44.8)	72	(57.6)

Note. Percentages may not total 100.0 due to rounding.

Table 1 presents descriptive statistics for the study respondents. In the case of the MIPT sample, there were 210 respondents. These individuals tended to be sworn personnel (67.1%), working either in an investigator/uniformed (39.3%) or analyst (31.8%) role, and been with their agency for more than 15 years (44.8%). The MSU sample included 125 respondents who were also more likely to have sworn status (79.2%) and an agency tenure of more than 15 years (57.6%), but the largest category for role was that of supervisor (32.2%) while analysts were fewest (16.1%).

Table 2: Agency Characteristics of Nonrespondents and Respondents by Sample

	MIPT				Toolbox			
	Non-respondents		Respondents		Non-respondents		Respondents	
	n	(%)	n	(%)	n	(%)	n	(%)
Jurisdiction								
State	20	(3.8)	7	(9.3)	11	(6.5)	7	(8.6)
Municipal	407	(77.4)	44	(58.7)	115	(68.1)	55	(67.9)
County	93	(17.7)	24	(32.0)	40	(23.7)	19	(23.5)
Tribal	6	(1.1)	0	(0.0)	3	(1.8)	0	(0.0)
Total	526		75		169		81	
Total personnel								
Less than 25	177	(33.7)	5	(6.7)	10	(5.9)	5	(6.2)
26-100	195	(37.1)	15	(20.0)	47	(27.8)	19	(23.5)
101-250	67	(12.7)	13	(17.3)	44	(26.0)	18	(22.2)
251-500	21	(4.0)	9	(12.0)	21	(12.4)	5	(6.2)
501-3,000	59	(11.2)	26	(34.7)	42	(24.9)	27	(33.3)
More than 3,000	7	(1.3)	7	(9.3)	5	(3.0)	7	(8.6)
Total	526		75		169		81	
Region								
Northeast	25	(4.8)	3	(4.0)	22	(13.0)	8	(9.9)
Midwest	168	(31.9)	11	(14.7)	20	(11.8)	11	(13.6)
South	269	(51.1)	56	(74.7)	68	(40.2)	39	(48.2)
West	64	(12.2)	5	(6.7)	59	(34.9)	23	(28.4)
Total	526		75		169		81	

Note. Percentages may not total 100.0 due to rounding.

Lastly, the total agency counts in Table 2 enable the calculation of agency response rates by using the formula (sample respondents / (sample nonrespondents + respondents) * 100). The response rates were 12.5% for the MIPT sample and 32.4% for the MSU sample. Allowing for the sensitivity of the research topic and declines in survey participation over the past thirty years (Anseel et al., 2010; Baruch & Holtom, 2008; Brick & Williams, 2013), the response rate for the latter sample is encouraging (Carter et al., 2014). However, the response rate for the MIPT is considerably lower. A possible explanation for the difference in rates is the receptiveness of

participants who have received training through MSU to engage in research being conducted by the same institution. Additionally, MIPT representatives informed the study team prior to data collection that they themselves had recently surveyed members of the MIPT sample, and as such they may have been less willing to participate in another study so soon after the first.

Strategy for Managing Missing Data

Item nonresponse is another aspect of survey research that requires attention due to respondents choosing to skip questions or end their involvement prematurely. In practical terms, missing data complicate statistical analysis and the production of meaningful results. One solution to address this situation is to discard incomplete submissions using a deletion method but removal of more than a few cases can lead to distorted parameter estimates and diminished statistical power (Enders, 2010; McKnight, McKnight, Sidani, & Figueredo, 2007). Another option is to fill missing values using the multiple imputation technique provided the underlying pattern of missingness is genuinely random (Rubin, 1976). If, even after controlling for all of the available observed information, the mechanism for missing data is due to the missing values themselves (i.e., missing not at random), multiple imputation is not viable (Jamshidian, 2004; Rubin, 1976; Schafer & Graham, 2002).

For this study, missing data pose a challenge because only 29 from all 335 submissions (8.7%) were fully completed. Of 177 variables capturing survey answers, all but seven had missing responses. The extent of missingness ranged from five to 56 per cent with questions found later in the survey being the least well answered. Critically, however, approximately 44 per cent of responses to questions measuring the dependent variable were missing. Due to concerns about using multiple imputation to estimate outcome measures when there are high levels of missing covariates and the missing mechanism is unclear (Little, 1992), listwise

deletion was selected as the most appropriate method for handling missing data. Adjustments were made in the following order:

1. Aggregation of responses to the agency level. Of the 147 distinct agencies represented in the collected data, 46 agencies (31.3%) had two or more responses that needed to be reduced to a single submission before analysis. Available solutions to achieve this included random selection, purposive selection based upon the completeness of response data, or purposive selection based upon a respondent characteristic. Consistent with the view that a participant's position in an organization shapes his or her interpretations of technology (Orlikowski & Gash, 1994), the selection criterion was respondent role. Specifically, where there were multiple responses then administrators were given priority due to their understanding of organizational motivations for using electronic systems, as opposed to an individual focus on use of the systems (Orlikowski & Gash, 1994); if there were two or more respondents from the same agency who were administrators, then one was selected at random; if there were no administrators, then priority was given to supervisors, then uniformed officers, and lastly analysts. At the end of this step, the number of agencies in the sample remained unchanged (N=147).
2. Removal of submissions where responses would compromise the construction of scale items. Several items in the survey presented respondents with an option indicating they did not know the information being requested, or, in the case of items referring to electronic sharing systems, that their agency did not use them. Placed after Likert items, however, inclusion of these data would skew scale estimates. For this reason these responses were removed and the result was a reduction in sample

size of 38 agencies (N=109).

3. Removal of all missing responses for questions measuring dependent variables. Possible reasons for respondent omissions include not knowing whether the agency uses electronic sharing systems, or not disclosing whether it does or does not use these systems due to sensitivity concerns about the topic. Without respondents providing more information it is not possible to know whether agencies do use electronic sharing systems. This adjustment reduced the sample size by 47 agencies (N=62).
4. Removal of all missing responses for the remaining study variables. After the deletions performed prior to this step it was still necessary to drop submissions lacking responses to items that measure study constructs. The removal of this missing data led to a decrease in sample size of 17 agencies (N=45).

An alternative course of action for the final step would have been to use multiple imputation to estimate missing values for the study covariates. An iterative process, multiple imputation uses observed data to derive sets of imputed values, or parameter estimates (McKnight et al., 2007). Production of these estimates, which accounts for different measurement levels, is invaluable when the objective is to use regression analyses for fitting models but it also limits the ability to meaningfully report univariate and bivariate statistics since satisfactory results often depend upon the generation of many imputed datasets (Horton & Lipsitz, 2001), and not a single set of results[8]. After careful consideration of the study goals and

[8] Although not included in the analyses for this study, Stata's *mi impute* command generated 30, 50, and 70 datasets for 21 variables with missing values. A sensitivity analysis revealed the means of pooled values for these variables (i.e., the means of means across datasets) did not deviate more than two-tenths from the means for completed cases. But the only descriptive statistic available was a mean.

the need to present variable frequencies, this study used listwise deletion as the final strategy for managing missing values.

Measurement

This section describes the operationalizations and measurements for the study variables. Where possible the study uses items from instruments validated in prior studies, but in several cases there was a need to either adapt or construct new measures. Table 3 summarizes the variables, question items, and measurement type for the following variables.

Table 3: Characteristics of Study Variables

Variable	Items	Questions
System utilization	5	q25
Perceived benefits	4	q27
Perceived disadvantages	4	q27
Organizational readiness	4	q23
Top management support	3	q28
Formal linking structure	1	q9
Agency size	1	q6
Threat perception	8	q15
Coercive pressures	1	q12
Mimesis	1	q45
Normative pressures	4	q35, q46

Dependent variable. The dependent variable measured agency use of electronic information sharing systems. This behavior was measured using the responses to a question asking study participants to indicate how often their agency accessed a networked information sharing system. The response categories were daily, once or twice a week, three times a week but not daily, every two weeks, monthly, less than once per month, and do not access a system. Here, responses were recoded "0" (we do not access a system), "1" (less than once per month or

monthly), “2” (every two weeks), “3” (three times a week, or once or twice a week), and “4” (daily) to indicate system use.

Independent variables. Perceived benefits measured respondents’ beliefs about the advantages associated with using law enforcement electronic information sharing systems. Items were derived from prior studies of information sharing between government (Dawes, 1996) and law enforcement agencies (Akbulut-Bailey, 2011). Respondents were asked to use a 7-point Likert-type scale to indicate their level of agreement with respect to statements about electronic information sharing systems leading to: (1) improved quality of information being shared, (2) increased information sharing between workers in their organization, (3) increased information sharing between workers in different agencies, and (4) secure communication of information shared. Responses were coded “1” (strongly disagree) through “7” (strongly agree) to signify their level of agreement.

Perceived disadvantages measured respondents’ beliefs about problems linked with the use of electronic information sharing systems. As in the case of perceived advantages, the items (Akbulut-Bailey, 2011; Dawes, 1996) asked respondents to use a 7-point Likert-type scale to record their level of agreement in relation to statements about electronic information sharing systems leading to: (1) Too much information being collected, (2) increased demands for information beyond their agency’s capacity to respond, (3) resources being diverted away from other agency priorities, and (4) shared data being misinterpreted or misused. Responses were coded “1” (strongly disagree) through “7” (strongly agree) to signify their level of agreement.

Organization readiness measured respondents’ perceptions about the level of organizational resources available for information and intelligence sharing. Respondents were asked to use a 4-point Likert-type scale to indicate their level of agreement with respect to

statements about specific resources being a problem in relation to the sharing of information and intelligence by their agency. The four items used to construct a measure were: (1) adequate personnel, (2) adequate training, (3) adequate resources, and (4) adequate time. Responses were coded "1" to indicate the item was a significant problem, "2" if somewhat of a problem, and "3" if not a problem at all.

Top management support measured respondents' perceptions about top management and their efforts to create a work environment that encourages the use of electronic information sharing systems (Akbulut-Bailey, 2011). Respondents were asked to use a 7-point Likert-type scale to indicate their level of agreement with respect to three items (Grover, 1993): (1) top management are interested in networked sharing systems, (2) top management consider these systems important to the organization, and (3) top management has effectively communicated its support for these systems. Responses were coded "1" (strongly disagree) through "7" (strongly agree) to show their level of agreement.

Formal linking structure measured the presence of an intelligence function in the agency. Respondents were asked to select one of five options for the item, "Which best describes the focus of your intelligence function?" The options included a focus on terrorism only, the use of an all-crimes approach, the use of an all-crimes, all-threats and all-hazards approach, focus not specified, or no intelligence function. Responses were coded to create an ordinal variable using "0" to indicate no intelligence function, "1" for a function with a limited focus (i.e., terrorism only, all-crimes, or not specified), and "2" for a function with an all-crimes, all-threats and all-hazards approach.

According to Tornatzky and Fleischer (1990), in the absence of accurate metrics for work performed, the number of employees is an adequate measure of organizational size. The item

used to determine agency size, therefore, was an ordinal variable asking respondents how many total sworn and nonsworn personnel work in their organization. Responses were coded "1" for agencies with less than 25 employees, "2" for agencies with 26-100 employees, "3" for agencies with 101-250 employees, "4" for agencies with 251-500 employees, "5" for agencies with 501-3000 employees, and "6" for agencies with more than 3000 employees.

Threat perception measured the likelihood of a homeland security incident taking place within an agency jurisdiction (Davis et al., 2004). Respondents were asked to use a 4-point Likert-type scale to indicate whether terrorism events would occur in their state in the next five years. Separate items asked about each of the following events: (1) a chemical incident, (2) a biological incident, (3) a nuclear or radiological incident, (4) a conventional explosive incident, (5) cyber terrorism, (6) agro-terrorism incident involving food, (7) agro-terrorism incident involving an animal disease nontransferable to humans, and (8) terrorism incident involving military weapons. Responses were coded "1" for very unlikely, "2" for unlikely, "3" for likely, and "4" for very likely.

Coercive pressures measured the influence of technical requirements for agency handling of law enforcement intelligence. The indicator used here was the question, "Is your criminal intelligence records system 28 CFR Part 23 compliant?" Responses were used to create a dichotomous variable with "0" denoting noncompliance, and "1" representing system compliance or ongoing modifications to meet the standard.

Mimesis measured an agency's practice of modeling other law enforcement organizations. The indicator used here was the question, "To what extent does your organization model its information sharing activities after those of other agencies that you view as successful?" Responses were coded with "0" for never, "1" for sometimes, and "2" for often.

Normative pressures measured agency exchanges of work-related ideas made possible through formal interactions between agency personnel and members of other law enforcement officials. Several items were adapted from prior research to construct this variable (Carter et al., 2012; Carter et al., 2013; Giblin, 2004; Giblin & Burruss, 2009). First, respondents were asked whether agency personnel had attended intelligence training programs: (1) Fundamentals of Intelligence Training (FIAT), (2) State and Local Anti-Terrorism Training (SLATT), and (3) Bureau of Justice Assistance (BJA) 28 CFR 23 Training. Responses were code with "0" for nonattendance and "1" for attendance. Second, data were gathered from the Commission of the Accreditation of Law Enforcement Agencies' (CALEA) website to create a dichotomous variable indicating whether agencies were accredited. These data were coded "0" for nonaccredited agencies and "1" for accredited agencies.

Agency creation measured the generation of intelligence products by agency workers to share with other organizations. Respondents were asked to indicate how frequently their agency created the following products: (1) bulletins, (2) threat assessments, (3), vulnerability assessments, (4) risk assessments, and (5) alerts. Responses were coded "1" for never, "2" for monthly, "3" for weekly, "4" for daily, and "5" for upon request.

Agency receipt measured workers' acceptance of intelligence products created by other organizations. Respondents were asked to use a 4-point Likert-type scale to indicate how frequently their agency received products with the following content: (1) new information, (2) information on officer safety threats, and (3) actionable information that facilitates an agency response. Responses were coded "1" for very infrequently, "2" for infrequently, "3" for frequently, and "4" for very frequently.

Construction of study indices. Principal component factor analysis with Promax rotation was used to assess the construct validity of scale items (Nunnally, 1978). This statistical method evaluates variation among a set of observed data for the purpose of determining how well they measure a latent structure, or factor. As an iterative process it involves estimation of a correlation matrix and the calculation of factor loadings, the correlations of a variable with a factor (Kline, 1994). The decision to drop items based upon their factor loadings may depend on their comparative magnitudes and the extent that items crossload on different factors, but a minimum threshold is a loading of ± 0.30 or higher (Matsunaga, 2010). Additionally, eigenvalues encapsulate the total amount of variance for a factor. Of several possible methods for selecting factors to retain (Zwick & Velicer, 1986), Kaiser's recommendation for keeping factors with eigenvalues greater than 1.0 (Kaiser, 1960) and scree plots of eigenvalues (Cattrell, 1966) were used to identify factors for inclusion in the study analyses.

Cronbach's alpha was used as an estimate of scale items' reliability, or the extent to which they are repeatable (Nunnally, 1978). Alpha coefficients of equivalence range from negative infinity to 1.0, with a positive score closer to 1.0 indicating a scale is internally consistent. What level below this value serves as an acceptable lower bound is unclear; Nunnally (1978) argues greater leeway may be tolerated in exploratory research, while still recommending a value of 0.8 or higher. However, alpha scores may be inflated when more items are included in a scale (Cortina, 1993) and values greater than 0.9 indicate the presence of redundant items (Tavakol & Dennick, 2011).

Table 4: Principal-Components Analysis With Promax Rotation and Coefficient Alphas for the Predictive Indices (N=45)

Item	Range of factor loadings	Percent of variance explained	Alpha coefficient
Perceived benefits	0.863-0.952	79.9	.91
Perceived disadvantages	0.747-0.858	61.9	.79
Organizational readiness	0.654-0.890	62.3	.80
Top management support	0.974-0.986	95.6	.98
Threat perception	0.685-0.809	56.2	.89
Normative pressures	(−0.516)-0.744	30.7	.26

Table 4 reports factor loadings, percentages of variance explained, and alpha coefficients for the study's predictive indices. For the first five indices, factor loadings were reasonably high, ranging from .654 to .986, and percentages of variance explained by the factors were approximately 50.0 percent or higher. Similarly, the alpha coefficients were approximately equal to or in excess of .80, thus indicating their reliability as measures of the study constructs. However, the results of the analyses for the normative pressures index were problematic as the factor loadings, percentage of variance explained, and reliability measure highlight. A decision was taken, therefore, to drop the normative pressures index and rely on CALEA accreditation as a single measure for normative pressures.

Data Analysis Plan

Allowing for the reduced number of usable cases, the present research is designed as a quantitative study that includes descriptive and inferential statistics. Several steps will be taken to generate and evaluate these statistics. Descriptive statistics will be used to highlight the frequency and distribution of single variables, followed by bivariate analyses to test relationships between independent and dependent variables, and the strength of relationships once established. Contingent upon the discovery of significant bivariate relationships, logistic regression models

will be used to develop partial models for context groups in order to explain agency use of electronic sharing systems.

Summary

This chapter set out the methodology and data used to address the research questions. A purposive sampling strategy was used to identify participants from two samples of law enforcement intelligence professionals that had received training conducted by the Memorial Institute for the Prevention of Terrorism or by the School of Criminal Justice at Michigan State University. Participant selection centered on sworn and nonsworn officers who worked for state, tribal, and local law enforcement agencies in the United States and whose work responsibilities enabled them to serve as key informants with respect to agency intelligence practices. The design of the online survey distributed to these individuals was discussed, along with data collection procedures, response rates, and details of nonrespondent analyses. Furthermore, problems with missing data were also highlighted and a strategy for identifying and including usable submissions was presented. A description of the operationalization and measurement of study constructs, as well as the results of principal component factor and reliability analyses, was provided. Lastly, a plan for analyzing the data was presented; results of these analyses are reported in the next chapter.

Chapter 4: Results

The previous chapter presented details about the cross-sectional survey data used in this study and their measurement. This chapter reports the quantitative analyses run on the data and the results. The work is presented in three sections. First, descriptive statistics will highlight agencies' self-reported use of electronic information sharing systems. Second, descriptive and inferential statistics will address each of the two research questions in turn. Third, descriptive statistics will draw attention to agency support for the Information Sharing Environment and sharing systems more generally.

