REFLECTIONS OF IDENTITY: HOW INFORMATION SYSTEMS MIRROR THE ORGANIZATION AS A SOCIAL ACTOR

A Dissertation in
Information Sciences & Technology

by
Michael J. Tyworth

© 2009 Michael J. Tyworth

Submitted in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

December 2009
The dissertation of Michael J. Tyworth was reviewed and approved by the following:

Andrea H. Tapia  
Assistant Professor of Information Sciences & Technology  
Dissertation Co-Advisor  
Co-Chair of Committee

Steven B. Sawyer  
Associate Professor of Information Studies  
Dissertation Co-Advisor  
Co-Chair of Committee

Barbara Gray  
Professor of Organizational Behavior

Sandeep Purao  
Associate Professor of Information Sciences & Technology

James B. Thomas  
Professor of Information Sciences & Management

Henry C. “Hank” Foley  
Dean, College of Information Sciences & Technology

*Signatures are on file in the Graduate School
Abstract

Through this research I pursue answers to two research questions. One, what is the role of an organization’s identity – that which is central, enduring, and unique about an organization – in shaping the ways organizations design and arrange information technologies? Two, what properties do organizational information technologies exhibit as facilitators of cross-boundary communication? I am motivated to pursue these questions because information technologies are central to modern organizational life, yet effective design and implementation remains a significant organizational challenge. The centrality of information technology to organizational life is particularly evident in the public safety domain where public safety agencies are struggling to overcome a high degree of institutionalized segregation of information systems. In order to more effectively design, build, and implement organizational information systems, it is critical that we develop a better understanding of how organizational life shapes, and is shaped by, the organization’s technologies.

This research makes use of multiple qualitative methods. Case studies of the Automated Regional Justice Information System and the Pennsylvania Justice Network provide micro-level detail. Secondary data situates the case studies in a broader institutional context. Analytic induction was used to test hypotheses across the cases. Two findings emerged from the analysis. One, the features and configurations of organizational ICT reflect the identities of the organizations that build and implement them. Two, the specific boundary-spanning properties organizational information technologies exhibit are linked to the nature of the boundaries spanned.

Three implications emerge from the findings presented in this dissertation. One, the influence of organizational identity on organizational information technologies means that
attempts to integrate various IJIS on a large scale (e.g., national or global) will prove very difficult. Two, the degree to which an information technology is successfully implemented in an organization is in part determined by the degree to which the design aligns with the organization’s identity. Three, design of organizational information technologies requires attention to the nature of the boundaries the systems will span.
Acknowledgements

Many individuals helped me bring this dissertation to fruition, and I cannot possibly acknowledge all of them, and all the ways they assisted me, without adding significantly to what is already too long of a manuscript. However, I would like to particularly thank the following individuals:

I would not have been able to complete this dissertation without the invaluable support and assistance of my dissertation committee co-chairs Dr. Steve Sawyer and Dr. Andrea Tapia. Steve’s seemingly endless patience and constant support made a critical difference in completing this work. As my graduate advisor, Steve helped me grow as a scholar by exposing me to different perspectives and challenging me to be more articulate and sharper in my reason. Andrea was invaluable to me in two ways. One, she agreed to become my co-chair which enabled me to continue and finish my dissertation work at Penn State. Two, she would never tolerate my penchant for self-doubt and as a result always left me motivated to work harder whenever we discussed my thesis.

I would also like to acknowledge the members of my dissertation committee: Dr. Barbara Gray, Dr. Sandeep Purao, and Dr. James B. Thomas who lent me their valuable time and guidance both as a student and during the completion of this dissertation.

My parents both played important roles in this journey. To a large extent, I was motivated to pursue this degree because I wanted to be like my father, Dr. John E. Tyworth. Having completed this stage of my career, I can only hope that I am as successful as he has been as both a scholar and a parent. My mother gave me the final impetus to embark upon my graduate career with her pithy insight: “Who cares if you’ll be forty and just getting out of school? You’re going to be 40 anyway, so do what you want to do!” And here I am Mom, 40 years old and just getting out of graduate school!

Finally, I want to acknowledge my wife Lori, my stepson Andrew, and my daughter Katherine. Without my wife’s sacrifice, indulgence, and patience this dissertation would not have been possible. My son Andrew’s persistent questions of “How’s the dissertation going Dad?” and “Are you going to defend yet?” served as a continual reminder to get to work! And my beautiful baby girl Katherine served as the ultimate inspiration to get going and get done.

This work was funded in part by grants IIS-05-0742687 and IIS-05-34889 from the National Science Foundation.
# Table of Contents

LIST OF FIGURES ................................................................................................................................. X

LIST OF TABLES ................................................................................................................................. XI

CHAPTER 1 INTRODUCTION TO DISSERTATION .................................................................................. 1

  INTRODUCTION ................................................................................................................................. 1
  MOTIVATION AND CONTRIBUTIONS ................................................................................................. 5
  STRUCTURE OF THESIS ....................................................................................................................... 7

CHAPTER 2 PRIOR EMPIRICAL WORK ON POLICING & TECHNOLOGY ...................................................... 10

  INTRODUCTION ................................................................................................................................. 10
  POLICING & TECHNOLOGY ................................................................................................................ 11
    The Institutional Complexity of U.S. Law Enforcement .................................................................... 14
    The Need for Integration ................................................................................................................... 17
  Government action after 9/11 and Hurricane Katrina ...................................................................... 18
  INTEGRATED CRIMINAL JUSTICE INFORMATION SYSTEMS ......................................................... 19
  THE NEED FOR FURTHER EMPIRICAL EVALUATION ................................................................... 22
  CONCLUSION ....................................................................................................................................... 25

CHAPTER 3 THE SOCIAL INFORMATICS PERSPECTIVE ........................................................................... 27

  INTRODUCTION ................................................................................................................................... 27
  WHAT IS SOCIAL INFORMATICS? ......................................................................................................... 28
    Information, Technology, & People ..................................................................................................... 30
    Social Informatics Principles .............................................................................................................. 34
    Challenges .......................................................................................................................................... 36
    Epistemological & Theoretical Implications ..................................................................................... 38
    This dissertation as social informatics research .............................................................................. 40
  CONCLUSION ....................................................................................................................................... 40