Descriptive Statistics for Electronic Information Sharing Systems Use

To gain insight into the extent of electronic information sharing systems use by state and local law enforcement agencies, the study participants were asked how often sharing systems were accessed at their agency. Table 5 provides a summary of the frequency distribution of systems access by agency size and agency jurisdiction. Almost three fourths of the total respondents indicated their agency used a sharing system on a weekly or daily basis, but only one fourth reported use on a daily basis. Among daily system users, agencies with less than 25 total sworn or nonsworn personnel were most active (50.0%). Agencies with 501-3,000 personnel made up the largest group (64.3%) to use systems on a weekly basis. Overall, three fourths of respondents from state agencies reported use on at least a weekly basis. Municipal (22.2%) and county (21.7%) agencies were the most infrequent self-reported users of sharing systems with respondents indicating access once per month or less.

Table 5: Frequencies of Electronic Information Sharing Systems Access by Agency Size and by Agency Jurisdiction (N=45)

	System use			
	Once per month or less	Once every two weeks	Once or more per week	Daily
	n	n	n	n
Agency size				
Less than 25	1	0	1	2
(%)	(25.0)	(0.0)	(25.0)	(50.0)
26-100	2	2	6	2
(%)	(16.7)	(16.7)	(50.0)	(16.7)
101-250	3	0	3	2
(%)	(37.5)	(0.0)	(37.5)	(25.0)
251-500	1	1	1	1
(%)	(25.0)	(25.0)	(25.0)	(25.0)
501-3,000	1	0	9	4
(%)	(7.1)	(0.0)	(64.3)	(28.6)
More than 3,000	1	0	1	1
(%)	(33.3)	(0.0)	(33.3)	(33.3)
Agency jurisdiction				
State	0	0	3	1
(%)	(0.0)	(0.0)	(75.0)	(25.0)
Municipal	4	2	9	3
(%)	(22.2)	(11.1)	(50.0)	(16.7)
County	5	1	9	8
(%)	(21.7)	(4.3)	(39.1)	(34.8)
Total	9	3	21	12

Note. Percentages may not total 100.0 due to rounding.

Additionally, responses to questions asking survey participants how well electronic systems have met their agencies' information sharing needs were examined to highlight the use of five systems (see Appendix C for descriptions). Table 6 shows counts and row percentages of self-reported agency use derived from a dichotomous treatment of each variable. These figures indicate most agencies in the sample use RISS.Net, Law Enforcement Online (LEO), and the Homeland Security Information Network (HSIN), but fewer agencies use the Automated Trust Information Exchange (ATIX) or FBINET. Respondents from agencies with more than 3,000

Table 6: Frequencies for Self-Reported Agency Use of Five Electronic Information Sharing Systems (N=45)

	RISS.Net		LEO		HSIN		ATIX		FBINET	
	Used	Not used	Used	Not used	Used	Not used	Used	Not used	Used	Not used
	n	n	n	n	n	n	n	n	n	n
Agency size										
Less than 25	4	0	4	0	3	1	0	4	0	4
(%)	(100.0)	(0.0)	(100.0)	(0.0)	(75.0)	(25.0)	(0.0)	(100.0)	(0.0)	(100.0)
26-100	9	3	12	0	12	0	5	7	4	8
(%)	(75.0)	(25.0)	(100.0)	(0.0)	(100.0)	(0.0)	(41.7)	(58.3)	(33.3)	(66.7)
101-250	8	0	6	2	5	3	1	7	3	5
(%)	(100.0)	(0.0)	(75.0)	(25.0)	(62.5)	(37.5)	(12.5)	(87.5)	(37.5)	(62.5)
250-500	4	0	4	0	4	0	1	3	3	1
(%)	(100.0)	(0.0)	(100.0)	(0.0)	(100.0)	(0.0)	(25.0)	(75.0)	(75.0)	(25.0)
501-3,000	12	2	14	0	13	1	5	9	7	7
(%)	(85.7)	(14.3)	(100.0)	(0.0)	(92.9)	(7.1)	(35.7)	(64.3)	(50.0)	(50.0)
More than 3,000	3	0	3	0	3	0	3	0	3	0
(%)	(100.0)	(0.0)	(100.0)	(0.0)	(100.0)	(0.0)	(100.0)	(0.0)	(100.0)	(0.0)
Total	40	5	43	2	40	5	15	30	20	25
Agency jurisdiction										
State	3	1	4	0	4	0	3	1	3	1
(%)	(75.0)	(25.0)	(100.0)	(0.0)	(100.0)	(0.0)	(75.0)	(25.0)	(75.0)	(25.0)
Municipal	18	1	17	2	16	3	3	16	6	13
(%)	(94.7)	(5.3)	(89.5)	(10.5)	(84.2)	(15.8)	(15.8)	(84.2)	(31.5)	(68.4)
County	19	3	22	0	20	2	9	13	11	11
(%)	(86.4)	(13.6)	(100.0)	(0.0)	(90.9)	(9.1)	(40.9)	(59.1)	(50.0)	(50.0)
Total	40	5	43	2	40	5	15	30	20	25

Note. Percentages may not equal 100.0 due to rounding.

personnel reported complete use of all systems. The responses for the remaining agencies were mixed. Self-reported use of all systems was higher for agencies with 250-500 and 501-3,000 personnel than smaller agencies. For example, while almost all respondents from agencies with less than 25 personnel indicated use of RISS.Net, LEO, and HSIN, none reported use of ATIX or FBINET. Similarly, state agencies reported more complete use of the five systems than municipal or county agencies. One difference between the latter groups was their uptake of FBINET, with a higher proportion of county agencies (50.0%) than municipal agencies (31.5%) using the system.

Findings for Research Question 1

The first research question asked, "Which technological, organizational, environmental factors are most likely to influence the use of law enforcement information sharing systems?" This section presents the findings for each of the study factors, organized by group. However, before reporting any statistics it is necessary to describe the selection of the inferential tests.

The dependent variable, system use, and virtually all of the explanatory factors were ordinal measures. It would, therefore, be questionable to treat ranked data as continuous because relationships between variables could be monotonic rather than linear. Nonparametric methods allow for this possibility by relaxing assumptions about measurement level — some tests allow data to be ordinal, interval, or ratio measures — and the normality of data, the latter being an important consideration when, as here, the sample size is small (Caruso & Cliff, 1997; Wilson, 1974). The following bivariate analyses use two nonparametric tests accordingly. Where the independent variable was also a study index then Spearman's ranked order correlation was used. A nonparametric version of the Pearson product-moment correlation, this test evaluates the strength of association between two variables based upon the squared differences of the ranked

responses. Interpreted in the same manner as a Pearson correlation (Hildebrand, Laing, & Rosenthal, 1977), Spearman's rho coefficient ranges from +1, a perfect positive association between ranks, to −1, a perfect negative association between ranks, while values close to zero indicate a weak association. Where the independent variable was a categorical measure then Fisher's exact test of independence was used. This test is suitable for small samples with row by column tables and enables calculation of probability values without the need to estimate unknown parameters (Agresti, 2010); unlike the chi-square statistic, it does not require a minimum amount of values for each cell (Agresti, 1990). In both cases, the null hypothesis stated there is no association between the two variables in the population. The study used a confidence level of 95 percent throughout the tests.

Technological factors. Perceived benefits were defined as the potential gains law enforcement agencies derive from using electronic information sharing systems. On average, respondents broadly agreed using a 7-point Likert-type scale (1=strongly disagree, 7=strongly agree) with statements highlighting benefits of electronic sharing systems technology (N=45, M=5.43, SD=1.11). Respondents registered slightly higher levels of agreement for items suggesting sharing systems leading to improved quality of information shared (M=5.71, SD=1.08) and increased information sharing outside their agency (M=5.53, SD=1.31) than those suggesting sharing systems lead to increased information sharing within their agency (M=5.33, SD=1.31) and secure communication of information shared (M=5.16, SD=1.33).

Hypothesis H1 states perceived benefits positively influence agency use of electronic information sharing systems. A Spearman's correlation was run to assess the relationship between perceived benefits and agency use of electronic information sharing systems (N=45).

There was a weak positive correlation between the two variables, which was statistically significant (r_s=0.369, p=0.013).

Perceived disadvantages were defined as the problems associated with law enforcement agencies' use of electronic information sharing systems. In comparison to perceived benefits, respondents were less likely to agree with statements identifying problems with sharing systems use (N=45, M=3.64, SD=1.32). While they agreed sharing systems lead to increased demands for information (M=4.42, SD=1.62) and shared data being misused (M=5.16, SD=1.33), there was less agreement with the view that the systems lead to resources being diverted away from agency priorities (M=3.51, SD=1.77) and too much information being collected (M=3.58, SD=1.74).

Hypothesis H2 states perceived disadvantages negatively influence agency use of electronic information sharing systems. A Spearman's correlation was run to assess the relationship between perceived disadvantages and agency use of electronic information sharing systems (N=45). There was a weak negative correlation between the two variables, which was not statistically significant (r_s=−0.215, p=0.156) and failed to support rejection of the null hypothesis.

Further examination of technological factors involved estimation of a partial, ordinal regression model with system use as the dependent variable (N=45). This model included perceived disadvantages as the predictor while controlling for agency size (reference category was less than 25 personnel). The chi-square statistic ($\chi 2(6)$=6.59, p=0.361) indicated the results for the model were not statistically significant. Accordingly, the model did not support rejection of the null hypothesis stating all of the regression coefficients in the model are equal to zero.

Organizational factors. Organizational readiness was defined as the amount of financial and technological resources available to support an innovation. Survey questions asked respondents (N=45) to indicate the extent to which four types of resource were a problem (1=Significant problem, 2=Somewhat of a problem, 3=Not a problem) for their agency to share information and intelligence: adequate personnel, adequate resources, adequate time, and adequate training. The mean score for all the items was 1.69 (SD=0.54) with most responses suggesting the adequacy of resources within agencies was problematic. For instance, almost half of respondents indicated adequate personnel (48.9%), adequate resources (46.7%), and adequate time (44.4%) were a significant problem. The figure for adequate training being a significant problem was slightly lower (33.3%), with most respondents (55.6%) characterizing this as somewhat of a problem.

Hypothesis H3 stated organizational readiness was a positive influence upon agency use of law enforcement information sharing systems. A Spearman's correlation was run to assess the relationship between organizational readiness and systems use. There was a weak positive correlation between the two variables, which was not statistically significant (r_s= 0.289, p=0.054) and failed to support rejection of the null hypothesis.

Top management support was defined as the commitment of leaders to create the conditions within an agency that promote an innovation. Respondents indicated their agreement (1=Strongly disagree, 7=Strongly agree) with three statements about top management and its treatment of electronic information sharing systems (M=4.76, SD=1.85). The item found to have the highest mean score stated top management considers networked information sharing systems as important to the organization (M=4.93, SD=1.86). Respondents reported slightly lower levels of agreement with respect to top management being interested in the implementation of sharing

systems (M=4.78, SD=1.92) and the view top management effectively communicated its support for sharing systems (M=4.56, SD=1.89).

Hypothesis H4 stated top management support will have a positive influence upon agency use of law enforcement sharing systems. A Spearman's correlation was run to assess the relationship between top management support and systems use. The result highlighted no relationship between the two variables (r_s=0.039, p=0.801) and failed to support rejection of the null hypothesis.

Formal linking structure was defined as a mechanism that enables organizations to reduce uncertainty by developing an awareness of events occurring in the external environment and communicating them internally. Analyses here examined responses to a survey item asking about the focus of their organization's intelligence function (N=45). The most commonly reported structure was the "all-crimes," "all-threats," and "all-hazards" intelligence function (73.3%). One fifth (22.2%) of respondents indicated their agency had a function with a more narrow specialization. Only two respondents disclosed the absence of any intelligence function.

Hypothesis H5 stated a formal linking structure will have a positive influence upon agency use of law enforcement information sharing systems. Fisher's exact test of difference was run to assess the relationship between formal linking structure and systems use. The result indicated there was no relationship between the two variables (p=0.158) and failed to support rejection of the null hypothesis.

Environmental factors. Threat perception was defined as the belief that a homeland security incident is likely to take place within an agency's jurisdiction. Eight survey items asked respondents to indicate the likelihood (1=Very unlikely, 2=Unlikely, 3=Likely, 4=Very unlikely) of specific terrorist events occurring in their state in the next five years (N=45). The events

designated as likely or very likely to take place were cyber terrorism (86.6%), conventional explosive incidents (77.8%), and incidents involving military weapons (57.8%). The events reported as unlikely or very unlikely to occur were nuclear or radiological incidents (73.4%), agro-terrorism involving animal disease nontransferable to humans (64.4%), and chemical events (62.2%). Beliefs about the remaining two items were less clear cut: roughly a half of respondents thought it unlikely or very unlikely a biological incident would happen (53.3%), while a similar amount (51.1%) suggested agro-terrorism involving food is likely or very likely to take place. The mean score for the threat index was 2.53 (SD=0.55).

Hypothesis H6 stated threat perception will positively influence agency use of law enforcement information sharing systems. A Spearman's correlation was run to assess the relationship between threat perception and systems use. The result indicated no relationship between the two variables (r_s=0.095, p= 0.535) and failed to support rejection of the null hypothesis.

Coercive pressures were defined as formal and informal pressures that powerful organizations exert on dependent organizations. In particular, the single dichotomous variable of interest measured the influence of technical requirements for agency handling of criminal investigations records established by 28 CFR Part 23 guidelines (N=45). Almost all of the respondents (93.3%) indicated their agency had taken steps to ensure compliance.

Hypothesis H7 stated coercive pressures will positively influence agency use of law enforcement information sharing systems. Fisher's exact test of difference was run to assess the relationship between coercive pressures and systems use. The result indicated there was no relationship between the two variables (p=0.338) and failed to support rejection of the null hypothesis.

Mimesis was defined as an organization's imitation of others in response to uncertainty. Analysis centered upon responses to the survey item asking about the extent (1=Never, 2=Sometimes, 3=Often) a respondent's agency modeled its information sharing activities upon other organizations that were viewed as being successful (N=45). Most respondents (60.0%) indicated their agency sometimes modeled sharing activities upon others, but nearly a third (31.1%) suggested this practice often occurred.

Hypothesis H8 stated mimesis will positively influence agency use of law enforcement information sharing systems. Fisher's exact test of difference was run to assess the relationship between mimesis and systems use. The result indicated there was no relationship between the two variables ($p=0.183$) and failed to support rejection of the null hypothesis.

Normative pressures were defined as isomorphic pressures arising from professionalization via interchanges between members of an occupational group that establish work definitions and procedures. Professionalization was assessed here through the use of a single dichotomous variable indicating whether agencies in the sample had been accredited through the Commission of the Accreditation of Law Enforcement Agencies (CALEA). One half of agencies were discovered to have CALEA accreditation.

Hypothesis H9 stated normative pressures will positively influence agency use of law enforcement information sharing systems. Fisher's exact test of difference was run to assess the relationship between normative pressures and systems use. The result indicated there was no relationship between the two variables ($p=0.150$) and failed to support rejection of the null hypothesis.

Findings for Research Question 2

The second research question asked, "Is there an association between agencies' use of

sharing systems and the exchange of law enforcement intelligence and information?" To examine the extent of agencies' law enforcement intelligence exchanges, respondents were asked a series of close-ended questions about how frequently their agency produced different analytical products and their assessment of the usefulness of products they received from other agencies. This section presents descriptive statistics for agencies' creation and receipt of intelligence products, and the results of bivariate analyses testing their covariance with agencies' use of electronic information sharing systems.

Creation of intelligence products and system use. In the case of law enforcement intelligence creation, respondents were asked how frequently (never, monthly, weekly, daily, upon request) their agencies generated five generic products: bulletins containing information about emerging threats, assessments about threats posed, location vulnerability, evaluations of risk, and actionable alerts about terrorist threats (Carter, 2009). Table 7 shows nearly a third of responding agencies produced bulletins and alerts on a daily basis, one fourth of agencies produced them on a weekly basis, and another fourth of agencies produced them upon request. In contrast, threat assessments (55.6%), vulnerability assessments (68.9%), and risk assessments (64.4%) were mostly generated upon request, while approximately one fifth of agencies did not produce them at all.

Cross tabulations for intelligence production and agency characteristics also revealed mixed patterns of activity between groups. Responding agencies with fewer than 25 (75.0%) or between 500 and 3,000 (64.3%) personnel produced most bulletins on a daily basis, while agencies with between 26 and 100 (41.6%) or more than 3,000 (100.0%) personnel created most bulletins upon request. Agencies with between 101-250 personnel produced bulletins in equal measure on a weekly (25.0%), daily (25.0%), and by request (25.0%) basis, while agencies with

between 251-500 personnel produced most bulletins on a weekly basis (75.0%).

Table 7: Frequency Distributions of Intelligence Products Created by Responding Agencies (N=45)

Product	Never n	Monthly n	Weekly n	Daily n	Upon request n
Bulletins	2	5	11	15	12
(%)	(4.4)	(11.1)	(24.4)	(33.3)	(26.7)
Threat assessments	8	5	3	4	25
(%)	(17.8)	(11.1)	(6.7)	(8.9)	(55.6)
Vulnerability assessments	8	3	1	2	31
(%)	(17.8)	(6.7)	(2.2)	(4.4)	(68.9)
Risk assessments	9	2	4	1	29
(%)	(20.0)	(4.4)	(8.9)	(2.2)	(64.4)
Alerts	1	3	12	13	16
(%)	(2.2)	(6.7)	(26.7)	(28.9)	(35.6)

Note. Percentages may not total 100.0 due to rounding.

Similar reports emerged for the creation of alerts. Agencies with 26 and 100 (75.0%) or between 501-3,000 (42.9%) personnel produced most alerts daily, while agencies with between 26-100 (58.3%) or between 101-250 (37.5%) or more than 3,000 (66.7%) personnel generated alerts upon request. Again, agencies with between 251-500 (75.0%) personnel produced most alerts weekly.

At least half of all agencies of all sizes produced threat, vulnerability, and risk assessments by request. The only exceptions were agencies with fewer than 25 personnel that produced threat assessments on a daily basis (50.0%), and agencies with between 26-100 workers that never produced threat (33.3%), vulnerability (25.0%), and risk (33.3%) assessments at all.

In terms of jurisdiction, well over half of state, municipal, and county agencies produced threat, vulnerability, and risk assessments upon request while about a third of municipal agencies

never produced threat assessments. Half of the responding state agencies produced bulletins daily and alerts weekly. Roughly a third of county agencies produced bulletins and alerts daily or by request. Nearly a third of municipal agencies reported the generation of bulletins and alerts weekly or by request.

Table 8: Agency Creation of Intelligence Products and Electronic Information Sharing Systems Use (N=45)

	System use							
	Monthly		Every 2 weeks		Weekly		Daily	
Product	n	(%)	n	(%)	n	(%)	n	(%)
Bulletin								
Daily	3	(33.3)	0	(0.0)	7	(33.3)	5	(41.7)
Upon request	3	(33.3)	1	(33.3)	7	(33.3)	1	(8.3)
Threat assessment								
Daily	0	(0.0)	0	(0.0)	1	(4.8)	3	(25.0)
Upon request	8	(88.9)	1	(33.3)	12	(57.1)	4	(33.3)
Vulnerability assessment								
Daily	0	(0.0)	0	(0.0)	1	(4.8)	1	(8.3)
Upon request	8	(88.9)	1	(33.3)	14	(66.7)	8	(66.7)
Risk assessment								
Daily	0	(0.0)	0	(0.0)	1	(4.8)	0	(0.0)
Upon request	7	(77.8)	1	(33.3)	13	(61.9)	8	(66.7)
Alert								
Daily	3	(33.3)	0	(0.0)	6	(28.6)	4	(33.3)
Upon request	3	(33.3)	1	(33.3)	8	(38.1)	4	(33.3)
Total	9		3		21		12	

Table 8 displays the frequencies for agency access to electronic information sharing systems against the frequencies for daily or by request agency intelligence production. The figures suggest that among reporting agencies the pattern of bulletin production was similar to that of alert production for all frequencies of sharing system use. As a result, despite a higher number of agencies that indicated daily bulletin production allied with daily system use, the pattern of bulletin production was similar to that of alert production irrespective of sharing

system use. The frequencies of threat, vulnerability, and risk assessment production were also similar across use categories with most production reported as occurring on request. In relative terms, most creation of assessments coincided with monthly or less frequent use of sharing systems.

Spearman's correlations were run to test the null hypothesis that the correlation between agency generation of intelligence products and agency access to sharing systems is equal to zero in the population (N=45). The test results indicate there is no relationship between the production of bulletins and system access (r_s=−0.086, p=0.576), production of threat assessments and system access (r_s=−0.242, p=0.110), production of vulnerability assessments and system access (r_s=−0.064, p=0.674), production of risk assessments and system access (r_s=0.012, p=0.935), and production of alerts and system access (r_s=0.049, p=0.749). Consequently, the results did not justify rejection of the null hypothesis.

Receipt of intelligence products and system use. Respondents were also asked how frequently (Very infrequently, Infrequently, Frequently, Very frequently) they received intelligence products generated by other agencies with three types of information: new information that agency personnel knew little about, information about threats to officer safety, and actionable information enabling better decisions or intervention in a threat. Table 9 presents the counts reported by agency respondents. Most individuals indicated their agencies received intelligence products with information about officer safety threats very frequently (48.9%) or frequently (37.8%). The findings for the remaining products were mixed. Three fifths of respondents (60.0%) indicated intelligence products their agencies frequently received included new information, but a fifth stated products infrequently provided new information. Receipt of intelligence products with actionable information was a less common event with only a third

(37.8%) of respondents indicating this happened frequently while two fifths (40.0%) of respondents reporting this happened infrequently.

Table 9: Frequency Distributions of Intelligence Received by Agencies (N=45)

Intelligence	Very infrequently n	Infrequently n	Frequently n	Very frequently n
New information	3	9	27	6
(%)	(6.6)	(20.0)	(60.0)	(13.3)
Officer safety threats	1	5	17	22
(%)	(2.2)	(11.1)	(37.8)	(48.9)
Actionable information	4	18	17	6
(%)	(8.9)	(40.0)	(37.8)	(13.3)

Note. Percentages may not equal 100.0 due to rounding.

Cross tabulations revealed respondents from agencies with between 26-100 personnel (75.0%) or between 501-3,000 personnel (71.4%) reported frequent receipt of intelligence products with new information. Nearly two thirds of respondents from municipal (63.2%) and county (63.6%) agencies also indicated products frequently contained new information, but three fourths (75.0%) of state agencies characterized this as an infrequent event.

With respect to products with information about officer safety threats, respondents from agencies with between 26-100 personnel (75.0%) or between 101-250 personnel (62.5%) indicated they received this intelligence very frequently while individuals from agencies with between 501-3000 personnel (57.1%) said this occurred frequently. Roughly two thirds of municipal agencies (68.4%) obtained officer safety threat information very frequently and about three fifths of county agencies (58.8%) received this information frequently.

Lastly, three fourths of respondents from agencies with less than 25 personnel reported receipt of products with actionable information as either a very frequent or frequent event, but

three fourths of respondents from agencies with between 26-100 personnel marked this as an infrequent occurrence.

Table 10 shows the frequencies of agency use to sharing systems against intelligence products that agencies received frequently and very frequently. Most respondents indicated their agency received officer threat information very frequently, irrespective of the rate of system use. For example, daily system use (50.0%) and use monthly or less (44.4%) both coincided with very frequent receipt of threats to officer safety. This pattern held for new information and actionable information, except respondents instead reported receipt of products with these information types on a frequent basis.

Table 10: Agency Receipt of Intelligence and Electronic Information Sharing Systems Use (N=45)

	System use							
	Monthly		Every 2 weeks		Weekly		Daily	
Intelligence	n	(%)	n	(%)	n	(%)	n	(%)
New information								
Frequently	4	(44.4)	2	(66.7)	12	(57.1)	9	(75.0)
Very frequently	2	(22.2)	1	(33.3)	2	(9.5)	1	(8.3)
Officer safety threats								
Frequently	1	(11.1)	1	(33.3)	10	(47.6)	5	(41.7)
Very frequently	4	(44.4)	2	(66.7)	10	(47.6)	6	(50.0)
Actionable information								
Frequently	4	(44.4)	0	(0.0)	6	(28.6)	7	(58.3)
Very frequently	1	(11.1)	0	(0.0)	3	(14.3)	2	(16.7)
Total	9		3		21		12	

Spearman's correlations were run to test the null hypothesis that the correlation between agency receipt of intelligence products and agency access to sharing systems equals zero in the population (N=45). The test results indicate there is no relationship between the receipt of new information and system access (r_s=−0.021, p=0.890), receipt of officer safety threats information

and system access (r_s=0.112, p=0.463), and receipt of actionable information and system access (r_s=0.183, p=0.230). As such, these results did not justify rejection of the null hypothesis.

Table 11: Summary of Bivariate Tests of Study Variables and Electronic Information Sharing Systems Use (N=45)

Variable	Coefficient	*p*-value	Conclusion
TOE factors			
Perceived benefits	.369	.013	Significant
Perceived disadvantages	−.215	.156	Not significant
Organizational readiness	.289	.054	Not significant
Top management support	.039	.801	Not significant
Formal linking structure		.158	Not significant
Threat perception	.095	.535	Not significant
Coercive pressures		.338	Not significant
Mimesis		.183	Not significant
Normative pressures		.150	Not significant
Agency creation			
Bulletins	−.086	.576	Not significant
Threat assessments	−.242	.110	Not significant
Vulnerability assessments	−.064	.674	Not significant
Risk assessments	.012	.935	Not significant
Alerts	.049	.749	Not significant
Agency receipt			
New information	−.021	.890	Not significant
Officer safety threats	.112	.463	Not significant
Actionable information	.183	.230	Not significant

Note. Results of the Fisher's exact test do not include a coefficient since the p-value is calculated directly.

Other Findings

This section reports the responses to additional survey questions. These items examined participants' perceptions of agency activities that aligned with the Information Sharing Environment and indications of agency support for the use of electronic information sharing systems.

Support for the Information Sharing Environment. The study survey included a question asking participants to indicate how prepared (Not at all, Not prepared, Somewhat prepared, Prepared, Very prepared) their agency was for terrorist or criminal extremist threats in their region (N=45). Nearly half of respondents (48.9%) stated their agency was prepared, less than a third of respondents (28.9%) stated their agency was somewhat prepared, and less than a fifth of respondents (17.8%) was not prepared. Of those agencies reported to be prepared, most agencies had between 25-100 personnel (27.3%) or 501-3,000 personnel (36.4%); municipal and county agencies were most likely to be described as being prepared (45.5%).

Furthermore, respondents were asked to use a 7-point Likert-type scale (1=Strongly disagree, 7=Strongly agree) to indicate their agreement with the statement that their agency is part of the Information Sharing Environment. The mean score and standard deviation for this item was 5.18 and 1.30 respectively. Taken together, the findings suggest most respondents believed their agency was actively taking steps to prepare for terrorist events and participating in the Information Sharing Environment.

Survey items also asked about sources of external funding that agencies received in support of information sharing functions, but outside their normal operating budgets. More than half of respondents indicated their agency received no such funding (52.5%), with all agencies with less than 25 personnel and three quarters (77.8%) of agencies with between 26-100 personnel falling into this category. The responses also suggested county agencies were in a similar situation, with roughly two thirds (61.9%) of respondents indicating a lack of external funding. On the other hand, approximately a third of respondents reported that their agency was a recipient of federal funding (32.5%). These agencies tended to be larger with between 501-3,000 personnel (46.2%) or more than 3,000 personnel (66.7%). State (66.7%) agencies, rather

than municipal (35.3%) or county (25.5%) agencies, fell into this category.

Advancing the use of electronic information sharing systems. Two items in the survey asked respondents about the advocacy of electronic information sharing systems. The first question asked respondents (N=44) if there was an individual who enthusiastically championed the adoption of information sharing systems in their organization. Almost all of the respondents (95.5%) acknowledged there was a champion. The second question asked respondents (N=42) what role the champion had within the agency. Half of the respondents indicated the champion was a manager, while the remainder reported the champion as being either the chief (23.8%) or a worker (26.2%). Thus, the study data suggest champions emerged from different levels of the organizational hierarchy.

To explore the degree of instructional support agency workers received within their organization, a close-ended question prompted respondents (N=44) to indicate what the main source of training was for using sharing systems. The modal category was "Self" (36.4%), meaning workers were left to learn how to use the systems by themselves. The remaining responses highlighted the use of training employees (20.5%) and outside professionals (20.5%), while the least frequently reported sources included a coworker or supervisor (13.6%) and online professional training (9.1%).

Cross tabulations of agency size and system training revealed the largest amount of self-taught workers came from agencies with between 26-100 personnel, while only agencies with more than 3,000 personnel relied on other methods of training. Likewise, the most common response to a second question asking about the amount of training agency workers received for using sharing systems (N=43) was "Too little" (76.7%), with less than a fourth (23.3%) indicating this amount was "About right."

Summary

This chapter began by reporting descriptive statistics for agencies' self-reported use of electronic information sharing systems. The results suggested that most agencies use sharing systems on at least a weekly basis and cross tabulations showed large and small agencies were frequent users of sharing systems. Further analyses indicated high numbers of agencies use the RISS.Net, LEO, and HSIN systems but fewer reported use of ATIX and FBINET. Agencies operating at the state level most frequently reported using all of the systems.

Descriptive statistics and the results of nonparametric tests were reported for the research questions. Results from the analyses for the first research question provided no evidence that the technological, organizational, and environmental factors identified in the study were statistically related to agency use of electronic information sharing systems. Although perceived disadvantages, organizational readiness, formal linking structure, and normative pressures approached statistically significant levels, only perceived benefits were associated with system use at the bivariate level and the results of a partial ordinal regression analysis failed to indicate perceived benefits were a meaningful predictor when controlling for agency size.

Descriptive analyses for the second research question addressed agencies' production and receipt of law enforcement intelligence. The results suggest agencies generate intelligence products at different rates. Threat assessments, vulnerability assessments, risk assessments, and alerts were generated primarily upon request while bulletins and alerts were created daily, weekly, or by request. Agencies also received information about officer safety threats at a more frequent rate than those with new information or actionable information. Nonparametric tests indicated there was no systematic relationship between agency use of sharing systems and intelligence production, or between system use and the receipt of intelligence.

Lastly, findings were presented for agency support of the Information Sharing Environment and the promotion of electronic sharing systems within responding organizations. While reported levels of preparedness were mixed and the majority of agencies stated they received no external funding to support information sharing functions, study participants did view their agencies as being part of the Information Sharing Environment. Furthermore, the main advocates of system adoption within agencies were found to occupy roles across the organizational hierarchy. The main source of training for use of sharing systems was the user, although large agencies relied upon professionals from inside or outside the organization to train workers. Most participants characterized this training as being too little.

The next chapter will discuss these findings in relation to previous studies. It will also present the implications for practice and future research.

Chapter 5: Discussion

The previous chapter reported the results of descriptive and inferential analyses run on the study data. This chapter begins with a summary of the research and then reviews the main findings and their implications. Additionally, limitations of the research are discussed to highlight concerns that warrant attention when assessing the study results. The final sections consist of recommendations for further research and closing remarks.

Summary of the Research

The goal of this study was to examine law enforcement agencies' use of electronic systems designed for sharing information about threats to public safety. An integral part of the Information Sharing Environment created after the attacks of 9/11, these systems provide the means for agencies to exchange information with other government organizations in order to prevent or mitigate threats directed at communities within the United States. Therefore, the study sought to develop an explanation for the variation in their use and to better understand what these systems contribute to law enforcement intelligence practices.

To guide the research, Tornatzky and Fleischer's (1990) technology-organization-environment (TOE) framework was used in conjunction with the diffusion of innovations theory (Rogers, 2003) and institutional theory (DiMaggio & Powell, 1983) to identify factors within agencies and their external environment that could explain agency use of sharing systems. A review of research looking at innovations within police agencies also highlighted salient factors. These explanatory factors included aspects of the technology itself (perceived benefits and perceived disadvantages), agency characteristics (organizational readiness, top management support, and formal linking structure), and environmental pressures that elicit responses from agencies (threat perception, coercive pressures, mimesis, and normative pressures). The

subsequent model reflected the view that innovation within law enforcement agencies is based upon technical-rational considerations of organizational processes and an institutional need to conform with stakeholders' expectations regarding legitimate police practices.

The study used data collected as part of a project sponsored by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) to advance an understanding of current law enforcement intelligence practices within agencies. This involved the distribution of a self-administered web survey to law enforcement intelligence professionals who had participated in trainings conducted by the Memorial Institute for the Prevention of Terrorism (MIPT) or the School of Criminal Justice at Michigan State University (MSU). Collection of respondent data was performed using an online survey provider. The study data consisted of 335 responses from individuals who were employed at 147 local, county, or state law enforcement agencies. However, the number of cases was reduced to ensure there was a single response for each agency and to account for missing data arising from incomplete submissions. The study analyses involved the generation and evaluation of descriptive and inferential, nonparametric statistics for 45 local, county, or state agencies.

Discussion of the Main Findings

The study findings suggested that a majority of responding agencies are using law enforcement information sharing systems at least weekly. In particular, almost all agency representatives indicated that of five federal systems capable of conveying Sensitive But Unclassified information, they use the Regional Information Sharing Systems Network (RISS.Net), Law Enforcement Online (LEO), and the Homeland Security Information Network (HSIN) while fewer than half reported using the Automated Trusted Information Exchange (ATIX) and the Federal Bureau of Investigation Network (FBINET). These results mirrored

other research with the exception of agencies' use of HSIN, which previously appeared to be underutilized (Carter et al., 2012). This pattern could be explained by the age of systems like RISS.Net and LEO, which have been in existence longer, and that they provide unique information to users such as data about violent crime (*RISS Overview*, n.d.) and suspicious activities (*HSIN Features*, n.d.).

Upon further examination it appeared small agencies with 100 total personnel or less, as well as larger agencies, frequently accessed sharing systems. This finding was somewhat at odds with literature identifying the largest police organizations as adopters of data management technologies (Weisburd et al., 2003). It is possible that a lower agency caseload, an organizational climate with fewer formal rules, and a willingness to innovate facilitate the uptake of sharing systems among smaller agencies (Akbulut et al., 2009). In contrast, state agencies more commonly reported use of, and access to, all five federal systems compared with municipal and county agencies. This trend reflects the view that in a post 9/11 environment state agencies have a central role in developing homeland security initiatives along with assisting local and tribal agencies in matters relating to intelligence activities, critical infrastructure protection, and emergency management planning and response (Carter & Carter, 2009a; Foster & Cordner, 2006; Freilich, Chermak, & Simone, 2009; Graphia-Joyal, 2012; Ratcliffe & Walden, 2010).

Research question 1. *Which technological, organizational, and environmental factors are most likely to influence agency use of sharing systems?*

The results indicate that the study factors fail to explain variation in law enforcement agencies' use of information sharing systems. That there were so many null findings was surprising given their divergence from previous research. This section presents and interprets these outcomes.

The study examined two technological factors, perceived benefits and perceived disadvantages associated with the use of electronic information sharing systems. The findings suggested law enforcement workers recognize the use of these systems is both beneficial and disadvantageous. For example, study participants agreed that system use had led to increased sharing of information outside their agency and improved quality of information being shared. This is consistent not only with the intended purpose of information sharing networks but also previous studies that found agency use of sharing systems depends upon users perceiving them to be useful (Akbulut et al., 2009; Akbulut-Bailey, 2011; Saviak, 2007). On the other hand, participants concurred less with the view that system use led to the secure communication of shared information. This finding was unexpected because authorities state the implementation of security protocols, such as registration and authentication processes, is intended to build trust in sharing systems for the community of practitioners who use them (*Mobilizing Information to Prevent Terrorism*, 2006; *President's National Strategy on Information Sharing*, 2007).