CHAPTER 4 THEORETICAL FRAMING ....................................................................................................... 42

  INTRODUCTION ................................................................................................................................... 42
  ORGANIZATIONAL IDENTITY ............................................................................................................. 42
    Organizational Identity Defined ......................................................................................................... 42
    Organizational Culture & Image ......................................................................................................... 46
    Prior Research on Organizational Identity ....................................................................................... 48
    Organizational Identity as a Shaper of ICT ....................................................................................... 49
  BOUNDARY OBJECTS ........................................................................................................................ 51
    Boundary Objects Defined ................................................................................................................. 51
    Prior Research on Boundary Objects ............................................................................................... 54
    IJIS as Boundary Objects ............................................................................................................... 55
  CONCLUSION ....................................................................................................................................... 55

CHAPTER 5 RESEARCH DESIGN ............................................................................................................... 56

  INTRODUCTION ................................................................................................................................... 56
  RATIONALE FOR RESEARCH DESIGN ............................................................................................. 56
CHAPTER 6 DATA COLLECTION & ANALYSIS ................................................................. 75

INTRODUCTION ........................................................................................................... 75

DATA COLLECTED ...................................................................................................... 75

Revised Data Collection Strategy ............................................................................. 75

Interviews ..................................................................................................................... 76

ARJIS ............................................................................................................................ 78

JNET .............................................................................................................................. 79

A note about the number of interviews ................................................................... 80

Document Analysis .................................................................................................... 81

Direct Observation ..................................................................................................... 82

Secondary Data .......................................................................................................... 83

ANALYSIS OF DATA .................................................................................................. 84

Analytic Induction ....................................................................................................... 87

CONCLUSION .............................................................................................................. 88

CHAPTER 7 – CASE STUDY: AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM (ARJIS) ................................................................. 90

INTRODUCTION ........................................................................................................... 90

WHAT IS ARJIS? .......................................................................................................... 90

ORIGINATION OF ARJIS ............................................................................................. 90

THE ARJIS ORGANIZATION ...................................................................................... 93

Organizational Structure .......................................................................................... 93

ARJIS Governance ...................................................................................................... 96

THE ARJIS TECHNICAL ARCHITECTURE ................................................................ 99

Hardware .................................................................................................................... 99

Software ....................................................................................................................... 101

Networking ................................................................................................................ 104

Architecture ............................................................................................................... 105
# INTRODUCTION

Contributions to scholarship .......................................................... 184
Contribution to social informatics ....................................................... 184
Empirical contributions .................................................................... 185

# IMPLICATIONS

Implications for theory ....................................................................... 187
Implications for practice .................................................................... 189
Implications specific to Criminal Justice & Policing .......................... 190

# LIMITATIONS AND NEED FOR FUTURE RESEARCH

This research going forward ............................................................... 191

# APPENDIX A – INITIAL INTERVIEW GUIDES

# APPENDIX B – FOLLOW-UP INTERVIEW GUIDES

# APPENDIX C – ARJIS APPLICATIONS

# APPENDIX D – JNET APPLICATIONS

# APPENDIX E – JNET PROJECT PRIORITY MATRIX

# APPENDIX F – LIST OF ACRONYMS

# APPENDIX G – LESSONS LEARNED

Detailed planning is critical to quality research ................................. 207
Research must be properly scoped .................................................... 208
Data collection is more effective when it is more structured ............... 208

# REFERENCES


List of Figures

FIGURE 1-1 STRUCTURE OF THESIS ........................................................................................................8
FIGURE 3-1 CONCEPTUALIZING THE DOMAIN. ....................................................................................31
FIGURE 3-2 APPROACHES TO THE STUDY OF ICT. .............................................................................33
FIGURE 4-1 DYNAMICS OF ORGANIZATIONAL CULTURE, IDENTITY, AND IMAGE. .........................48
FIGURE 6-1 ANALYTICAL PROCESS ..................................................................................................85
FIGURE 6-2 EXAMPLE OF DOCUMENTARY EVIDENCE. .....................................................................87
FIGURE 7-1 THE ARJIS GOVERNANCE STRUCTURE. .........................................................................94
FIGURE 7-2 ARJIS OPERATING BUDGET 2005-2010 .........................................................................96
FIGURE 7-3 ARJIS PROJECT BUDGET 2005-2010 ..............................................................................97
FIGURE 7-4 ARJIS EXPENDITURES BY CATEGORY (2005-2010). .......................................................98
FIGURE 7-5 ARJIS TOTAL EXPENDITURES BY TYPE. .........................................................................98
FIGURE 7-6 CHANGES IN ARJIS BUDGET OVER TIME ....................................................................99
FIGURE 7-7 THE ARJIS NETWORK ARCHITECTURE. .......................................................................101
FIGURE 7-8 THE ARJIS ENTERPRISE PROJECT DESIGN. ..................................................................104
FIGURE 8-1 HISTORY OF JNET .........................................................................................................109
FIGURE 8-2 GROWTH OF JNET USER BASE OVER TIME ..................................................................110
FIGURE 8-3 THE JNET GOVERNANCE STRUCTURE .......................................................................111
FIGURE 8-4 JNET OPERATING BUDGET 1999-2009 .......................................................................115
FIGURE 8-5 JNET OPERATING BUDGET TRENDS. ..........................................................................116
FIGURE 8-6 JNET NETWORK ARCHITECTURE. ..............................................................................120
FIGURE 9-1 ARJIS’ GOVERNANCE STRUCTURE REFLECTS ITS COLLABORATIVE IDENTITY. ..........131
FIGURE 9-2 ORGANIZATIONAL IDENTITY SHAPES DESIGN OUTCOMES ......................................134
FIGURE 9-3 THE JNET PROJECT SCORING MATRIX ....................................................................150
FIGURE 9-4 THE JNET SYSTEM ARCHITECTURE. ..........................................................................152
FIGURE 9-5 THE JNET ENTERPRISE PORTAL APPLICATION ........................................................153
FIGURE 9-6 THE JNET MESSAGING APPLICATION ........................................................................155
FIGURE 10-1 THE ARJIS AND JNET BOUNDARY OBJECTS. ............................................................161
FIGURE 10-2 THE ARJIS PUBLIC CRIME MAPPING APPLICATION. ...............................................168
FIGURE 10-3 "FAST FACTS" FROM A REPORT GENERATED USING ARJIS DATA. ......................170
FIGURE 10-4 THE JNET ENTERPRISE PORTAL APPLICATION .........................................................178
List of Tables

TABLE 1-1 RESEARCH QUESTIONS ..........................................................................................................................5
TABLE 2-1 PROPERTIES OF IJIS ............................................................................................................................21
TABLE 3-1 PRINCIPLES OF SOCIAL INFORMATICS ...............................................................................................35
TABLE 4-1 COMPONENTS OF ORGANIZATIONAL IDENTITY ................................................................................45
TABLE 4-2 ORGANIZATIONAL IDENTITY PROPOSITIONS ..................................................................................50
TABLE 4-3 TYPES OF BOUNDARY OBJECTS ........................................................................................................53
TABLE 5-1 DEFINING THE PHENOMENON OF INTEREST ..................................................................................69
TABLE 5-2 SAMPLING CRITERIA ..........................................................................................................................71
TABLE 5-3 ESTABLISHING VALIDITY....................................................................................................................74
TABLE 6-1 SOURCES OF EVIDENCE ....................................................................................................................75
TABLE 6-2 DETAILED BREAKDOWN OF DOCUMENTARY EVIDENCE .................................................................82
TABLE 6-3 DETAILED BREAKDOWN OF DIRECT OBSERVATIONS .....................................................................82
TABLE 8-1 JNET GOVERNANCE COMMITTEE MEMBERSHIP .............................................................................113
TABLE 9-1 ELEMENTS OF ARJIS’ ORGANIZATIONAL IDENTITY .................................................................123
TABLE 9-2 ELEMENTS OF JNET’S ORGANIZATIONAL IDENTITY .................................................................141
TABLE 9-3 DIFFERENCES IN IDENTITY ARE REFLECTED IN DESIGN DIFFERENCES .........................................156
TABLE 10-1 TYPES OF BOUNDARY OBJECTS ....................................................................................................159
TABLE 10-2 PROPERTIES OF BOUNDARY OBJECTS ............................................................................................160
TABLE 10-3 COMPARISON OF TWO JNET USER ROLES ....................................................................................179
Chapter 1 Introduction to Dissertation

Introduction

Through this dissertation I develop a greater understanding of the design and use of complex inter-organizational information and communications technologies (ICT). Specifically, this dissertation answers, at least in part, two overarching research questions. One, how do organizational ICT reflect organizational traits such as identity? And two, what forms do inter-organizational ICT adopt to facilitate communication and collaboration among heterogeneous groups?

I pursued research on these questions because ICT are ubiquitous in organizations, and therefore understanding how organizations engage ICT is important to the understanding and improving of organizational life. Forms of organizational ICT are almost as varied as the organizations themselves; often tailored to specific organizational needs or attributes. Idiosyncratic organizational information systems remain prevalent even with the advent of systems that advocate the application of generic best practices such as enterprise resource planning systems (Brehm, Heinzl, & Markus, 2001; Truex, Baskerville, & Klein, 1999). With the advent of modern inter-networking technologies, our governments and industries have placed increasing emphasis on integrating heterogeneous systems to improve efficiency of service.

Integration of government ICT has been, and continues to be, a policy objective at all levels of government (Raths, 2007; Towns, 2009). One area of government that has been particularly active in trying to integrate heterogeneous ICT is public safety. Though not a new goal – the U.S. government has made integration of criminal justice information systems a policy goal since the 1960’s (Dunworth, 2005), particular emphasis has recently been placed on the integration of ICT in the criminal justice – law enforcement – public safety. Recent events such
as the terrorist attacks on September 11th and Hurricane Katrina, as well as pressing sociopolitical issues such as border security and immigration, have resulted in an increased policy emphasis on system integration. Currently, there are numerous efforts to increase the degree of integration among heterogeneous information systems among law enforcement and public safety agencies ongoing within the United States. These complex technological and organizational architectures, often referred to as an integrated criminal justice information system (IJIS), generally involves both an organizational and a technological component (National Association of State Chief Information Officers (NASCIO), 2003).

What we know about these efforts to develop IJIS is that the approaches to IJIS design are varied. Research to date has shown that IJIS initiatives vary in both their approach to design, the ways in which systems, devices, and applications are configured, and in governance and administration (Gil-Garcia, Schneider, & Pardo, 2004; Tyworth & Sawyer, 2006; C. B. Williams et al., 2009). Why this variance occurs, and how this variance impacts the IJIS design and action remain outstanding questions. To help answer these questions, I have chosen the theoretical lenses of organizational identity and boundary objects. I have chosen these theories for two reasons. One, evidence suggests that key sources of variance in the design of IJIS are local organizational characteristics such as identity. Two, boundary objects theory is an intuitive way for describing how collaborative work is accomplished by heterogeneous groups of the kind we see in public safety.

Organizational identity is collectively perceived by an organization’s members to be what is central, enduring, and unique about the organization (Albert & Whetten, 1985; Whetten,

---

1 The exact number of IJIS initiatives currently in operation within the United States is exceedingly difficult to determine as IJIS occur at all levels of government (local, county, regional, state) and many are unknown outside their local jurisdiction.
Organizational identity shapes the behavior of organizational members in a number of ways including organizational identification (the degree to which members see themselves as belonging to the organization), response to ambiguity or organizational threats, and branding. Organizational identity reflects and is reflected in both the organizational culture – shared, often tacit understandings of organizational values, and the organizational image – how outsiders perceive the organization (Hatch & Schultz, 2002). Members of an organization draw on their perception of the organization’s identity to differentiate their organization from others and to guide organizational action.