In terms of disadvantages, participants were less likely to agree that sharing system use resulted in the diversion of resources away from agency priorities or too much information being collected. But they also indicated system use led to increased demands for information, although they were not asked where these requests originated from or what purpose they served. These findings are consistent with the view that law enforcement information networks support agencies' ability to more efficiently handle information and serve requests from external institutions seeking knowledge to manage risks (Ericson & Haggerty, 1997). More noticeable, however, was their agreement with the view that system use leads to the misuse of shared information. Scholars have documented similar findings in both mainstream government (Dawes, 1996) and police organizations (Akbulut, 2003), and the current findings also indicated

law enforcement remains sensitive to the threat of mishandled information.

Researchers have drawn attention to the perceived benefits as a strong predictor of sharing system use. Yet the results here only highlighted a weak association between variables. One explanation for this outcome rests with the study measures of which were few in number and focused on advantages linked with organizational problem solving. Other studies, on the other hand, have also captured technical dimensions of information sharing expected to improve productivity and reduce costs (e.g., reductions in paperwork and information duplication) as well as political benefits of interagency sharing like improved agency image (Akbulut-Bailey, 2011; Dawes, 1996). It is quite possible, therefore, this study failed to adequately consider salient benefits of sharing system use.

Alternatively, law enforcement workers may simply view systems that transmit Sensitive But Unclassified information as having less utility than criminal justice information systems that provide access to official information such as individual fingerprints or criminal histories. This perspective implies law enforcement information sharing systems are functionally distinct and are characterized less by their technical capabilities (e.g., processing, transmitting, and storing data) than by the specialized information they provide access to.

Organizational readiness, top management support, and formal linking structure did not appear to be associated with sharing system use. First, participants reported varying degrees of readiness in relation to sharing information and intelligence. Approximately half of them indicated their agency had a significant problem finding adequate personnel, resources, and time for sharing activities. In addition, the majority of participants suggested the amount of training they received for using sharing systems was too little. Previous work has highlighted concerns about the continuing availability of resources for law enforcement intelligence activities (Carter

et al., 2012) and, more specifically, a relationship between agencies' IT capability and electronic sharing (Akbulut et al., 2009; Akbulut-Bailey, 2011). It follows that slack resources promote implementation of a technological innovation because agencies can acquire new computers, and find and train additional staff where needed. On the other hand, federal sharing networks may instead place relatively small technical demands on agencies since they are web portals accessed via the Internet. Moreover, control over information notifications pushed from sharing systems to agencies could encourage participation by organizations with fewer resources (Rocheleau, 2006).

Second, almost all responding agencies were said to have an intelligence function with the majority of these designed to respond to all crimes, all threats, and all hazards. This was surprising because past research has suggested the presence of an intelligence function within agencies, especially those engineered for intelligence-led policing, to be the exception rather than the rule (Carter et al., 2012). The results here found agencies with this type of formal linking structure use electronic information sharing systems, but not necessarily on a frequent basis. This is understandable if one assumes sharing systems are simply one source of electronic information, in addition to agency records including citizen reports, criminal justice records, and open source information, used to develop prevention information for confronting terrorist or criminal threats, and strategic information intended to assist agency planning (Carter, 2009). It follows that, irrespective of their ability to span organizational and jurisdictional boundaries, sharing systems may complement the goals of an intelligence function while being only one type of electronic resource that workers use for intelligence-related tasks (Carter & Carter, 2009a).

Third, while participants indicated their agency's top management view sharing systems as important to the organization, top management were reported to be less interested in their

implementation and did not effectively communicate support for them. This finding was surprising because scholars have drawn attention to the importance of leadership commitment during the adoption (Saviak, 2007) and implementation stages (Akbulut et al., 2009; Akbulut-Bailey, 2011) of sharing systems. That only a fourth of respondents identified the agency leader as a champion of electronic sharing systems instead offered support to the argument that adoption and subsequent use of electronic systems might be attributed to a managerial decision as opposed to an agency policy initiative (Mullen, 1996). This, in part, could explain variation in levels of top management support for sharing systems across agencies in the study sample.

The findings for environmental factors were also mixed. For instance, most respondents indicated cyber terrorism, conventional explosive incidents, and incidents involving military weapons were likely to occur in their state within the next five years. But threat perception failed to explain agencies' use of electronic systems to share information. This result was unexpected because several studies have highlighted perceived risk as a predictor of agencies' participation in homeland security preparedness activities (Burruss et al., 2010; Davis et al., 2004; Giblin et al., 2014; Haynes & Giblin, 2014; Schafer et al., 2009). On the other hand, information sharing is only one of many activities intended to enhance preparedness levels. Given that nearly half of the respondents indicated their agencies were unprepared for terrorist or criminal extremist threats in their region, it is possible agencies are instead directing their efforts toward local emergency planning and coordination with community partners (Schafer et al., 2009).

In terms of institutional pressures, half of the agencies in the sample had CALEA accreditation but this action was not significantly associated with system use. This was a departure from research suggesting accreditation, as an indicator of normative pressures,

promotes practices intended to address concerns of external stakeholders and signal membership to a progressive network (Giblin, 2004, 2006; Skogan & Hartnett, 2005). Likewise, while most respondents indicated their agency modeled its sharing practices based upon other organizations and complied with 28 CFR Part 23 guidelines, neither mimesis nor coercive pressures were found to be associated with system use.

Problems with measurement validity could explain the divergence between previous and present findings. This issue is discussed separately as a study limitation. Alternatively, and in line with the findings, it is possible that institutional pressures do not have a direct effect upon sharing system use. This would be consistent with the technical-rational view that resources and experience with systems (i.e., perceived benefits across time) are more likely to explain their implementation (Skogan & Hartnett, 2005). Professionalization, in the form of CALEA accreditation, might therefore be indicative of a general commitment to improving organizational performance (Mastrofski & Uchida, 1996).

Research question 2. *Is there an association between agencies' use of sharing systems and the exchange of law enforcement intelligence and information?*

The results found law enforcement generated intelligence bulletins, threat assessments, vulnerability assessments, risk assessments, and alerts at different rates. Most responding agencies produced assessments upon request, or not at all. In contrast, daily creation of bulletins appeared to be most common while bulletins were produced daily, weekly, or by request. The findings highlighted similar variation for types of intelligence received by agencies. Respondents indicated frequent receipt of products created by other agencies with information about threats to officers and, to a lesser extent, new information. They were also divided in their assessments about the regularity of actionable information received with most suggesting there

was infrequent sharing of products containing this information type. Previous researchers have also highlighted similar patterns with agencies reporting selective production of intelligence (Carter et al., 2012).

There did not appear to be any association between agency production of intelligence and agencies' use of sharing systems, or agency receipt of intelligence and system use. The most plausible explanation for these outcomes is agencies create products in different ways with different organizational goals in mind. Some agencies may use intelligence to prevent crime, while others seek to use intelligence for planning purposes (Carter, 2011). If so, it becomes important to consider what information sources are used to construct different intelligence and to whom they are disseminated (Bullock, 2013; Carter et al., 2012). Furthermore, an emphasis on quality products may require workers to take longer and evaluate different sources of information (Carter, 2009; Carter et al., 2012). This implies they are likely to access different databases rather than simply rely upon federal networks. In turn, slower production coupled with selective distribution will likely influence workers' perceptions of how frequently other agencies' share intelligence and information.

Implications for Practice

Since the events of 9/11 there have been calls to enhance information sharing between agencies across all levels of government. Proponents of the Information Sharing Environment argue electronic networks provide the means for government workers to share information in a more effective and timely manner so that they can take steps to protect citizens and critical infrastructure from criminal and terrorist threats. Therefore, these systems transcend organizational and jurisdictional boundaries, promote interagency collaboration, and signal a

willingness on the part of departments to release information that law enforcement partners can use to strengthen public safety (Gil-Garcia et al., 2005).

This study explored law enforcement agencies' use of electronic sharing systems and its findings will be of interest to individuals with an interest in homeland security and law enforcement intelligence in the United States. Researchers may also find this work useful because of the intersections between computer technology, law enforcement intelligence, and homeland security, subjects that warrant further investigation within the criminal justice field. In this case the conceptualization of electronic sharing, which explicitly identifies concepts central to intelligence activities, and the study findings, which appear to both support and contradict the conclusions of previous studies, could guide future empirical research.

For agency administrators, the study provides insight into how frequently law enforcement agencies of different sizes and jurisdiction types are using federal networks capable of sharing Sensitive But Unclassified information. The data suggest that agencies, both large and small, are leveraging these information technologies. State agencies were found to be especially active systems users and produce a range of intelligence products. Researchers have indicated that state agencies occupy a position in the ISE that enables workers from these organizations to reach out to local, tribal, as well as federal counterparts (Carter & Carter, 2009a; Foster & Cordner, 2006; Graphia-Joyal, 2012; Schaible & Sheffield, 2012). It follows that administrators at municipal or county agencies in need of assistance may liaise with state agencies in order to draw upon the latter's experience with sharing systems and knowledge of other intelligence practices.

It is reasonable to expect that in agencies where workers access information sharing networks infrequently if at all, administrators are concerned about the consequences of more

extensive system use. Indeed, in line with previous work (Carter & Carter, 2009a; Carter et al., 2012; Chermak et al., 2013), the findings point to limited external funding for information sharing activities and worries about a lack of threat preparedness. On the other hand, it is interesting to note the extent that representatives of agencies using sharing networks identified their organization as being part of the Information Sharing Environment. In tangible terms this means having access to an improved quality of information for the purposes of making operational and strategic decisions, although sharing participation is likely lead to other organizations requesting information. Overall, these findings will offer administrators a degree of encouragement with regard to the use of sharing networks.

Policymakers and persons maintaining the federal networks will also be interested to learn the extent of system use by agencies. In most cases, agencies reported practices that align with national guidelines. These included access to multiple sharing systems, the presence of an intelligence function within the agency, and the use of 28 CFR Part 23 guidelines for guiding the operation of information sharing systems (GIWG, 2003). The finding that workers did not believe system use has caused resources to be diverted away from agency priorities or excessive amounts of information being collected also suggests agency workers are mindful of what information they gather and share. However, training in the use of sharing systems is an issue that could undermine sharing system use. At a time when there is uncertainty about the sustainability of homeland security funding, one solution would be for federal authorities to review, and where necessary provide, instructional materials to support learning of sharing systems. This is likely to be especially important for agencies that cannot afford to invest in professional training for its workforce.

The current literature stresses the importance of practitioners having trust in the electronic networks if they are to share information and intelligence products (*Creating a Trusted Network*, 2003; GIWG, 2003; *Mobilizing Information to Prevent Terrorism*, 2006). The study findings suggest workers see sharing benefits derived from agency use of the systems, but they are well aware that shared information can be misused. This suggests law enforcement workers recognize the need for intelligence practices to uphold civil and privacy rights of individuals (Carter, 2010). Another implication, however, is technological safeguards are unlikely to compensate for human error and agencies could remain reluctant to disseminate information. For policymakers, there remains a need to stress interagency sharing offers achievable benefits to agencies and the wider community, and its risks are manageable (Dawes, 1996; Dawes et al., 2009; GIWG, 2003; Pardo et al., 2008).

Another finding was senior managers within agencies consider electronic systems to be important for information sharing but do not necessarily communicate this belief. The data indicate that in most agencies the champions of sharing systems are either middle managers or line workers. Consequently, it is possible that the use of these systems rests upon a managerial decision rather than an organizational directive that makes clear system use supports the agency mission. The perceived absence of top management support and clear goals present a barrier to electronic information sharing because many workers interpret a wavering commitment to the practice and what benefits it should yield (Gil-Garcia et al., 2007). This result may lead administrators to assess their agency's vision for intelligence and information sharing, and whether there are processes in place that support a sharing culture and clarify organizational outcomes (Carter, 2009). For researchers, the idea of champions residing at lower levels of the

organizational hierarchy could stimulate work that contrasts bottom-up and top-down innovation within police organizations.

This study used Tornatzsky & Fleischer's (1990) TOE framework to integrate different theoretical explanations for organizational innovation. This approach is consistent with the view that workers' beliefs about a technology, agency structure and processes, and characteristics of the external environment are likely to impact agency adaptation. In particular, the examination of isomorphic pressures builds upon other work that suggests institutional theory is relevant to our understanding of policing practices. Yet the absence of statistically significant results calls into question the adequacy of the proposed model and its constituent theories for explaining agency use of electronic information sharing systems. The data suggested perceived benefits of systems may make a difference to sharing practices, but workers' ability to recognize them does not explain access to the systems. This finding could serve as a starting point for further investigation into agency use of sharing systems and the production of intelligence products.

Study Limitations

The study has shortcomings that will have influenced the results. This section identifies and explains the main limitations impacting the research.

Sampling strategy. The study used two purposive samples of individuals who attended trainings organized by two separate organizations. A nonrandom sampling strategy introduces bias because some individuals are less likely to be included than others and this in turn reduces the ability to generalize findings from the samples to the population from which they are supposedly drawn.

In this instance, the goal was to identify law enforcement workers who were familiar with agency intelligence practices and that could serve as informants. However, the individuals who

attended trainings were only a subset of agency workers who could have attended. One reason why individuals did not attend was because their agencies, especially those with fewer workers, could not justify their absence. For example, the sampling frames (reported in Chapter 3) included a total of nine tribal agencies and no representative from any of these agencies responded to the survey. Although these types of agency are relatively few in number compared to their municipal counterparts (Reaves, 2011a), they are still an important segment of local law enforcement and the law enforcement intelligence community (Carter, 2009; Carter et al., 2012; Reaves, 2011b). Yet the study findings cannot address their information sharing practices.

Unless researchers examining law enforcement intelligence practices have enough resources to sample police organizations at random, sample selection will remain a challenge. Any project relying on a random sample is likely to require a large number of agencies in order to identify enough organizations that collect and share information for analytic purposes. Use of a police directory might provide an initial list from which to make random selections, but this would require additional steps to reach individuals within the agencies who are able to provide accurate information. An alternative may be to approach an association whose members routinely handle and analyze police data[9]. While this could simplify access to police workers via paper-based or electronic distribution lists, this strategy is again nonrandom and would target a very specific population.

Sample size and statistical power. The number of cases included in the analyses (N=45) was extremely low. Low sample size undermines confidence in the statistical estimates,

[9] The memberships of The International Association of Crime Analysts (IACA) and International Association of Law Enforcement Intelligence Analysts (IALEIA) would meet this requirement.

particularly for inferential analyses involving multiple variables, and further complicates the generalizability of the findings.

The START data posed three challenges. First, of 695 target agencies in the combined sampling frames, the data consisted of responses for only 147 agencies. Second, some participants failed to provide the name of their agency and therefore rendered their submissions unusable for organizational analyses. Third, in many cases respondents did not answer questions with the result that the dataset included a significant amount of missing data. When one considers there are 17,985 law enforcement agencies in the United States (Reaves, 2011a), the number of agencies evaluated in the current study is a serious limitation.

A single informant strategy relies on the ability of the individual to provide valid responses. A concern here is whether participants were able to answer questions or chose not to. Although some items were less well answered than others, the general pattern of missingness across responses suggested many individuals ended their involvement early. The length of the survey may therefore have led these respondents to withdraw because they found participation unnecessarily burdensome.

However, it is also likely respondents did not believe it was appropriate to disclose information about law enforcement practices that they deem are sensitive and potentially harmful to their agency (Carter et al., 2012; Carter, 2011; Chermak et al., 2013). Evidence to support this view was the failure to provide an agency name and nonresponse for questions asking about electronic information sharing systems. Because the present study focused on system use and the pattern of missing data was nonrandom, incomplete cases were discarded with the effect that the sample size was further reduced.

It is worth noting the START project investigators did consider the use of incentives to increase participation. Research has shown that the inclusion of a monetary incentive (i.e., a few one dollar bills) at the time of the initial survey mailing is likely to yield higher rates of response (Church, 1993). As a social rather than an economic exchange, the offer of a monetary gift before the survey is completed signals the researchers' trust in potential respondents, who may take the incentive without participating, and it demonstrates the ability of researchers to deliver rewards to respondents (Dillman et al., 2009).

However, this strategy was not used because of four concerns. First, the physical mailing of surveys with incentives, or a mixed-mode design using a mailed incentive with the initial invitation and an online survey (De Leeuw, 2005), would have been problematic due to the increased costs of mailing out to two samples and the uncertainty involved with surveys moving from generic agency addresses to study participants' work areas. Second, electronic incentives with minimum purchase values (e.g., online gift certificates) may represent a higher cost to researchers, be a burden for respondents to redeem, and fail to match cash effects on response (Birnholtz, Horn, FInholt, & Bae, 2004). Third, although researchers have examined the ethics of incentives (Singer & Couper, 2008), the team was worried about police officers interpreting a monetary or nonmonetary incentive linked to survey participation as a bribe. Fourth, it was not apparent whether criminal justice researchers had used incentives before and the team was undecided about the wisdom of setting a precedent (i.e., an expectation for survey research to include monetary incentives), or how funding authorities would view the use of incentives in future projects supported with public monies.

Previous researchers have reported the results of interviews with nonrespondents who were invited to participate in a national study of law enforcement intelligence practices (Carter et

al., 2012; Chermak et al., 2013). This was not possible for the START study because the research team had only access to the contact details of individuals in the MSU sample. Control over the data collection process, to the extent that it is possible to identify respondents, should therefore be a future consideration. A shorter instrument may also elicit a larger number of complete submissions because it reduces the time required to complete the survey, a factor likely to be appreciated by workers who are willing to participate but can spare little time to do so. Nevertheless, irrespective of assurances provided to participants concerning the confidentiality of study data, it is necessary for researchers to understand respondent distrust and beliefs about the sensitivity of law enforcement intelligence — i.e., consenting to disclose information that has the potential to compromise agencies and in turn jeopardize individual careers — that could thwart efforts to study these activities.

Concept measurement. Measurement of the study factors was also problematic. In particular, discussion of the main findings highlighted concerns about the indicators used to represent perceived benefits and the institutional pressures. First, it was unclear whether enough indicators were used for the concept of benefits. Scholars have noted that the identification of benefits derived through innovation is challenging, not least because implementation is likely to be a highly contextualized activity (Damanpour, 1991; Tornatzky et al., 1983). Future research could include items that capture technological, organizational, and environmental dimensions of sharing system benefits (Dawes, 1996), as well as open-ended questions to discover advantages not documented previously.

Burruss and Giblin (2009) have argued the advancement of institutional explanations of policing and criminal justice practices will depend on researchers' attention to conceptual and measurement issues. For this reason the study sought to build upon the work of previous studies.

However, the use of previously validated survey items in this study was only of partial help since respondents did not respond to all of the questions. As a consequence, and in contrast to scholarship that has reported institutional pressures as multidimensional constructs (Burruss & Giblin, 2014; Burruss et al., 2010; Giblin & Burruss, 2009), the current work treated normative pressures and mimesis as unidimensional. Thus normative pressures focused on accreditation but not trainings, publications, or membership to professional groups, and mimesis was framed as modeled activity but excluded observation of other agencies. If system use does depend on different normative, mimetic, and coercive pressures, then the test model should include multiple measures to assess them.

The operationalization for coercive pressures was agency compliance with 28 CFR Part 23 guidelines that specify how to handle electronic records used for intelligence practices. These guidelines serve to minimize the risk of legal actions being launched against the agency due to a lack of safeguards protecting information about individuals and organizations. This choice represented a departure from previous research that treated funding made available through grants as an inducement or positive incentive from authorities for agencies to adopt new structures (Crank & Langworthy, 1996; Scott, 2013). Reasons for this decision rested upon mixed support in the literature for funding as a measure of coercive pressures (Burruss & Giblin, 2014; Burruss et al., 2010; Giblin, 2006; Giblin & Burruss, 2009) and conceptual ambiguity about whether funding reflects an institutional argument or theory highlighting agencies' dependency on resources for survival (Giblin, 2004; Giblin & Burruss, 2009; Oliver, 1991; Wilson, 2005). Yet the results here indicated 28 CFR Part 23 compliance, although widespread among agencies in the study, was unrelated to agency use of sharing systems. This may be because compliance represents a commitment to professional practice, which aligns more with

normative pressures. If lawsuits do pose a serious threat to the legitimacy of agencies' intelligence activities, a better measure would be to ask workers about their perceptions of civil litigation arising from information misuse.

The study used the total number of full- and part-time personnel to represent organizational size. But its treatment as an ordinal measure presented analytical and conceptual challenges. Critically, it is important to ask what interpretation of organizational size has and what it means when studying innovation. Tornatzky and Fleischer (1990) argue size does not reflect structure within the organization, the scale of operations, task complexity, or decision-making processes, and it essentially serves as a proxy for underlying organizational attributes. To move beyond the limitations of its use in this study, one option would be to use public data to derive a measure of slack resources within agencies. For example, a focus on municipal agencies would allow the use of agency, census, and crime data to create a continuous measure for either the number of residents served by officers, or crime rates for the agency jurisdiction (Skogan & Hartnett, 2005). A refined measure would offer greater conceptual clarity and include a dimension of the population that an agency serves.

Cross-sectional design. Another limitation of the study was its use of cross-sectional data. Observations made at a single point in time provide no insight into agency change. As a consequence the study was unable to explore how system use by agencies develops over time. Because the law enforcement intelligence and homeland security fields have undergone many changes since 9/11, it is therefore difficult to place the findings for sharing systems in perspective. Although the results for agencies' self-reported system use were contrasted with previous research, such a strategy cannot explain shifts in organizational practices and workers' perceptions of them.

In terms of theoretical development, a cross-sectional design also prevents the examination of time-ordered effects among variables. For example, the perceived benefits of sharing systems and resources available for information sharing practices were treated as separate contextual factors that explain system use by agencies. An expectation of information sharing, however, is law enforcement agencies exchange information that supports preventive and planning actions. Across time, evidence that system use promotes agency responses to emerging threats may instead shape perceptions of the technology's utility, that in turn influence decisions about resource planning. To untangle the relationships between these variables, future studies will need to have a longitudinal dimension.

Selection of the research method. So far the discussion in this section has highlighted the difficulties involved with researchers identifying law enforcement professionals who are informed about their agency's intelligence practices, successfully engaging these individuals, gathering valid measures, and examining causal mechanisms. Taken together, is a survey methodology appropriate for a study such as this?

If the goal is to generalize across a large population, a survey design may be the only choice that enables researchers to efficiently gather and analyze information about sample subjects (Bachman & Schutt, 2014). As we have seen, however, it remains unclear whether an online survey can elicit sufficient information about intelligence practices to satisfy this objective. This realization suggests a need to revisit the research agenda and the choice of investigative approach for understanding the use of law enforcement sharing systems.

One alternative would be the case study method. Case studies have a strong tradition in social science research (Dooley, 2002) and, in particular, empirical studies of information systems (Lee, 1989). The method is appropriate when the boundaries between a phenomenon

and its context are unclear (Yin, 2009), and the phenomenon is embedded within larger systems (Ellinger, Watkins, & Marsick, 2005). This prescription is significant because the use of sharing systems within agencies is likely to reflect changes in the field of law enforcement intelligence. It is also consistent with calls to conceptualize information technologies as situationally embedded, dynamic systems that consist of technical, data, and social components (Orlikowski & Iacono, 2001).

Sampling in case study research centers on a need to establish theoretical replications which is distinct from the sampling logic of quantitative research which relies on sample size (Yin, 2009). In practice, while a study of sharing systems will likely involve multiple cases, the number of cases is likely to be smaller than that involved in survey research. But access to and time spent with agency workers could serve to counter workers' distrust of researchers' motives. Moreover, the ability to gather different types of information through observation, interviews, archives, and even questionnaires (Eisenhardt, 1989; Ellinger et al., 2005; Yin, 2009) may provide evidence that better explains the circumstances under which electronic exchanges of information take place.

Recommendations for Further Research

The existing literature and policies relating to information sharing highlight a continuing need for research examining this topic. Despite the limitations of this work, the questions that guided it are important and one recommendation is to conduct a replication study, perhaps using a different sampling frame and refined measures, to determine whether the current results are valid. Additionally, researchers could examine whether respondents' perceptions of information sharing vary based upon their organizational role or tenure. For instance, do analysts view technological, organizational, and environmental factors believed to shape the use of sharing

systems differently to supervisors and administrators? This line of inquiry might explore the routinization and formalization of the activity, concepts the current research did not evaluate, and the extent of decoupling between institutional expectations and worker practices.

Another direction could be to examine how workers use shared information as part of the intelligence fusion process. Do workers rely on specific systems for different types of information? In what ways do sharing systems help workers generate information for threat prevention or strategic planning? Such an investigation would allow researchers to discover why networks such as RISS.Net, LEO, and HSIN enjoy widespread use among agencies while other systems such as ATIX and FBINET do not. It would also be possible to more authentically frame sharing technologies as dynamic rather than fixed entities (Orlikowski & Barley, 2001), and to explore how workers use their experience to interpret agency objectives and directives when selecting systems for information acquisition and dissemination (Bullock, 2013). This agenda implies an embedded, qualitative study design that includes participant observation, open interviews with workers, and access to organizational materials such as written procedures and reports. As noted in the comments about the case study method, this work would likely focus on a handful of organizations at most in order to generate rich data with which to better understand how agency use of electronic sharing systems relates to intelligence production within a 9/11 environment.

Conclusions

The findings of this study expanded previous research in the area of law enforcement intelligence and information sharing. This work highlighted the use of federal networks that facilitate electronic exchanges of Sensitive But Unclassified information between law enforcement agencies across government. Large and small agencies were found to use these

sharing systems, but state agencies reported access to more systems on a regular basis. System use was not found to be associated with the production or receipt of intelligence. Of the technological, organizational, and environmental factors examined in the study, none were found to explain variation in use. While law enforcement workers recognized benefits of sharing system use, they were also concerned about the risk of misused information. Further assessment of the results revealed middle managers, rather than agency leaders, were champions of sharing systems and the amount of training workers received to use electronic information sharing systems was characterized as inadequate.

The literature indicates police practices have undergone significant changes since the events of 9/11 (Chermak et al., 2013). In a dynamic environment with emerging threats, there remains a need to understand what electronic systems contribute to intelligence practices undertaken to support public safety in the United States. There are many directions for researchers to pursue, but it may be helpful to focus on how workers use sharing technologies to discover information that ultimately serves agency and community goals.

APPENDICES

Appendix A: Definition of Terms

This study includes terms drawn from different government and academic reports. To establish a shared understanding of these terms, a list of working definitions follows.

Information: Information consists of pieces of raw, unanalyzed data that identify persons, organizations, evidence, and events, or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event (Carter 2009, p.11).

Intelligence: Intelligence is the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature (GIWG, 2003, p.27).

Intelligence focus: Intelligence focus refers to the strategic priority of a law enforcement agency's intelligence activities (Carter, 2009).

Information sharing: Information sharing is the volitional conveyance of information generated or obtained by one entity to another entity (Akbulut et al., 2009, p.146).

Electronic information sharing system: An electronic information sharing system may be defined as a collection of digital, networked services that facilitates the sharing of information and intelligence between law enforcement agencies and relevant partners in a secure manner (Akbulut et al., 2009; Akbulut-Bailey, 2011; Carter, 2009; *Mobilizing Information to Prevent Terrorism*, 2006).

Appendix B: Survey Instrument

You are invited to participate in a research study conducted by researchers from the School of Criminal Justice at Michigan State University and sponsored by the National Consortium for the Study of Terrorism and Responses to Terrorism (START). The purpose of this research is to document current intelligence practices in your organization and understand major obstacles for effective intelligence gathering and information sharing. You are receiving this survey since you attended a law enforcement intelligence training program and are known to have unique knowledge related to law enforcement intelligence practices. This survey has also been officially endorsed by the Memorial Institute for the Prevention of Terrorism (MIPT) for the purposes of learning about these practices.

There are no foreseeable risks or discomforts from participating in this research study. Your answers will provide us with valuable insight into what is working in law enforcement intelligence and what are the problem areas. You will not directly benefit from your participation in this study. However, your participation in this study may contribute to the understanding best practices in intelligence and critical training gaps.

Your responses are confidential and are protected to the extent allowable by federal, state, and local laws. The U.S. Department of Justice regulations (28 CFR 22) and Federal Statute (42 USC 3789(g)) prohibits us from disclosing your information for any purpose other than research, or in any judicial or administrative proceedings, without your consent.

The data will be stored for 10 years after the project closes and stored in the office of the principal investigator. Only the principal investigators of the study and Michigan State University's Institutional Review Board will have access to these data.

Your participation is voluntary, you may choose not to participate at all, or you may refuse to answer certain questions or discontinue your participation at any time without consequence. Refusal to participate will involve no penalty or loss of benefits to which you were otherwise entitled.

If you have concerns or questions about this study, such as scientific issues, how to do any part of it, please contact the Steven Chermak, the principal investigator, at 517-355-2210, or email chermak@msu.edu, or regular mail at the School of Criminal Justice, MSU, East Lansing, MI 48824.

If you have questions or concerns about your role and rights as a research participant, would like to obtain information or offer input, or would like to register a complaint about this study, you may contact, anonymously if you wish, the Michigan State University's Human Research Protection Program at 517-355-2180, Fax 517-432-4503, or e-mail irb@msu.edu or regular mail at 207 Olds Hall, MSU, East Lansing, MI 48824.

Consent: By completing this survey you have indicated that you have read the information and have consented to participate in this study.

1. Do you consent to participation in this research study?
    a. Yes; No.

Respondent and Agency Information

2. Are you?
    a. Sworn personnel; Non-sworn personnel.

3. Which of the following best describes your role in your agency?
    a. Administrator/Manager; Supervisor; Investigator/Uniformed; Analyst; Other (please specify).

4. How many years have you been at the agency?
    a. Less Than 1 Year; 1-3 Years; 4-9 Years; 10-15 Years; More Than 15 Years.

5. What is your sex?
    a. Male; Female.

6. How many total personnel work in your organization?
    a. Less than 25; 26-100; 101-250; 251-500; 501-3,000; More than 3,000.

7. Which of the following best describes the jurisdiction of your organization?
    a. Federal; State; Municipal; County; Tribal; State Fusion Center; Other Fusion Center.

8. What organization do you work for?
    a. [Open-ended response.]

Your Organization's Intelligence Function.

9. Which best describes the focus of your intelligence function?
    a. Our focus is only on terrorism; We use an "all-crimes" approach; We use an "all-crimes", "all-threats", and "all-hazards" approach; Our focus is not specified; The organization has no intelligence function.

10. How many of the intelligence analysts are (please enter a best estimate):
    Sworn personnel? a. [Open-ended response.]
    Non-sworn personnel? a. [Open-ended response.]

11. Number of persons assigned to work intelligence who are not analysts (please enter a best estimate):
    Sworn personnel? a. [Open-ended response.]
    Non-sworn personnel? a. [Open-ended response.]

12. Is your criminal intelligence records system 28 CFR Part 23 compliant?
    a. Yes; It is being modified to become compliant; No.

Perceptions of Terrorist Threats

13. Indicate whether your agency strongly agrees, agrees, disagrees, or strongly disagrees that each of the following extremist groups is considered a serious threat to your jurisdiction. Please check the appropriate response.

a. Scale: Strongly Disagree; Disagree; Agree; Strongly Agree.

Militia/Patriotism

Sovereign Citizens

Ku Klux Klan

Christian Identity

Idiosyncratic Sectarians/Christian Identity

Neo-Nazi

Reconstructed Traditions (e.g., Odinism)

Racist Skinheads

Islamic extremists/Jihadists (e.g., Al Qaeda)

Left-wing revolutionary (e.g., Weathermen)

Black Nationalist

Extreme environmental (e.g., Environmental Liberation Front)

Extreme animal rights (e.g., Animal Liberation Front)

Extreme anti-tax

Extreme anti-abortion

Extreme anti-immigration

Millenial/Doomsday cults (Y2K, spiritual cults, etc)

Other single issue constituencies

Other (please specify).

14. In your opinion, how prepared is your organization for terrorist or criminal extremist threats in your region?

a. Very prepared; Prepared; Somewhat prepared; Not prepared; Not at all prepared.

Beliefs About other Activities

15. According to your agency, what is the likelihood that each of the following terrorist events will occur in your state in the next five years? Please check the appropriate response.

a. Scale: Very Unlikely; Unlikely; Likely; Very Likely.

Chemical incident (e.g., Sarin gas)

Biological incident (e.g. Anthrax)

Nuclear or radiological incident (e.g., Dirty bomb)

Conventional explosive incident (e.g., IED)

Cyber terrorism

Agro-terrorism incident involving food

Agro-terrorism incident involving animal disease non-transferable to humans (e.g., hoof and mouth disease)

Terrorism incident involving military weapons (i.e., mortars, automatic weapons)

Inter-agency Interactions

16. The following are sources of information relating to domestic terrorism that some police agencies have used as a resource. Please indicate how useful these sources have been to your agency by checking the appropriate response.

a. Scale: Not Used; Not Useful; Somewhat Useful; Very Useful.

Federal Bureau of Investigation (FBI)

FBI Joint Terrorism Task Force (JTTFs)

Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A)

Immigration and Customs Enforcement (ICE)

Drug Enforcement Administration (DEA)

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

Customs and Border Protection (CBP)

Your state's Office of Homeland Security

Your state's Attorney General Anti-Terrorism Task Force

State/Local Fusion Center

Law enforcement professional associations

Law Enforcement Online (LEO)

RISS.Net

HSIN-Intel

Risk assessment services or publications

Internet (open source)

Media (electronic or print)

Professional law enforcement publications

Books, journals, or periodicals from non-law enforcement

Radical publications or alternative literature

Informants or sources on the street

17. How satisfied are you with the working relationship between your organization and the following agencies? Please check the appropriate response.

a. Scale: We Have No Relationship; Not Satisfied; Not Very Satisfied; Somewhat Satisfied; Very Satisfied.

Federal Bureau of Investigation (FBI)

State Law Enforcement Agencies

Local Law Enforcement Agencies

Tribal Law Enforcement Agencies

Your State/Local Fusion Center

State Government Officials

Critical Infrastructure Security Representatives

Department of Corrections

Emergency Management

Fire Marshal

Department of Homeland Security (DHS)

Your state's Office of Homeland Security

Homeland Security Investigations (HSI)

IRS

Hospitals

Private Sector Agencies

Public Health Agencies

Public Works

Public Transportation

National Guard

Information and Intelligence Sharing

18. Is your agency a member of your Regional Information Sharing Systems (RISS) center?
    a. Yes; No; Unknown.

19. Does your agency have a formal system for officers to submit Suspicious Activity Reports (SARs) system?
    a. Yes; In the process of implementing it; No; Unknown.

20. Are all SARs from your agency submitted to the state Fusion Center?
    a. Yes; No; Unknown.

21. Do any members of your agency regularly search the NSI "Shared Space" or NSI "eGuardian" (computer networks) for comparable suspicious activity in your jurisdiction?
    a. Yes; No; Unknown.

22. Has using the NSI Shared Space or eGuardian led to further investigations?
    a. Yes; No; Unknown.

23. Indicate the extent to which the following are a problem for your organization to share information and intelligence? Please check the appropriate response.
    a. Scale: Not a Problem At All; Somewhat of a Problem; Significant Problem; Don't Know.

    Security Clearances

    Adequate Personnel

    Adequate Training

    Adequate Resources

    Adequate Time

    Organizational Culture

    Other (please specify).

24. To what extent do you agree your organization is part of the Information Sharing Environment (ISE)? Please choose a number between 1 and 7 where 1 represents "strongly disagree" and 7 represents "strongly agree."
    a. Scale: 1-Strongly Disagree through 7-Strongly Agree.

Networked Information Sharing Systems

25. The following networked information sharing systems meet our information sharing needs. Please check the appropriate response.
    a. Scale: Not Satisfied; Not Very Satisfied; Somewhat Satisfied; Very Satisfied; Do Not Use.