Information and communications technologies that are designed, configured, and employed by an organization are artifacts of that organization (Leidner & Kayworth, 2006). Given that organizational identity shapes both an organization’s action and its culture, it is reasonable to expect that the unique attributes of any organization’s identity are reflected in both its actions, and in its artifacts. Therefore, organizational identity seems likely to be a contributor to the variance in IJIS design. To this end this research focused on understanding the influence of organizational identity on IJIS development in three ways:

1. How are the organizational identities of IJIS reflected in their organizational attributes?
2. How do IJIS-specific identities get manifested in IJIS-specific design practices?
3. How do the designs of IJIS systems, devices, and applications reflect their unique identity?

Combined, these questions speak to how organizational identity serves to shape both organizational structure and organizational action.
But how do differences in IJIS design impact the way IJIS act? Since IJIS span many organizations, levels of government and geographical boundaries – as well as serve multiple constituencies including government, police, and the public – one place to look for how differences in design impact IJIS action is in how they span these communities. The concept of a boundary object is useful for this purpose.

Boundary objects are people, places, practices and artifacts that facilitate communication across social boundaries (Star, 1989). The essence of a boundary object is that people belong to communities or social worlds – groups, organizations, societies, paradigms, disciplines, etc. – that are centered around joint or common activity and bounded together by a network of communication (Fleischmann, 2006a). Further, because communities have their own languages, methods, and understandings, boundary objects are needed to facilitate communication with other social worlds across their boundaries. In prior research, scholars have applied boundary objects to the study of how quality control teams collaborate with customers (Lutters & Ackerman, 2007), how groups with different operational responsibilities engage design (Carlile, 2002), and how anatomical simulations bridge the world of programmers, animal rights activists, and educators (Fleischmann, 2006a). Boundary objects theory has proven useful in the past as a tool for explaining how technologies can facilitate communication among heterogeneous groups which is why I chose it as one of the theoretical lenses for this research.

In this research I examine the ways IJIS serve as boundary objects to diverse constituencies. Specifically I sought to understand IJIS as boundary objects in two ways:

1. In what ways do IJIS serve the role of boundary object among various social worlds such as governments, publics, and systems?
2. What are the properties of IJIS boundary objects?

In answering these questions this dissertation provides insight into IJIS as boundary-spanning systems. Specifically, the answers to these questions inform us of the different communities IJIS span, how IJIS facilitate communication and collaboration among those communities, and how differences in system design translate into differences in the boundary-spanning properties of IJIS.

<table>
<thead>
<tr>
<th>General Research Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RQ1</strong></td>
</tr>
<tr>
<td><strong>RQ2</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organizational Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OI1</strong></td>
</tr>
<tr>
<td><strong>OI2</strong></td>
</tr>
<tr>
<td><strong>OI3</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Boundary Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BO1</strong></td>
</tr>
<tr>
<td><strong>BO2</strong></td>
</tr>
</tbody>
</table>

**Table 1-1 Research Questions**

**Motivation and Contributions**

I pursue this research for three reasons. One, there is a practical need to understand why current IJIS initiatives vary in their approaches to design so that policymakers may make more informed decisions about how to approach the supremely challenging problem of large-scale
integration of heterogeneous criminal justice information systems. Two, there has been an identified need for development of both organizational identity and boundary objects theory in order to increase their validity as concepts and utility as theoretical lenses. Three, I am motivated to contribute to social informatics research by adding to the body of empirical evidence of the socio-technical nature of ICT and by offering a new theoretical approach to the understanding of organizational ICT.

The purpose of this dissertation is therefore, to contribute to our understanding of ICT as complex socio-technical systems by examining the influence of organizational identity on design processes; and to enhance our understanding of how inter-organizational socio-technical systems act in a boundary-spanning capacity. One contribution implicit in this purpose is the demonstration of the utility of organizational identity as a means to understand social influences on the design of organizational ICT. There are at least three other contributions of this research.

One, this research also contributes to our understanding of organizational life by tying the theory of organizational identity to a critical component of organizational life – information and communications technologies. This contribution is enhanced by the potential of future research to show that as organizational identity becomes structurally entrenched in the ICT of the organization, existing ICT serve as identity-affirming structures that constrain future organizational behavior related to the development and use of ICT.

Two, this research contributes to social informatics through the application of organizational identity theory to ICT. Theory building (and arguably extension) is considered to be a key step in the institutionalization of social informatics as a scholarly approach (Sawyer & Tapia, 2007). This research serves to add to the social informatics theoretical toolkit through its
application of organizational identity theory to the study of ICT. This research also may serve to provide the basis for the building of new theory through future research on the impact of identity (individual, organizational, cultural) on the design and use of ICT.

Three, this dissertation makes an empirical contribution through the case studies of ARJIS and JNET. In particular these cases add new knowledge of ARJIS’ and JNET’s organizational identities and their approaches to system development. These cases also add to the empirical record of police ICT which to a large extent has focused on internal organizational systems or the technologies employed by individual officers.

**Structure of Thesis**

This dissertation is organized into eleven chapters within four larger sections organized by theme. The first section – comprised of chapters 2, 3, and 4 – presents a review of the extant literature. Three objectives are accomplished within this section. One, the ontological and epistemological basis for this work is established via a presentation and discussion of social informatics research. Two, a theoretical framework is built for this problem through synthesis of the organizational identity and boundary objects literature. Three, I establish the setting for this research: policing and ICT. Here I detail both historical and current practices that have contributed to the problem of integrating criminal justice information systems; define the IJIS concept; and discuss why there is a key need to understand what is currently happening in IJIS development.
The second section of this dissertation presents the research design and a summary and discussion of the collection and analysis of data performed in the process of completing this dissertation. In Chapter 5 I define the level of analysis, the relevant constructs, the methods of data collection and analysis, and the rationale behind the choosing of the ARJIS and JNET systems for case study. In Chapter 6 I summarize and discuss the actual collection of data. Additionally, modifications to the proposed research design once initial data collection began are presented and justified.