    Regional Information Sharing System Network (RISS.Net)

    Law Enforcement Online (LEO)

    Homeland Security Information Network (HSIN)

    Automated Trusted Information Exchange (ATIX)

Federal Bureau of Investigation Network (FBINET)

Lessons Learned Information Sharing (LLIS)

Open Source Center.

26. How often do you access a networked information sharing system (such as HSIN, LEO, RISS.Net, InfraGard, NLETS, or any others)? Please select the appropriate response.

a. Daily; Once or twice a week; Three times a week, but not daily; Every two weeks; Monthly; Less than once per month; We do not access a networked information sharing system.

27. To what extent do you agree with the following statements? Please choose a number between 1 and 7 where 1 represents "strongly disagree" and 7 represents "strongly agree"; if workers don't use networked information sharing systems, select the last option.

a. Scale: 1-Strongly Disagree through 7-Strongly Agree; Do not use them.

Networked information sharing systems have led to:

Improved quality of information being shared.

Increased information sharing between workers in your organization.

Increased information sharing between workers in different agencies.

Secure communication of information shared.

Agency workers using inbuilt directory services (e.g., prebuilt email list) to directly contact workers in different agencies during the course of investigations.

Too much information being collected.

Increased demands for information beyond the agency's capacity to respond.

Resources being diverted away from other agency priorities.

Shared data being misinterpreted or misused.

Improved agency accountability.

Improved worker accountability.

A less trusting (or more paranoid) organizational atmosphere.

New formalized interagency relations.

A fundamental change in the way your organization shares information with other law enforcement agencies.

28. To what extent do you agree with the following statements? Please choose a number between 1 and 7 where 1 represents "strongly disagree" and 7 represents "strongly agree"; if workers don't use networked information sharing systems, select the last option.

a. Scale: 1-Strongly Disagree through 7-Strongly Agree; Do not use them.

Workers have no difficulty telling others about the results of using a networked information sharing system.

It is easy to communicate to others the consequences of using a networked information sharing system.

The results of using a networked information sharing system are apparent to workers.

Workers have difficulty explaining why using a networked information sharing system may or may not be beneficial.

Networked information sharing systems are consistent with my organization's beliefs and values.

The attitude towards networked information sharing systems in my organization is favorable.

Networked information sharing systems are compatible with my organization's information technology (IT) infrastructure.

Top management is interested in the implementation of networked information sharing systems.

Top management considers networked information sharing systems as important to the organization.

Top management has effectively communicated its support for networked information sharing systems.

29. Please indicate whether there is (or was) one individual who has enthusiastically championed the adoption of networked information sharing systems in your organization.

a. Yes; No; Unknown.

30. If "yes" above, please indicate whether this individual was a:

a. Worker (non-supervisory); Manager; Chief/Agency leader.

31. Does your agency offer incentives to intelligence workers for information sharing and collaboration? Incentives may also include nominations for individual or group awards.

a. Yes; No; Unknown.

32. To what extent do you agree the attitude of your top management toward the deployment of information technology in your organization is supportive. Please choose a number between 1 and 7 where 1 represents "strongly disagree" and 7 represents "strongly agree."

a. Scale 1-Strongly Disagree through 7-Strongly Agree.

33. To what extent do you agree with the following statements? Please choose a number between 1 and 7 where 1 represents "insignificant" and 7 represents "highly significant."

To what extent is information technology important for the fulfillment of:

a. Scale: 1-Insignificant through 7-Highly significant.

Productivity improvement.

Improved access to information.

Improved quality of decision making.

Service to citizens.

34. Think about all the networked information sharing systems you use. Which one of the following information sharing systems do you use the most frequently?

a. We do not use any networked information sharing systems; Regional Information Sharing System Network (RISS.Net); Law Enforcement Online (LEO); Homeland Security Information Network (HSIN); Automated Trusted Information Exchange (ATIX); Federal Bureau of Investigation Network (FBINET); Lessons Learned Information Sharing (LLIS); Open Source Center.

Other (please specify).

Intelligence Training

35. What intelligence training programs have workers attended? Please check the appropriate response.

a. Have Not Attended; Have Attended; Unknown.

Fundamentals of Intelligence Training (FIAT)

Federal Law Enforcement Training Center (FLETC) Analyst Training

DHS Critical Thinking Training

DEA's Federal Law Enforcement Analyst Training (FLEAT)

FBI National Academy

FBI Center for Intelligence Training (CIT)

National White-Collar Crime Center (NW3C) Intelligence Analyst Training

State and Local Anti-Terrorism Training (SLATT)

Bureau of Justice Assistance (BJA) 28 CFR 23 Training

Regional Counterdrug Training Academy (RCTA) Intelligence Training

DHS Report Writing

Other (please specify).

Intelligence Products

36. The main source of training to use networked information sharing systems is:
a. Self; Co-worker or supervisor; Training employees; Outside professionals – in person; Outside professionals – online; Unknown.

37. The amount of training workers receive in order to use networked information sharing systems is:
a. Too little; About right; Too much; Unknown.

38. How frequently does your agency create the following intelligence products? Please check the appropriate response.
a. Scale: Never; Monthly; Weekly; Daily; Upon Request.

Bulletins

Threat assessments

Vulnerability assessments

Risk assessments

Advisories

Alerts

Warnings

Executive reports

Briefings

Other (please specify).

39. How useful are intelligence products for providing you with situational awareness of terrorist threats?

a. Very useful; Somewhat useful; Not very useful; Not useful; Have not received intelligence products related to terrorist threats; Have not received intelligence products of any type.

40. How often do intelligence products provide you with new information that you previously knew little about?

a. Very frequently; Frequently; Infrequently; Very infrequently; Unknown.

41. How often do intelligence products provide you with information on officer safety threats?

a. Very frequently; Frequently; Infrequently; Very infrequently; Unknown.

42. How often do these intelligence products provide you with information that is actionable – that is, the product allowed you to make a better decision or there was something you could do that may intervene in a threat?

a. Very frequently; Frequently; Infrequently; Very infrequently; Unknown.

Organizational Characteristics

43. Please indicate below what sources of external funding your agency has received in support of information sharing functions. Please consider only funding outside your agency's normal operating budget. It can include external funding for personnel, equipment, or training.

a. No external funds for information sharing functions; Private organization/agency; Local (e.g., municipal or county) government agency; State government agency; Federal government agency.

Other (please specify).

44. In evaluating your own agency's performance with respect to information sharing, to what extent does your agency pay attention to the practices of other law enforcement agencies like your own?

a. Pay significant attention; Pay some attention; Pay little attention; Pay no attention.

45. To what extent does your organization model its information sharing activities after those of other agencies that you view as successful?

a. Often; Sometimes; Never.

46. Has your organization been accredited through the Commission of the Accreditation of Law Enforcement Agencies (CALEA) during 2013 or earlier?

a. Yes; No; Unknown.

47. Do you or any other person in the agency responsible for information sharing belong to the following organizations? Please check the appropriate response.

a. Scale: No; Yes; Unknown.

International Association of Law Enforcement Intelligence Analysts (IALEIA)

Association of Law Enforcement Intelligence Units (LEIU)

National Fusion Center Association

Major Cities Chiefs Intelligence Commanders

International Association for Intelligence Education

International Association of Crime Analysts.

48. What system(s) or resources do you use on a regular basis? Please check the appropriate response.

a. Scale: Never; Rarely; Often; Very Often.

Department of Justice – Law Enforcement Information Sharing Program (LEISP)

Homeland Security – State and Local Intelligence Community of Interest (HS SLIC)

Lesson Learned Information Sharing (LLIS)

Open Source Center

National Criminal Intelligence Resource Center

Law enforcement professional associations

Other (please specify).

Thank you! We greatly appreciate you taking the time to complete the START survey.

Appendix C: Description of Federal Sharing Systems

The current research focuses on five federal sharing systems. This section provides a basic description of these systems.

RISS.Net refers to the Regional Information Sharing Systems' secure intranet operated by the United States Department of Justice. Active for more than 40 years, the program serves officers in all 50 states, the District of Columbia, and U.S. territories, along with justice practitioners in other countries including Australia, Canada, England, and New Zealand. RISS.Net provides access to a number of information sources intended to combat organized and violent crime, drug trafficking, human trafficking, and gang activity (*RISS Overview*, n.d.), and it has been explicitly promoted as an "initial communications backbone" (GIWG, 2003, p.23) for Sensitive But Unclassified/Controlled Unclassified Information (SBU/CUI) information.

Law Enforcement Online (LEO) was created in 1995 as an FBI communications network for law enforcement personnel. Designed to enhance sharing of SBU/CUI information, LEO enables users to connect to the RISS system via a single web interface (*Law Enforcement Online*, n.d.). Other features include access to FBI intelligence products, a national alert system, tools that support communications between users, and learning resources (Carter, 2009; Koestner, 2008).

HSIN is the United States Department of Homeland Security's Information Network. HSIN facilitates sharing of information between governmental and nongovernmental organizations responsible for counterterrorism and management of critical incidents. HSIN's collaborative tools include instant (Jabber) and secure (HSINBox) messaging, and web conferencing. Like LEO, the system sends out alerts and notifications, and it has online resources to promote user learning (*HSIN Features*, n.d.; *What is HSIN?*, n.d.). A distinction,

however, is HSIN's focus on activity information, such as reports of suspicious activities, and applications capable of analyzing geospatial mapping and imaging information, as well as terrorist threats, tactics, and weapons (Carter, 2009; *HSIN Features*, n.d.).

ATIX, or RISS Automated Trusted Information Exchange, enables law enforcement, critical infrastructure, and first responder personnel to securely exchange homeland security information, including details about terrorist threats and disasters. Users of ATIX participate within community groups — i.e., government, emergency management, law enforcement, private security, utilities, transportation, agriculture, chemical manufacturing, banking and finance — reflecting their professional focus (*ATIX*, n.d.). ATIX transmits advisories, bulletins, and alerts from the United States' Department of Homeland Security and Department of Transportation, Federal Bureau of Investigation, and other government sources. The system's collaborative tools consist of live chat rooms, electronic conferencing along with a discussion forum, and online bulletin boards. Learning resources include a searchable document library organized by community (*ATIX*, n.d.; Carter, 2009).

FBINET is the Federal Bureau of Investigation Secret Network. Little information about this system is publicly available, but Carter (2009) notes FBINET's conveyance of investigative case files and national security information, and user access to administrative utilities.

BIBLIOGRAPHY

BIBLIOGRAPHY

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. (2004). New York: W. W. Norton & Company.

Ackroyd, S., Harper, R., Hughes, J. A., & Shapiro, D. (1992). *New technology and practical police work: The social context of technical innovation*. Philadelphia, PA: Open University Press.

Agresti, A. (1990). *Categorical data analysis*. New York: John Wiley & Sons.

Agresti, A. (2010). *Analysis of ordinal categorical data* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Akbulut, A. Y. (2003). *An investigation of the factors that influence electronic information sharing between state and local agencies.* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3098054)

Akbulut, A. Y., Kelle, P., Pawlowski, S. D., Schneider, H., & Looney, C. A. (2009). To share or not to share? Examining the factors influencing local agency electronic information sharing. *International Journal of Business Information Systems, 4*(2), 143-172.

Akbulut-Bailey, A. Y. (2011). Information sharing between local and state governments. *Journal of Computer Information Systems, 51*(4), 53-63.

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. *Journal of Enterprise Information Management, 26*(3), 250-275.

Anseel, F., Lievens, F., Schollaert, E., & Choragwicka, B. (2010). Response rates in organizational science, 1995-2008. *Journal of Business and Psychology, 25*(3), 335-349.

ATIX. (n.d.). Retrieved from http://www.riss.net/resources/atix

Bachman, R., & Schutt, R. K. (2014). *The practice of research in criminology and criminal justice*. Thousand Oaks, CA: Sage.

Baird, Z., & Barksdale, J. (2006). Building a trusted information-sharing environment. In C. Northouse (Ed.), *Protecting what matters: Technology, security, and liberty since 9/11* (pp. 51-62). Washington, DC: Computer Ethics Institute, Brookings Institution Press.

Baker, J. (2012). The Technology-Organization-Environment framework. In Y. K. Dwivedi, M. R. Wade & S. L. Schneberger (Eds.), *Information systems theory: Explaining and predicting our digital society* (Vol. 1, pp. 231-245). New York: Springer.

Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human Relations, 61*(8), 1139-1160.

Bhaskar, R., & Zhang, Z. (2007). Knowledge sharing in law enforcement: A case study. *Journal of Information Privacy & Security, 3*(3), 45-68.

Billiet, J., & Matsuo, H. (2012). Non-response and measurement error. In L. Gideon (Ed.), *Handbook of survey methodology for the social sciences* (pp. 149-178). Boston: Springer.

Birnholtz, J. P., Horn, D. B., FInholt, T. A., & Bae, S. J. (2004). The effects of cash, electronic, and paper gift certificates as respondent incentives for a web-based survey of technologically sophisticated respondents. *Social Science Computer Review, 22*(3), 355-362.

Bolman, L. G., & Deal, T. E. (1991). *Reframing organizations: Artistry, choice, and leadership*. San Francisco: Jossey-Bass.

Brewster, B., Akhgar, B., Staniforth, A., Waddington, D., Andrews, S., Mitchell, S. J., & Johnson, K. (2014). Towards a model for the integration of knowledge management in law enforcement agencies. *International Journal of Electronic Security and Digital Forensics, 6*(1), 1-17.

Brick, J. M., & Williams, D. (2013). Explaining rising nonresponse rates in cross-sectional survey. *The ANNALS of the American Academy of Political and Social Science, 20*(3), 36-59.

Brodeur, J.-P., & Dupont, B. (2006). Knowledge workers or "knowledge" workers? *Policing and Society, 16*(1), 7-26.

Brown, M. (2000). Criminal justice discovers information technology. In G. LaFree (Ed.), *The nature of crime: Continuity and change* (Vol. Vol. 1 of the National Institute of Justice 2000 Series, pp. 219-259). Washington, DC: National Institute of Justice.

Brown, M. K. (1981). *Working the street: Police discretion and the dilemmas of reform*. New York: Russell Sage Foundation.

Brown, M. M., & Brudney, J. L. (2003). Learning organizations in the public sector? A study of police agencies employing information and technology to advance knowledge. *Public Administration Review, 63*(1), 30-42.

Bullock, K. (2013). Community, intelligence-led policing and crime control. *Police & Society, 23*(2), 125-144.

Burke, P. A. (2009). *Collecting and connecting the dots: Leveraging technology to enhance the collection of information and the dissemination of intelligence*. (Master's thesis, Naval Postgraduate School). Retrieved from http://calhoun.nps.edu/public/handle/10945/4661

Burruss, G. W., & Giblin, M. J. (2014). Modeling isomorphism on policing innovation: The role of institutional pressures in adopting community-oriented policing. *Crime & Delinquency, 60*(3), 331-355.

Burruss, G. W., Giblin, M. J., & Schafer, J. A. (2010). Threatened globally, acting locally: Modeling law enforcement homeland security practices. *Justice Quarterly, 27*(1), 77-101.

Carter, D. L. (2005). Brief history of law enforcement intelligence: Past practice and recommendations for change. *Trends in Organized Crime, 8*(3), 51-62.

Carter, D. L. (2009). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Carter, D. L. (2010). Critical issues in civil rights for law enforcement intelligence and counterterrorism. *Criminal Law Bulletin, 46*(4), 587-624.

Carter, D. L., & Carter, J. G. (2009a). The intelligence fusion process for state, local, and tribal law enforcement. *Criminal Justice and Behavior, 36*(12), 1323-1339.

Carter, D. L., & Carter, J. G. (2009b). Intelligence-led policing: Conceptual considerations for public policy. *Criminal Justice Policy Review, 20*(3), 310-325.

Carter, D. L., Chermak, S. M., Carter, J. G., & Drew, J. (2014). *Understanding law enforcement intelligence processes: Report to the Office of University Programs, Science and Technology Directorate, U.S. Department of Homeland Security*. College Park, MD: START.

Carter, D. L., Chermak, S. M., McGarrell, E. F., Carter, J. G., & Drew, J. (2012). *Understanding the intelligence practices of state, local, and tribal law enforcement agencies*. Washington, DC: National Institute of Justice. U.S. Department of Justice.

Carter, D. L., & Schafer, J. A. (2007). The future of law enforcement intelligence. In J. A. Schafer (Ed.), *Policing 2020: Exploring the future of crime, communities, and policing* (pp. 226-256). Quantico, VA: U.S. Department of Justice, Federal Bureau of Investigation.

Carter, J. G. (2011). *Policing innovation: Exploring the adoption of intelligence-led policing.* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3450658)

Carter, J. G., Carter, D. L., & Chermak, S. M. (2013). Intelligence training. *Law Enforcement Executive Forum, 13*(2), 1-18.

Caruso, J. C., & Cliff, N. (1997). Empirical size, coverage, and power of confidence levels for Spearman's Rho. *Educational and Psychological Measurement, 57*(4), 637-654.

Casey, J. (2004). Managing joint terrorism task forces. *FBI Law Enforcement Bulletin, 73*(11), 1-6.

Cattrell, R. B. (1966). The scree test for the number of factors. *Multivariate Behavioral Research, 1*(2), 245-276.

Center for Technology in Government. (1999). Reconnaissance study: Developing a business case for the integration of criminal justice information. Retrieved from http://www.ctg.albany.edu/publications/reports/reconnaissance

Chan, J., Brereton, D., Legosz, M., & Doran, S. (2001). *E-policing: The impact of information technology on police practices*. Brisbane, Australia: Criminal Justice Commission.

Chan, J. B. L. (2001). The technological game: How information technology is transforming police practice. *Criminal Justice, 1*(2), 139-159.

Chau, P. Y. K., & Tam, K. Y. (1997). Factors affecting the adoption of open systems: An exploratory study. *MIS Quarterly, 21*(1), 1-24.

Chen, H., Schroeder, J., Hauck, R. V., Ridgeway, L., Atabakhsh, H., Gupta, H., . . . Clements, A. W. (2002). COPLINK Connect: Information and knowledge management for law enforcement. *Decision Support Systems, 34*(3), 271-285.

Chermak, S. M., Carter, J. G., Carter, D. L., McGarrell, E. F., & Drew, J. (2013). Law enforcement's information sharing infrastructure: A national assessment. *Police Quarterly, 16*(2), 211-244.

Chong, A. Y.-L., & Ooi, K.-B. (2008). Adoption of interorganizational systems standards in supply chains: An empirical analysis of RosettaNet standards. *Industrial Management & Data Systems, 108*(4), 529-547.

Chu, J. (2001). *Law enforcement information technology: A managerial, operational, and practioner guide*. Boca Raton, FL: CRC Press.

Church, A. H. (1993). Estimating the effect of incentives on mail survey response rates: A meta-analysis. *Public Opinion Quarterly, 57*(1), 62-79.

Chwelos, P., Benbasat, I., & Dexter, A. S. (2001). Empirical test of an EDI adoption model. *Information Systems Research, 12*(3), 304-321.

Collins, H. (2003). *Enterprise knowledge portals: Next-generation portal solutions for dynamic information access, better decision making, and maximum results*. New York: American Management Association.

Concept for operations for integrated justice information sharing. (2003). Lexington, KY: National Association of State Chief Information Officers.

Cornell University Law School. (n.d.). *42 U.S. Code § 1983 - Civil action for deprivation of rights.* Retrieved October 28, 2014, from http://www.law.cornell.edu/uscode/text/42/1983

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology, 78*(1), 98-104.

Cragg, P. B., & King, M. (1993). Small-firm computing: Motivators and inhibitators. *MIS Quarterly, 17*(1), 47-60.

Crank, J. P. (2003). Institutional theory of police: A review of the state of the art. *Policing: An International Journal of Police Strategies & Management, 26*(2), 186-207.

Crank, J. P., & Langworthy, R. (1992). An institutional perspective of policing. *The Journal of Criminal Law and Criminology, 83*(2), 338-363.

Crank, J. P., & Langworthy, R. (1996). Fragmented centralization and the organization of the police. *Policing and Society, 6*, 213-229.

Creating a trusted network for homeland security. Second Report of the Markle Foundation Task Force. (2003). New York: Markle Foundation.

Cycyota, C. S., & Harrison, D. A. (2006). What (not) to expect when surveying executives: A meta-analysis of top manager response rates and techniques over time. *Organizational Research Methods, 9*(2), 133-160.

Damanpour, F. (1991). Organizational innovation: A meta-analysis of effects of determinants and moderators. *The Academy of Management Journal, 34*(3), 555-590.

Darroch, S., & Mazerolle, L. (2013). Intelligence-led policing: A comparative analysis of organizational factors influencing innovation uptake. *Police Quarterly, 16*(1), 3-37.

Davis, L., Pollard, M., Ward, K., Wilson, J. M., Varda, D., Hansell, L., & Steinberg, P. (2010). *Long-term effects of law enforcement's post-9/11 focus on counterterrorism and homeland security*. Santa Monica, CA: RAND.

Davis, L. M., Riley, K. J., Ridgeway, G., Pace, J., Cotton, S. K., Steinberg, P. S., . . . Smith, B. L. (2004). *When terrorism hits home: How prepared are state and local law enforcement*. Santa Monica, CA: RAND Corporation.

Dawes, S. S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management, 15*(3), 377-394.

Dawes, S. S., Cresswell, A. M., & Pardo, T. A. (2009). From "need to know" to "need to share": Tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Adminstration Review, 69*(3), 392-402.

De Leeuw, E. D. (2005). To mix or not to mix data collection modes in surveys. *Journal of Official Statistics, 21*(2), 233-255.

Denney, A. S., & Tewksbury, R. (2013). How to write a literature review. *Journal of Criminal Justice Education, 24*(2), 218-234.

Dillman, D. A., & Melani Christian, L. (2005). Survey mode as a source of instability across surveys. *Field Methods, 17*(1), 30-52.

Dillman, D. A., Smyth, J. D., & Melani Christian, L. (2009). *Internet, mail, and mixed-mode surveys: The tailored design method* (3rd ed.). Hoboken, NJ: John Wiley & Sons.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147-160.

Dooley, L. M. (2002). Case study research and theory building. *Advances in Developing Human Resources, 4*(3), 335-354.

Duecy, C. P. (2006). Intelligence and information sharing in counterterrorism. In D. G. Kamien (Ed.), *The McGraw-Hill Homeland Security Handbook* (pp. 391-412). New York: McGraw-Hill.

Dulin, J. M. (2009). *The components necessary for successful information sharing*. (Master's thesis, Naval Postgraduate School). Retrieved from http://calhoun.nps.edu/public/handle/10945/4884

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532-550.

Ellinger, A. D., Watkins, K. E., & Marsick, V. J. (2005). Case study research methods. In R. A. Swanson & E. F. Holton III (Eds.), *Research in organizations: Foundations and methods of inquiry* (pp. 327-350). San Francisco: Berrett-Koehler.

Ellis III, J. O. (2008). Countering terrorism with knowledge. In H. Chen, E. Reid, J. Sinai, A. Silke & B. Ganor (Eds.), *Terrorism informatics: Knowledge management and data mining for homeland security* (pp. 141-155). Boston, MA: Springer.

Enders, C. K. (2010). *Applied missing data analysis*. New York: The Guilford Press.

Enhancing the Law Enforcement Intelligence Capacity: Recommendations from the IACP Strategic Planning Session. (2010). Alexandria, VA: The International Association of Chiefs of Police.

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society*. Toronto: University of Toronto Press.

Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behavior, 26*(2), 132-139.

Fichman, R. G. (1992). *Information technology diffusion: A review of empirical research.* Paper presented at the 13th International Conference on Information Systems, Dallas, TX.

Ford, K. J. (2007). Building capabilitiy throughout a change effort: Leading the transformation of a police agency to community policing. *American Journal of Community Psychology, 39*(3-4), 321-333.

Ford, K. J., Weissbein, D. A., & Plamondon, K. E. (2003). Distinguishing organizational from strategy commitment: Linking officers' commitment to community policing to job behaviors and satisfaction. *Justice Quarterly, 20*(1), 159-186.

Foster, C., & Cordner, G. W. (2006). *The impact of terrorism on state law enforcement: Adjusting to new roles and changing conditions*. Washington, DC: U.S. Department of Justice.

Foster, R. E. (2005). *Police technology*. Upper Saddle River, NJ: Pearson Prentice Hall.

Freilich, J. D., Chermak, S. M., & Simone, J., Jr. (2009). Surveying American state police agencies about terrorism threats, terrorism sources, and terrorism definitions. *Terrorism and Political Violence, 21*(3), 450-475.

Galbraith, J. R. (1973). *Designing complex organizations*. Reading, MA: Addison-Wesley.

Gerber, B. J., Cohen, D. B., Cannon, B., Patterson, D., & Stewart, K. (2005). On the front line: American cities and the challenge of homeland security preparedness. *Urban Affairs Review, 41*(2), 182-210.

Ghobakhloo, M., Arias-Aranda, D., & Benitez-Amado, J. (2011). Adoption of e-commerce applications in SMEs. *Industrial Management & Data Systems, 111*(8), 1238-1269.

Gibbs, J. L., & Kraemer, K. L. (2004). A cross-country investigation of the determinants of scope of e-commerce use: An institutional approach. *Electronic Markets, 14*(2), 124-137.

Giblin, M. J. (2004). *Institutional theory and the recent adoption and activities of crime analysis units in U.S. law enforcement agencies.* (Doctoral dissertation). Available from ProQuest Dissertation and Theses Full Text. (UMI No. 3133873)

Giblin, M. J. (2006). Structural elaboration and institutional isomorphism: The case of crime analysis units. *Policing: An International Journal of Police Strategies & Management, 29*(4), 643-664.

Giblin, M. J., & Burruss, G. W. (2009). Developing a measurement model of institutional processes in policing. *Policing: An International Journal of Police Strategies & Management, 32*(2), 351-376.

Giblin, M. J., Burruss, G. W., & Schafer, J. A. (2014). A stone's throw from the metropolis: Re-examining small-agency homeland security practices. *Justice Quarterly, 31*(2), 368-393.

Gil-Garcia, J. R., Berg, S. A., Pardo, T. A., Burke, G. B., & Guler, A. (2009). *Conducting web-based surveys of government practitioners in social sciences: Practical lessons for e-government researchers*. Paper presented at the 42nd Hawaii International Conference on System Sciences, Hilton Waikoloa, Big Island, HI.

Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative e-Goverment: Impediments and benefits of information-sharing projects in the public sector. *European Journal of Information Systems, 16*(2), 121-133.

Gil-Garcia, J. R., Schneider, C. A., Pardo, T. A., & Cresswell, A. M. (2005). *Interorganizational information integration in the criminal justice enterprise: Preliminary lessons from state and county initiatives.* Paper presented at the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05).

GIWG (Global Intelligence Working Group). (2003). *The National Criminal Intelligence Sharing Plan*. Washington, DC: U.S. Department of Justice.

Graphia-Joyal, R. (2012). *State fusion centers: Their effectiveness in information sharing and intelligence analysis*. El Paso: LFB Scholarly Publishing.

Grover, V. (1993). An empirically derived model for the adoption of customer-based interorganizational systems. *Decision Sciences, 24*(3), 603-640.

Hagan, J. (1989). Why is there so little criminal justice theory? Neglected macro- and micro-level links between organization and power. *Journal of Research in Crime and Delinquency, 26*(2), 116-135.

Hameed, M. A., & Counsell, S. (2014). Establishing relationships between innovation characteristics and IT innovation adoption in organisations: A meta-analysis approach. *International Journal of Innovation Management, 18*(1), 1-41.

Hameed, M. A., Counsell, S., & Swift, S. (2012). A meta-analysis of relationships between organizational characteristics and IT innovation adoption in organizations. *Information & Management, 49*(5), 218-232.

Hamm, M. S. (2007). *Terrorist recruitment in American correctional institutions: An exploratory study of non-traditional faith groups*. Washington, DC: U.S. Department of Justice.

Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination*. Thousand Oaks, CA: Sage.

Haynes, M. R., & Giblin, M. J. (2014). Homeland security risk and preparedness in police agencies: The insignificance of actual risk factors. *Police Quarterly, 17*(1), 30-53.

Heberlein, T. A., & Baumgartner, R. (1978). Factors affecting response rates to mailed questionnaires: A quantitative analysis of the published literature. *American Sociological Review, 43*(4), 447-462.

Henry, V. E. (2002). The need for a coordinated and strategic local police approach to terrorism: A practitioner's perspective. *Police Practice and Research, 3*(4), 319-336.

Herman, M. (2001). *Intelligence services in the information age: Theory and practice*. London: Frank Cass.

Hildebrand, D. K., Laing, J. D., & Rosenthal, H. (1977). *Analysis of ordinal data*. Beverly Hills, CA: Sage.

Hinings, B., & Greenwood, R. (1988). The normative prescription of organizations. In L. G. Zucker (Ed.), *Institutional patterns and organizations: Culture and environment* (pp. 53-70). Cambridge, MA: Ballinger.

Homburg, V. (2008). *Understanding e-government: Information systsms in public administration*. New York: Routledge.

Homeland Security Information Network. (n.d.). Retrieved from http://www.dhs.gov/homeland-security-information-network

Homeland Security: Efforts to improve information sharing need to be strengthened. Report to the Secretary of Homeland Security (GAO-03-760). (2003). Washington, DC: U.S. General Accounting Office.

Horton, N. J., & Lipsitz, S. R. (2001). Multiple imputation in practice: Comparison of software packages for regression models with missing variables. *American Statistician, 55*(3), 244-254.

HSIN Features You Need. (n.d.). Retrieved from http://www.dhs.gov/sites/default/files/publications/HSIN-Fact Sheet-Features.pdf

Huysman, M., & De Wit, D. (2002). *Knowledge sharing in practice*. Boston: Kluwer Academic Publishers.

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic data interchange and small organizatios: Adoption and impact of technology. *MIS Quarterly, 19*(4), 465-485.

Implementing 9/11 Commission recommendations: Progress report. (2011). Washington, DC: U.S. Department of Homeland Security.

Information Sharing Environment Implementation Plan. (2006). Washington, DC: Office of the Director of National Intelligence.

Information Sharing Environment: Background and authorities. (n.d.). Retrieved from http://www.ise.gov/background-and-authorities

Information Sharing Environment: Definition of the results to be achieved in improving terrorism-related information sharing is needed to guide implementation and assess progress (GAO-08-492). (2008). Washington, DC: U.S. Government Accountability Office.

Information sharing systems: A survey of law enforcement. (2006). Washington, DC: The Justice Research and Statistics Association.

Information sharing: Progress made and challenges remaining in sharing terrorism-related information: Statement for the Record to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, 112th Cong. (2011) (Testimony of Eileen R. Larence).

Innes, M., Fielding, N., & Cope, N. (2005). 'The appliance of science?' The theory and practice of crime intelligence analysis. *British Journal of Criminology, 45*(1), 39-57.

Jamshidian, M. (2004). Strategies for analysis of incomplete data. In M. Hardy & A. Bryman (Eds.), *Handbook of data analysis* (pp. 113-130). Thousand Oaks, CA: Sage.

Johnson, R. K. (2012). Do police learn from lawsuit data? *Rutgers Law Record, 40*, 30-47.

Jones, R. W. (2000). *Critical Incident Protocol: A public and private partnership*. East Lansing, MI: Michigan State University.

Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educational and Psychological Measurement, 20*(1), 141-151.

Kapoor, K. K., Dwivedi, Y. K., & Williams, D. A. (2014). Roger's innovation adoption attributes: A systemic review and synthesis of existing research. *Information Systems Management, 31*(1), 74-91.

Kappeler, V. E. (2006). *Critical issues in police civil liability* (4th ed.). Long Grove, IL: Waveland Press.

Katz, C. M. (2001). The establishment of a police gang unit: An examination of organizational and environmental factors. *Criminology, 39*(1), 37-74.

King, W. R. (2000). Measuring police innovation: Issues and management. *Policing: An International Journal of Police Strategies & Management, 23*(3), 303-317.

King, W. R. (2014). Organizational failure and the disbanding of local police agencies. *Crime & Delinquency, 60*(5), 667-692.

Koch, H. (2005). Inter-organizational information system adoption and diffusion: A review and analysis of empirical research. In S. B. Eom (Ed.), *Inter-organizational information systems in the Internet age* (pp. 214-230). Hersey, PA: Idea Group Publishing.

Koestner, L. G. (2008). Law Enforcement Online. *FBI Law Enforcement Bulletin, 77*(10), 21.

Kraska, P. B. (2004). *Theorizing criminal justice*. Long Grove, IL: Waveland Press.

Kumar, N., Stern, L. W., & Anderson, J. C. (1993). Conducting interorganizational research using key informants. *Academy of Management Journal, 36*(6), 1633-1651.

Law Enforcement Enterprise Portal. (n.d.). Retrieved from http://www.cjis.gov/static/CJISEAI/20140502_leep_trifold.pdf

Law Enforcement Online (LEO). (n.d.). Retrieved from https://http://www.leidos.com/justice/leo

Lee, A. S. (1989). A scientific methodology for MIS case studies. *MIS Quarterly, 13*(1), 33-50.

Lee, J., & Rao, H. R. (2007). *Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains*. Paper presented at the 8th Annual International Digital Government Research, Sheraton Society Hill, Philadelphia, PA.

Lin, H.-F. (2014). Understanding the determinants of electronic supply chain management system adoption: Using the technology-organization-environment framework. *Technological Forecasting and Social Change, 86*, 80-92.

Lip-Sam, T., & Hock-Eam, L. (2011). Estimating the determinants of B2B e-commerce adoption among small & medium enterprises. *International Journal of Business and Society, 12*(1), 15-30.

Little, R. J. A. (1992). Regression with missing X's: A review. *Journal of the American Statistical Association, 87*(420), 1227-1237.

Liu, H., Ke, W., Wei, K. K., Gu, J., & Chen, H. (2009). The role of institutional pressures and organizational culture in the firm's intention to adopt internet-enabled supply chain management systems. *Journal of Operations Management, 28*(5), 372-384.

Louie, G., & Von Eckartsberg, G. (2006). Security and liberty: How technology can bridge the divide. In C. Northouse (Ed.), *Protecting what matters: Technology, security, and liberty since 9/11* (pp. 63-73). Washington, DC: Computer Ethics Institute, Brookings Institution Press.

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems, 111*(7), 1006-1023.

Lum, C., Haberfeld, M., Fachner, G., & Lieberman, C. (2009). Police activities to counter terrorism: What we know and what we need to know. In D. Weisburd, T. E. Feucht, I. Hakimi, L. Mock & S. Perry (Eds.), *To Protect and To Serve: Policing in an Age of Terrorism* (pp. 101-141). New York: Springer.

MacLennan, E., & Van Belle, J.-P. (2014). Factors affecting the organizational adoption of service-oriented architecture (SOA). *Information Systems and e-Business Management, 12*(1), 71-100.

Maguire, E. R., Shin, Y., Zhao, J., & Hassell, K. D. (2003). Structural change in large police agencies during the 1990s. *Policing, 26*(2), 251-275.

Maguire, E. R., & Uchida, C. D. (2000). Measurement and explanation in the comparative study of police organizations. In D. Duffee (Ed.), *Measurement and analysis of crime and justice*. Washington, DC: National Institute of Justice.

Manning, P. K. (1992). Technological dramas and the police: Statement and counterstatement in organizational analysis. *Criminology, 30*(3), 327-346.

Manning, P. K. (2001). Technology's ways: Information technology, crime analysis and rationalizing of policing. *Criminal Justice, 1*(1), 83-103.

Manning, P. K. (2008). *The technology of policing: Crime mapping, information technology, and the rationality of crime control*. New York: New York University Press.

Mastrofski, S. D. (1998). Community policing and police organization structure. In J.-P. Brodeur (Ed.), *How to recognize good policing: Problems and issues* (pp. 161-240). Thousand Oaks, CA: Sage.

Mastrofski, S. D., Ritti, R. R., & Hoffmaster, D. (1987). Organizational determinants of police discretion: The case of drinking-driving. *Journal of Criminal Justice, 15*(5), 387-4042.