The third section is the empirical section of this dissertation. The ARJIS and JNET case studies (Chapters 7 and 8 respectively) are presented in detail and situated in a broader macro-level context. Both a historical and current account is given of these organizations.

The fourth section is the analysis section. Here I present the findings from the conducted research. Chapter 9 presents findings pertaining to organizational identity and the design of ICT and Chapter 10 presents findings pertaining to IJIS as boundary objects. I have segregated the findings this way for clarity.

I conclude this dissertation with a discussion of conclusions about the performed research, applications, limitations, and promising avenues future research in Chapter 11. In
particular I note the potential for further theoretical development of organizational identity as it pertains to ICT.
Chapter 2 Prior Empirical Work on Policing & Technology

Introduction

In this chapter I examine the role of ICT in policing and criminal justice organizations and emphasize the role of technology in criminal justice and detail the technological and institutional factors that have contributed to the push to develop integrated criminal justice information systems\(^2\). In conducting this review I make the case for integrated IJIS as the phenomena of interest of this research, detail the institutional nature of criminal justice in the United States, and review police use of ICT historically.

The criminal justice community in general, and law enforcement in particular, has long embraced technology as a tool to serve organizational purposes (Manning, 2003a, p. 123). A review of the literature shows that policymakers and criminal justice professionals have identified the need to integrate the multitude of information and communications technologies employed by criminal justice agencies. These same commentators have identified the complexity of law enforcement’s organizational structures and institutional practices as critical issues that must be addressed simultaneously with technological change as part of the integration process; and have offered recommendations on strategies for doing so. While there is a significant volume of – sometimes conflicting – prescription for how to integrate ICT systems among law enforcement agencies, there is a substantial lack of empirical analysis of the results of integration initiatives and minimal coordination of integration efforts nationally.

\(^2\) It is worth noting here the relationship of law enforcement to criminal justice. In general, criminal justice is viewed to be the broader domain of agencies and institutions involved in the administration of justice and the enforcement of law. Law enforcement is a component of the criminal justice system. I emphasize law enforcement in this chapter because of the centrality of law enforcement operations to the criminal justice system in general and IJIS specifically
The remainder of this chapter is developed in three sections. First is a review of the role of technology in the conducting of policing activity within the United States. This review focuses on the historical use of ICT by law enforcement as well as current trends in law enforcement information technology. Through this review I will establish that the use of ICT as a fundamental component of policing activity.

Second is an analysis of the institutional complexity of law enforcement in the United States. This review will show that there is a high level of institutional complexity in U.S. law enforcement. Further, that this institutional complexity has directly contributed to historical and current ICT-related practices among law enforcement resulting in the subsequent policy emphasis on the need for integration of ICT across law enforcement agency boundaries.

Third, I will examine the current socio-political emphasis on integrating law enforcement ICT that has resulted in ongoing efforts to develop and deploy integrated criminal justice information systems (IJIS). Through this examination I will show that the development of IJIS continues to be a priority of policymakers resulting in significant resources being devoted to the task. Finally, though integration of law enforcement technologies has been made a policy priority, there is a shortage of empirical analysis of the outcomes of integration initiatives.

Policing & Technology
Law enforcement has employed ICT for over seventy years. Information and communications technologies have been and continue to be used by law enforcement agencies for the purposes of crime analysis, crime prevention, and agency administration. For example, one of the earliest ICT to be employed by law enforcement agencies was the paper map of a jurisdiction and push-pins to monitor crime activity trends within it (Maguire & King, 2004; 3

3 In this dissertation I treat ‘policing’ and ‘law enforcement’ synonymously.
Though paper map and push pins is an admittedly simple contrast to the complex technologies employed by modern police agencies, the example serves to demonstrate how police have long sought to develop and use ICT for operational purposes.

Today, law enforcement has adopted a variety of different ICT including radios, cellular phones, wireless computing, computer-aided dispatch (CAD) systems, electronics record management systems (RMS), biometric scanners, and others (Dunworth, 2005). These systems are used for a variety of purposes including communication, coordination, crime prevention, crime analysis, and agency administration. Use of ICT in law enforcement has reached the point of ubiquity and is considered to be fundamental to policing activity (Hoey, 1998). Further, the belief in the utility of ICT in policing is of such durability that individuals will continue to support the adoption and use of ICT even when the promised gains of doing so are unrealized and new burdens are created (M. M. Brown, 2001; Brown & Brudney, 2003; Hoey, 1998; Sawyer, Tapia, Pesheck, & Davenport, 2004). Consistent with this institutional mentality, law enforcement agencies and policymakers continue to look for opportunities to exploit ICT to improve operations, satisfy the demands of external constituents, and meet new statutory reporting requirements (Chan, 2001).

The variety in ICT adopted by law enforcement technologies has resulted in an equal variety of uses. An officer patrolling the beat may have a dispatcher run a license plate number through the RMS to check the status of a vehicle (e.g., stolen, outstanding traffic warrants, registration status, etc.) and have that information sent to a mobile data terminal (MDT) located in the officer’s car. At the same time, a detective may run a query of the RMS to identify if the vehicle is linked to other crimes; while later a crime analyst may mine the data in the RMS to identify patterns of criminal activity (Northrop, Kraemer, & King, 1995).
In the era of the World Wide Web, police ICT may even end up being used by individuals or organizations outside of the organization. For example, recently a local news station in the San Diego area made use of publicly available data from the Automated Regional Justice Information System (ARJIS) to study auto thefts and auto break-ins at local parking locations⁴.

The increased reliance on ICT by law enforcement raises a number of issues institutionally, organizationally, and technologically. For example, increased collection of electronic data by law enforcement agencies has been questioned in relation to Fourth Amendment protections, privacy regulations, and standards of evidence (Nunn, 2003). Organizationally, challenges such as data ownership and protection, the costs of system administration and support, and user training have come with the widespread adoption and use of ICT in law enforcement (Nunn, 2001).