Mastrofski, S. D., & Uchida, C. D. (1996). Transforming the police. In B. W. Hancock & P. M. Sharp (Eds.), *Public policy, crime, and criminal justice* (pp. 196-219). Upper Saddle River, NJ: Prentice-Hall.

Mathis Beath, C. (1991). Supporting the information technology champion. *MIS Quarterly, 15*(3), 355-372.

Matsunaga, M. (2010). How to factor-analyze your data right: Do's, don'ts, and how-to's. *International Journal of Psychological Research, 3*(1), 97-110.

McClellan, S. E., & Gustafson, B. G. (2012). Communicating law enforcement professionalization: Social construction of standards. *Policing: An International Journal of Police Strategies & Management, 35*(1), 104-123.

McEvily, B., Soda, G., & Tortoriello, M. (2014). More formally: Rediscovering the missing link between formal organization and informal social structure. *The Academy of Management Annals, 8*(1), 299-345.

McGarrell, E. F., Freilich, J. D., & Chermak, S. M. (2007). Intelligence-led policing as a framework for responding to terrorism. *Journal of Contemporary Criminal Justice, 23*(2), 142-158.

McKnight, P. E., McKnight, K. M., Sidani, S., & Figueredo, A. J. (2007). *Missing data: A gentle introduction*. New York: The Guilford Press.

Memorandum for the heads of executive departments and agencies. (2008). Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2008/05/20080509-6.html

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340-363.

Meyer, J. W., & Scott, W. R. (1992). Centralization and the legitimacy problems of local government. In J. W. Meyer & W. R. Scott (Eds.), *Organizational environments: Ritual and rationality* (2nd ed., pp. 199-216). Newbury Park, CA: Sage.

Mobilizing information to prevent terrorism: Accelerating development of a trusted information sharing environment. Third Report of the Markle Foundation Task Force. (2006). New York: Markle Foundation.

Monahan, T., & Palmer, N. A. (2009). The emerging politics of DHS fusion centers. *Security Dialogue, 40*(6), 617-636.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192-222.

Moore, M. H., & Stephens, D. W. (1991). *Beyond command and control: The strategic management of police departments*. Washington, DC: Police Executive Research Forum.

Mullen, K. L. (1996). *The computerization of law enforcement: A diffusion of innovation study.* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 9626420)

Nardi, P. M. (2006). *Doing survey research: A guide to quantitative methods*. Boston, MA: Pearson Education.

National Strategy for Information Sharing and Safeguarding. (2012). Washington, DC.

Norris, D. F., & Moon, M. J. (2005). Advancing e-government at the grassroots: Tortoise or hare? *Public Administration Review, 65*(1), 64-75.

Northrup, A., Kraemer, K. L., & King, J. L. (1995). Police use of computers. *Journal of Criminal Justice, 23*(3), 259-275.

Nunn, S. (2001). Police information technology: Assessing the effects of computerization on urban police functions. *Public Administration Review, 61*(2), 221-234.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation, 14*(1), 110-121.

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of Management Review, 16*(1), 145-179.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science, 3*(3), 398-427.

Orlikowski, W. J., & Barley, S. R. (2001). Technology and institutions: What can research on information technology and research on organizations learn from each other? *MIS Quarterly, 25*(2), 145-165.

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems, 12*(2), 174-207.

Orlikowski, W. J., & Iacono, S. C. (2001). Desperately seeking the "IT" in IT research -- a call to theorizing the IT artifact. *Information Systems Research, 12*(2), 121-134.

Pan, M.-J., & Jang, W.-Y. (2008). Determinants of the adoption of enterprise resource planning within the technology-organization-environment framework: Taiwan's communications industry. *Journal of Computer Information Systems, 48*(3), 94-102.

Pan, Y., Nam, T., Ogara, S., & Lee, S. (2013). Adoption model of mobile-enabled systems in supply chain. *Industrial Management & Data Systems, 113*(2), 171-189.

Pardo, T. A., Gil-Garcia, J. R., & Burke, G. B. (2008). Sustainable cross-boundary information sharing. In H. Chen, L. Brandt, V. Gregg, R. Traunmüller, S. S. Dawes, E. Hovy, A. Macintosh & C. A. Larson (Eds.), *Digital government: E-goverment research, case studies, and implementation* (pp. 421-438). New York: Springer Science+Business Media.

Parker, C. M., & Castleman, T. (2007). New directions for research on SME-eBusiness: Insights from an analysis of journal articles from 2003 to 2006. *Journal of Information Systems and Small Business, 1*(1-2), 21-40.

Parker, C. M., & Castleman, T. (2009). Small firm e-business adoption: A critical analysis of theory. *Journal of Enterprise Information Management, 22*(1/2), 167-182.

Phillips, L. W. (1981). Assessing measurement error in key informant reports: A methodological note on organizational analysis in marketing. *Journal of Marketing Research, 18*(4), 395-415.

Premkumar, G., & Ramamurthy, K. (1995). The role of interorganizational and organizational factors on the decision mode for adoption of interorganizational systems. *Decision Sciences, 26*(3), 303-336.

President's National Strategy on Information Sharing: Successes and challenges in improving terrorism-related information sharing. (2007). Washington, DC: The White House.

Protecting America's freedom in the Information Age. A Report of the Markle Foundation Task Force. (2002). New York: Markle Foundation.

Ramdani, B., Chevers, D., & Williams, D. A. (2013). SME's adoption of enterprise applications: A technology-organisation-environment model. *Journal of Small Business and Enterprise Development, 20*(4), 735-753.

Ramdani, B., Kawalek, P., & Lorenzo, O. (2009). Knowledge management and enterprise systems adoption by SMEs: Predicting SME's adoption of enterprise systems. *Journal of Enterprise Information Management, 22*(1/2), 10-24.

Randol, B. M. (2012). The organizational correlates of terrorism response preparedness in local police departments. *Criminal Justice Policy Review, 23*(3), 304-326.

Randolph, J. J. (2009). A guide to writing the dissertation literature review. *Practical Assessment, Research & Evaluation, 14*(13), 1-13.

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Portland, OR: Willan Publishing.

Ratcliffe, J. H., & Walden, K. (2010). State police and the intelligence center: A study of intelligence flow to and from the street. *IALEIA Journal, 19*(1), 1-19.

Reaves, B. A. (2011a). *Census of State and Local Law Enforcement Agencies, 2008. NCJ 233982*. Washington, DC: Bureau of Justice Statistics, Office of Justice Programs. U.S. Department of Justice.

Reaves, B. A. (2011b). *Tribal law enforcement, 2008. NCJ 234217*. Washington, DC: Bureau of Justice Statistics, Office of Justice Programs. U.S. Department of Justice.

Reaves, B. A. (2012). *Federal law enforcement officers, 2008. NCJ 238250*. Washington, DC: Bureau of Justice Statistics, Office of Justice Programs. U.S. Department of Justice.

Regional Information Sharing Systems (RISS) Program. (n.d.). Retrieved from http://www.riss.net/default/Overview

Relyea, H. C., & Seifert, J. W. (2005). *Information sharing for homeland security: A brief overview (RL32597)*. Washington, DC: Congressional Research Service.

Riley, K. J., Treverton, G. F., Wilson, J. M., & Davis, L. M. (2005). *State and local intelligence in the War on Terrorism*. Santa Monica, CA: RAND Corporation.

Rizzi, C., Ponte, D., & Bonifacio, M. (2009). A new institutional reading of knowledge management technology adoption. *Journal of Knowledge Management, 13*(4), 75-85.

Roberts, A., & Roberts, J. M., Jr. (2007). The structure of information communication between police agencies. *Policing, 30*(1), 93-107.

Roberts, A., Roberts, J. M., Jr, & Liedka, R. V. (2012). Elements of terrorism preparedness in local police agencies, 2003-2007: Impact of vulnerability, organizational characteristics, and contagion in the post-9/11 era. *Crime & Delinquency, 58*(5), 720-747.

Roberts, D. J. (2004). *Integration in the context of justice information systems: A common understanding*. Sacromento, CA: SEARCH, The National Consortium for Justice Information and Statistics.

Rocheleau, B. (2006). *Public management information systems*. Hersey, PA: Idea Group.

Rogelberg, S. G., & Stanton, J. M. (2007). Understanding and dealing with organizational survey nonresponse: Introduction. *Organizational Research Methods, 10*(2), 195-209.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York: Free Press.

Roy, C., & Séguin, F. (2000). The institutionalization of efficiency-oriented approaches for public service improvement. *Public Productivity & Management Review, 23*(4), 449-468.

Rubin, D. B. (1976). Inference and missing data. *Biometrika, 63*(3), 581-592.

Ryan, S. D., & Prybutok, V. R. (2001). Factors affecting the adoption of knowledge management technologies: A discriminative approach. *The Journal of Computer Information Systems, 41*(4), 31-37.

Saviak, J. (2007). *An investigation into the predictors of adoption and utilization of information-sharing networks by local law enforcement in three states.* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3302937)

Schaefer Morabito, M. (2010). Understanding community policing as an innovation: Patterns of innovation. *Crime & Delinquency, 56*(4), 564-587.

Schafer, J. A., Burruss, G. W., & Giblin, M. J. (2009). Measuring homeland security innovation in small municipal agencies: Policing in a 9/11 world. *Police Quarterly, 12*(3), 263-288.

Schafer, J. L., & Graham, J. W. (2002). Missing data: Our view of the state of the art. *Psychological Methods, 7*(2), 147-177.

Schaible, L. M., & Sheffield, J. (2012). Intelligence-led policing and change in state law enforcement agencies. *Policing: An International Journal of Police Strategies & Management, 35*(4), 761-784.

Schlegel, K. (2000). Transnational crime: Implications for local law enforcement. *Journal of Contemporary Criminal Justice, 16*(4), 365-385.

Schwartz, J. C. (2009). Myths and mechanics of deterrence: The role of lawsuits in law enforcement decisionmaking. *UCLA Law Review, 57*(4), 1023-1094.

Scott, W. R. (2008). Approaching adulthood: The maturing of institutional theory. *Theory and Society, 37*(5), 427-442.

Scott, W. R. (2013). *Institutions and organizations: Ideas, interests, and identities* (4th ed.). Thousand Oaks, CA: Sage.

Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology, 1*(3), 307-332.

Shih, T.-H., & Fan, X. (2008). Comparing response rates from web and mail surveys: A meta-analysis. *Field Methods, 20*(3), 249-271.

Sila, I. (2013). Factors affecting the adoption of B2B e-commerce technologies. *Electronic Commerce Research, 13*(2), 199-236.

Sila, I., & Dobni, D. (2012). Patterns of B2B e-commerce usage in SMEs. *Industrial Management & Data Systems, 112*(8), 1255-1271.

Silverman, E. B. (2006). Comstat's innovation. In D. Weisburd & A. A. Braga (Eds.), *Policing innovation: Contrasting perspectives* (pp. 267-283). Cambridge, UK: Cambridge University Press.

Singer, E., & Couper, M. P. (2008). Do incentives exert undue influence on survey participation? Experimental evidence. *Journal of Empirical Research on Human Research Ethics, 3*(3), 49-56.

Skogan, W. G. (2008). Why reforms fail. *Police & Society, 18*(1), 23-34.

Skogan, W. G., & Frydl, K. (Eds.). (2004). *Fairness and effectiveness in policing: The evidence*. Washington, DC: National Research Council.

Skogan, W. G., & Hartnett, S. M. (2005). The diffusion of information technology in policing. *Police Practice and Research, 6*(5), 401-417.

Skolnick, J. (1966). *Justice without trial: Law enforcement in a democratic society*. New York: John Wiley & Sons.

Small, K., & Taylor, B. (2006). State and local law enforcement response to transnational crime. *Trends in Organized Crime, 10*(2), 5-17.

Soares-Aguiar, A., & Palma-dos-Reis, A. (2008). Why do firms adopt e-procurement systems? Using logistic regression to empirically test a conceptual model. *IEEE Transactions on Engineering Management, 55*(1), 120-133.

Stinchcombe, A. L. (1968). *Constructing social theories*. New York: Harcourt, Brace & World.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Journal, 20*(3), 571-610.

Swanson, R. A. (2005). The challenge of research in organizations. In R. A. Swanson & E. F. Holton III (Eds.), *Research in organizations: Foundations and methods of inquiry* (pp. 3-10). San Francisco: Berrett-Koehler.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53-55.

Taylor, R. W., & Russell, A. L. (2012). The failure of police "fusion" centers and the concept of a national intelligence sharing plan. *Police Practice and Research, 13*(2), 184-200.

Tolbert, P. S., & Zucker, L. G. (1983). Institutional sources of change in the formal structure of organizations: The diffusion of civil service reform, 1880-1935. *Administrative Science Quarterly, 28*(1), 22-39.

Tornatzky, L. G., Eveland, J. D., Boylan, M. G., Hetzner, W. A., Johnson, E. C., Roitman, D., & Schneider, J. (1983). *The process of technological innovation: Reviewing the literature*. Washington, DC: National Science Foundation, Productivity Improvement Research Section.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington, MA: Lexington Books.

Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management, 29*(1), 28-45.

Tushman, M., & Nadler, D. (1986). Organizing for innovation. *California Management Review, 18*(3), 74-92.

Tweel, A. (2012). *Examining the relationship between technological, organizational, and environmental factors and cloud computing adoption.* (Doctoral dissertation). Available from ProQuest Dissertation and Theses Full Text. (UMI No. 3529668)

Valledor, J. C. (2010). *Connecting the dots: Enduring challenges in the nation's information sharing environment*. Fort Leavenworth, KS: U.S. Army Command and General Staff College, School of Advanced Military Studies.

Van Huy, L., Rowe, F., Truex, D., Robinson, J. M., & Huynh, M. Q. (2012). An empirical study of determinants of e-commerce adoption in SMEs in Vietnam: An economy in transition. *Journal of Global Information Management, 20*(3), 23-54.

Vaughn, M. S., Cooper, T. W., & del Carmen, R. V. (2001). Assessing legal liabilities in law enforcement: Police chiefs' views. *Crime & Delinquency, 47*(1), 3-27.

Venkatesh, V., & Bala, H. (2012). Adoption and impacts of interorganizational business process standards: Role of partnering synergy. *Information Systems Research, 23*(4), 1131-1557.

Weisburd, D., & Lum, C. (2005). The diffusion of computerized crime mapping in policing: Linking research and practice. *Police Practice and Research, 6*(5), 419-434.

Weisburd, D., Mastrofski, S. D., McNally, A. M., Greenspan, R., & Willis, J. J. (2003). Reforming to preserve: Compstat and strategic problem solving in American policing. *Criminology and Public Policy, 2*(3), 421–456.

Weiss, A. (1997). The communication of innovation in American policing. *Policing: An International Journal of Police Strategies & Management, 20*(2), 292-310.

Weiss, A. (1998). *Informal information sharing among police agencies*. Washington, D.C.: National Institute of Justice.

Wejnert, B. (2002). Integrating models of diffusion of innovations: A conceptual framework. *Annual Review of Sociology, 28*, 297-326.

What is HSIN? (n.d.). Retrieved from http://www.dhs.gov/what-hsin

White, J. R. (2004). *Defending the homeland: Domestic intelligence, law enforcement, and security*. Belmont, CA: Wadsworth/Thompson Learning.

Willis, J. J., & Mastrofski, S. D. (2011). Innovations in policing: Meanings, structures, and processes. *Annual Review of Law and Social Science, 7*, 309-334.

Willis, J. J., Mastrofski, S. D., & Weisburd, D. (2007). Making sense of COMPSTAT: A theory-based analysis of organizational change in three police departments. *Law & Society Review, 41*(1), 147-188.

Wilson, J. M. (2005). *Determinants of community policing: An open systems model of implementation*. Washington, DC: U.S. Department of Justice, National Institute of Justice.

Wilson, J. M. (2006). *Community policing in America*. New York, NY: Routledge.

Wilson, J. M., & Heinonen, J. A. (2011). Advancing a police science: Implications from a national survey of police staffing. *Police Quarterly, 14*(3), 277-297.

Wilson, J. Q. (1968). *Varieties of police behavior: The management of law and order in eight communities*. Cambridge, MA: Harvard University Press.

Wilson, J. Q. (1989). *Bureaucracy: What government agencies do and why they do it*. New York: Basic Books.

Wilson, T. P. (1974). Measures of association for bivariate ordinal hypotheses. In H. M. Blalock (Ed.), *Measurements in the social sciences: Theories and strategies* (pp. 327-342). Chicago: Aldine Publishing.

Wolfe, R. A. (1994). Organizational innovation: Review, critique and suggested research directions. *Journal of Management Studies, 31*(3), 405-431.

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly, 28*(2), 164-175.

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Thousand Oaks, CA: Sage.

Zhang, C., & Dhaliwal, J. (2009). An investigation of resource-based and institutional theoretic factors in technology adoption for operations and supply chain management. *International Journal of Production Economics, 120*(1), 252-269.

Zhang, J., & Dawes, S. S. (2006). Expectations and perceptions of benefits, barriers, and success in public sector knowledge networks. *Public Performance & Management Review, 29*(4), 433-466.

Zhang, J., Dawes, S. S., & Sarkis, J. (2005). Exploring stakeholders' expectations of the benefits and barriers of e-government knowledge sharing. *Journal of Enterprise Information Management, 18*(5), 548-567.

Zhu, K., Kraemer, K., & Xu, S. (2003). Electronic business adoption by European firms: A cross-country assessment of the facilitators and inhibitors. *European Journal of Information Systems, 12*(4), 251-268.

Zorn, T. E., Flanagin, A. J., & Shoham, M. D. (2011). Institutional and noninstitutional influences on information and communication technology adoption and use among nonprofit organizations. *Human Communication Research, 37*(1), 1-33.

Zucker, L. G. (1983). Organizations as institutions. In S. B. Bacharach (Ed.), *Research in the sociology of organizations* (Vol. 2, pp. 1-47). New York: JAI Press.

Zucker, L. G. (1987). Institutional theories of organization. *Annual Review of Sociology, 13*, 443-464.

Zwick, W. R., & Velicer, W. F. (1986). Comparison of five rules for determining the number of components to retain. *Psychological Bulletin, 99*(3), 432-442.