Perhaps the most pressing issue resulting from the incorporation of ICT into policing is both a technological and organizational issue: the segregation of ICT both within and across agency boundaries. Historically, system design and administration has, to a large extent, been done in an ad hoc and isolated manner (Dunworth, 2005; National Association of State Chief Information Officers (NASCIO), 2003). This piecemeal approach to the design and development of information systems and applications within in law enforcement has resulted in agencies being burdened with inflexible-but-entrenched systems that are generally incompatible with other law enforcement systems operating outside of agency boundaries, and occasionally incompatible with other intra-organizational information systems. Incompatibility of ICT in law enforcement not only impacts tactical operations by hampering the sharing of mission-critical information; but

---

⁴ See http://www.10news.com/investigations/11077306/detail.html
it also hampers information sharing initiatives such as the development of the National Crime Information Center (NCIC) (Dunworth, 2005).

It is the complexity of the organizational and technological challenges associated with the adoption of ICT that are of particular relevance to this research. In particular, this research is focused on how law enforcement agencies attempt to integrate their internal systems with the systems of other agencies and the role of organizational identity in those integration efforts. Prior to addressing the integration question however, it is important to establish the historical foundation from which the current integration efforts arise.

**The Institutional Complexity of U.S. Law Enforcement**

Another factor contributing to the lack of ICT integration among law enforcement agencies is the institutional model of policing in the United States. Law enforcement in the United States is organized on the federalist model – with authority decentralized and distributed to the local level. The federalist model of policing is rooted in the U.S. Constitution which assigns policing authority to the states and local authorities in the Tenth Amendment (Richman, 2000). Though in recent years legislation has expanded federal policing authority and responsibility, policing remains largely a state and local operation. (Richman, 2000)

At the federal level of government, law enforcement agencies include the FBI, the U.S. Customs and Border Protection, the U.S. Attorney’s Office, the U.S. Marshals, the U.S. Secret Service, and the various military police agencies. The jurisdictions of these agencies are interstate and international and their focus is on the prevention and prosecution of federal and federal-level (interstate/international) crimes and the enforcement of civil rights (Richman, 2000).
At the state level of government there is a state police force and occasionally a state marshal service (e.g., the Texas Rangers). The predominant role of state police is traffic law enforcement on state highways; however state police also enforce state laws; for example the Pennsylvania State Police are also involved in enforcing customs and prosecuting organized crime (Rendell & Miller, 2003).

At the local level there can be county, city, township, and even institutional (e.g., university) law enforcement agencies operating within a limited geographical area. These agencies are engaged in the enforcement of local laws (including traffic), as well as the prevention, response to, and solving of local crimes.

The basis for the federalist model is twofold. One, the federalist model reflects the framers’ desire to retain power within the states and have a weak federal government. More practically, the informational resources required to prevent and solve local crimes reside in the greatest amount at the local level (Richman, 2000). This approach intuitively makes sense. The local officer or agency is more likely to have much more knowledge of local individuals, locations, activities than an individual or agency at the federal level with an inherently broader perspective.

There are over 17,000 state and local law enforcement agencies in the United States (Bureau of Justice Statistics, 2000a). The number of agencies per state varies greatly. For example, Texas has the most agencies with 1,775, while Hawaii has the least with 5. There is a strong correlation between state population and number of agencies operating within the state (.655); however the agency/population ratio is often contrary to expectation. For example, the most populous state, California with a population of 34,008,499 people has only 516 state and
local police agencies in operation; while Wisconsin, the eighteenth most populous state with 5,374,747 people (3/20 the population) has 10 more agencies than California (526) operating within its borders. Though these agencies often work in close jurisdictional proximity, each of these agencies has its own chain of command, funding mechanisms, organizational structures, policies, identities, and technological infrastructure.

For example, the town of State College, Pennsylvania where The Pennsylvania State University is located, is a medium-sized town with a population of approximately 80,000 residents when including the student population (The Pennsylvania State University, 2005; U.S. Census Bureau, 2003). Agencies that have jurisdiction in the State College area include two township police departments, the Borough of State College police department, The Pennsylvania State University police department, the Pennsylvania State Police, the Pennsylvania Domestic Relations Service, Corrections, and Game Wardens, and the Centre County Sheriff’s Department (Centre County Government Office of Communications, 2005). In total 19 separate criminal justice agencies are active in a relatively small geographic area, each with its own jurisdiction, management structure, funding mechanisms, organizational goals, and ICT infrastructures. Though these organizations share many common goals, practices, and capabilities they are in fact independent organizations with their own (albeit similar) cultures, management structures and practices, and information technology infrastructures. Designing any ICT to be compatible with this many disparate agencies is a remarkably complex task; one that grows more complex when attempting to incorporate federal level agencies.

5 According to the Centre Area Transportation Authority which serves the State College area (http://www.catabus.com/acgeninfo.htm) the geographical area is approximately 133 square miles. As a comparison, San Diego County in California has a geographical area of 4,199 square miles (http://quickfacts.census.gov/qfd/states/06/06073.html).
The complexity of the institutional environment within which law enforcement organizations operate, and the complexity of ICT infrastructures that have developed in that environment, has contributed to a critical need to integrate ICT across organizational boundaries in order to facilitate the quick flow of information among agencies. Policymakers at the national, state, and local level have and continue to dedicate significant resources to achieving the goal of integration.

**The Need for Integration**

The goal of integrating the information and communication technologies of criminal justice organizations in general, and law enforcement specifically is not a new phenomenon. The Uniform Crime Reporting (UCR) system in which local agencies submitted aggregated crime data to the federal government dates back to the 1920’s (Dunworth, 2005, p. 5). In 1985 the criminal justice community began the process of implementing the National Incident-Based Reporting System (NIBRS) to replace the UCR, a system where agencies submitted individual incident data to state and local systems (Dunworth, 2005, pp. 10-11). The National Crime Information Center (NCIC), founded in 1967 and updated in 1999 (Federal Bureau of Investigation, 2007b), and the National Instant Criminal Background Check System (NICBCS – established by the Brady Act in 1993) are more recent examples of systems designed to integrate information across agency boundaries (Federal Bureau of Investigation, 2007a).

However, systems such as the NCIC and the NICBCS represent integrated systems that are distinctly different than current integration initiatives. These systems act as integrators by serving as data aggregators, so while information is being shared across agency boundaries, it is done in a primarily push (an agency submits its incident data to a federal database) / pull (an agency queries the federal database about an incident or suspect) manner. In the aftermath of the
terrorist attacks on September 11\textsuperscript{th}, 2001 the concept of integrated criminal justice information systems shifted to one of not only shared information, but shared communication and inter-agency collaboration.

**Government action after 9/11 and Hurricane Katrina**

One outcome of the attacks on September 11, 2001 – and later Hurricane Katrina – has been an increased emphasis at all levels of government to improve inter-organizational information sharing and collaboration. This emphasis is a result of post hoc analysis that identified lack of information sharing and collaboration among government agencies as a key contributor to the government’s failure to identify and prevent the attacks before they happened (Shelby, 2002). Cross-agency collaboration among federal agencies was not the only issue to be found in post-event analyses. Also cited as a key issue was first responders’ inability to coordinate their efforts in responding to international terrorism (National Commission on Terrorist Attacks upon the United States, 2004, pp. 396-398). The government took a number of actions in response to these analyses.

One action was to restructure government agencies to facilitate coordination collaboration resulting in the creation of a new bureaucracy – the Department of Homeland Security – and a new cabinet-level officer – the National Intelligence Director. Another action was to focus on the creation of the technological infrastructure necessary for first responders to be able to communicate and collaborate more effectively. Project SAFECOM which focuses on the creation of a national communications network for first responders, and the Global Justice XML Data model that standardizes criminal justice information and metadata are examples of this form of government action (Department of Homeland Security, 2006; Department of Justice Office of Justice Programs, 2006). A third action was to increase the resources dedicated to
terrorism-response preparation and counterterrorism activities by law enforcement (Maguire & King, 2004). An element of the emphasis on law enforcement preparation for terrorism was to fund initiatives to foster the development of new, and expansion of existing, technological an organizational systems premised on collaboration and information sharing – integrated criminal justice information systems. It is the development of IJIS that is the focus of this research.

To summarize, the need to integrate ICT across law enforcement boundaries has been identified as a political, technological, and organizational priority. Technology is a key component of law enforcement operations. However, as a result of the ways in which law enforcement in the United States has been institutionally structured historically – a federalist model where authority was distributed primarily at the state and local level – ICT have been developed ad hoc and in isolation. This system development practice has resulted in a situation where individual agency information systems are often technologically incompatible and agencies are often impeded their ability to collaborate through the sharing of operationally critical information. In the aftermath of terrorist attacks and catastrophic natural disasters in the United States, policymakers have emphasized the need to integrate information systems across organizational boundaries. These systems – integrated criminal justice information systems – are being developed to address that need.

**Integrated Criminal Justice Information Systems**

Integrated criminal justice information systems are systems that encompass technological infrastructures; governance policies, work practices and procedures, and often new organizational structures intended to facilitate effective communication and the sharing of information both within and across organizational and jurisdictional boundaries. This
complexity differentiates the IJIS from the single computer application, database or device\(^6\).

Examples of existing IJIS include Pennsylvania’s Justice Network (JNET) system, the Washington D.C. metro area Capital Wireless Integrated Network (CAPWIN) system, and the San Diego County Automated Regional Justice Information Sharing System (ARJIS).

Integrated criminal justice information system initiatives pursue integration at varying levels. Some systems integrate comprehensively at multiple levels of government and across many agencies; others integrate selectively, choosing to integrate a single system across multiple levels of government; and others integrate incrementally, integrating specific agencies, levels of government and systems, but often expanding with time (Gil-Garcia et al., 2004). An IJIS can include multiple agencies and span jurisdictions horizontally (across the same level of government) or vertically (across varying levels of government) (National Association of State Chief Information Officers (NASCIO), 2003).

The integration process is a long-term process and it is embedded in the broader evolution of agency business practices (National Association of State Chief Information Officers (NASCIO), 2003). Further, integrated criminal justice information systems are multi-agency and multi-jurisdictional. The long-term nature of the integration process and its linkage to the evolution of business practices is a key characteristic of IJIS initiatives that distinguishes such initiatives from the “simple” task of purchasing and implementing a software or hardware application, such as a computer-aided-dispatch system, in a “one-off” manner.

---

\(^6\) An example of a single application that often gets conflated with the integrated criminal justice information system is COPLINK. While the COPLINK application does facilitate information sharing (and potentially collaboration), the level of integration across agency boundaries is minimal. Similarly, two agencies partnering on a cellular phone contract does not represent an integration of systems.
<table>
<thead>
<tr>
<th>Property</th>
<th>Characteristic</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-organizational</td>
<td>IJIS integrates systems of at least two separate agencies</td>
<td>The ARJIS system integrates the data stored in the records management system of all member agencies</td>
</tr>
<tr>
<td>Multi-jurisdictional</td>
<td>IJIS spans multiple jurisdictions, either horizontally (at same level of government) or vertically (up and down levels of government)</td>
<td>Pennsylvania’s JNET system is vertically integrated at local, county, and state level</td>
</tr>
<tr>
<td>Governing</td>
<td>IJIS initiative develops governance structures that may be comprised of, but exists outside of participating agencies</td>
<td>The ARJIS organizational structure is comprised of committees filled by member representatives, a management team that works for the county government organization, and reports to a county-level political body.</td>
</tr>
<tr>
<td>Centered around law enforcement activity</td>
<td>Primary focus of IJIS is to facilitate law enforcement operations</td>
<td>Primary clients of ARJIS, JNET, and CapWIN are law enforcement agencies</td>
</tr>
</tbody>
</table>

Table 2-1 Properties of IJIS

Integrated criminal justice information systems are also more than just infrastructure or standards setting collaborations. Initiatives such as the aforementioned federal government’s Project SAFECOM which seeks to create a universal communicates infrastructure for first responders, and the Global Justice XML Data Model which seeks to develop standard data formats for information sharing are not integrated criminal justice information systems\(^7\). Rather they are infrastructure development projects that may be incorporated into an IJIS. Integrated

\(^7\) For more information on Project SAFECOM see (Department of Homeland Security, 2006); for more information on the Global Justice XML data model see (Department of Justice Office of Justice Programs, 2006).
criminal justice information systems often include infrastructural components, particularly in terms of back-office hardware, but just as an application in isolation does not comprise an IJIS, neither does infrastructure (e.g., a shared radio frequency) in isolation.

Law enforcement agencies have been told to expect many benefits from participating in the creation and deployment of IJIS. These benefits include improved data quality, gains in efficiency (in terms of time and money savings), timely access to information, improved safety, and greater information sharing (Dunworth, 2005; Gil-Garcia et al., 2004). Some have even posited second-order benefits from such systems such as increased deterrence of criminal activity as a result of the perception among criminals that law enforcement is more aware of who commits crimes (Agrawal, Rao, & Sanders, 2003). Consistent with the overall use of technology in law enforcement, evidence of the realization of these benefits remains scarce and inconclusive (Maguire & King, 2004).

**The Need for Further Empirical Evaluation**

The evidence of the efficacy of police use of technology in general, and integrated criminal justice information systems is inconclusive (Chan, 2001) or unavailable. Empirical analyses to date makes clear that many of the benefits of information criminal justice information systems remain unrealized (General Accounting Office, 2004; Government Accountability Office, 2005). For example, the National Conference of State Legislatures (NCSL) – a major advocate for the deployment of IJIS, states explicitly that participating agencies should not expect to realize a financial savings as a result of their participation (Morton, 2004). Similarly, Nunn (2001) found that efficiency gains in the field were often offset by the cost of dedicating increased resources to supporting the system.
Efficiency in one area of law enforcement has in some cases been offset by the decrease in efficiency in others. For example, the Charlotte-Mecklenburg Police Department (CMPD) found that as a result of the implementation of their KBCOPS system, officers were now spending on average 30 minutes to two hours keying paper-based incident reports into a web-form for submission to the system (S. R. Williams & Aasheim, 2005). CMPD effectively transferred the burden of data entry from record-management staffers to field officers. As a result, instead of achieving the goal of improved data collection, CMPD found that officers would skip fields that lead to increased data entry.

In their study of a prototype wireless system as part of Pennsylvania’s JNET system, Sawyer and his colleagues (Sawyer et al., 2004) report similar findings. They found that connectivity drops, dual-layer authentication, and battery drain all added significantly to the cost borne by the officer trying to use the system. These issues were exacerbated by the limited IT support available within the agencies studied. Additionally, the authors report that the implementation of wireless access did not alter existing organizational structures, so officers using the technology still relied on existing communications structures (dispatch).

In another study of mobile computing in policing, Ioimo and Aronson (2004) found that there was no significant evidence that providing access to ICT in the field improves officer productivity. Further, like the KBCOPS study, while the introduction of new mobile technologies may not have benefited the intended recipients (patrol cops in the field), they do provide benefits for unintended recipients (administrators and detectives). And like the study of the JNET system, in spite of the lack of actual results of improvement in job productivity, patrol officers continued to express their recognition for the benefits of technology and support the use of technology in policing.
Empirical analysis of IJIS has begun to make its appearance in the literature in the past few years. For example, one study looked at the role of institutional and rational choice factors in the formation of public safety networks (C. B. Williams et al., 2009). Another study by the same group of authors proposed an empirically-based taxonomy of public safety information sharing systems (Sawyer, Fedorowicz, Tyworth, Markus, & Williams, 2007). A third study found that data, organizational, and environmental characteristics played a key role in information-sharing initiatives (Akbulut, 2003), and DuBois and colleagues (2007) reported on the evolution of Chicago’s CLEAR system.

The issues that helped spur the movement to integrate ICT in law enforcement agencies have also plagued the development efforts. The National Association of Chief Information Officers (NASCIO) found that aging and often incompatible infrastructures; a limited and fragmented communications spectrum; and stovepipe development practices hamper development efforts (National Association of State Chief Information Officers (NASCIO), 2003). Similarly, the General Accountability Office (General Accountability Office, 2004) in a report on the Department of Homeland Security’s (DHS) Project SAFECOM, found the goal of enhanced interagency communication to be hampered by limited standards, lack of funding, and a lack of interagency collaboration. Battles over organizational turf continue to be an major obstacle resulting in a “lack of resource pooling, lack of information sharing, poor procedure development, and a lack of adaptation (Clayton & Haverty, 2005; Gil-Garcia et al., 2004)”.

Implementing the needed institutional reforms has often been relegated a low priority or resisted altogether (Clayton & Haverty, 2005). There has been such difficulty in integrating systems among first responders that the issue came to the forefront of the political discourse after
Hurricane Katrina (Manoj & Baker, 2007), and was used as a campaign issue in the 2006 congressional elections; a full five years after the September 11th attacks (Hsu, 2006).

In spite of the documented difficulties and ambiguous results, agencies continue to press on with their IJIS initiatives, and new initiatives continue to proliferate both in the United States and globally (Northrop et al., 1995). Each of these initiatives has its own design methodology, governance structures, and system components (Morton, 2004). The goal is to integrate disparate information systems: but, the level of integration has been in many ways limited to the scope of the project. Simply reducing the degree of balkanization of IJIS would represent an incomplete result.

Conclusion

In this chapter I established the practical motivation for engaging this research. Historically the law enforcement community in the United States has embraced the use of technology to enhance operational capability. This trend continues through the present day. Yet the institutional complexity of law enforcement, with organizational control widely dispersed to the local level has resulted in a pattern of developing and implementing technologies in an ad hoc and isolated manner. This pattern has led to significant disintegration of systems among the law enforcement community as a whole.

As a result of catastrophic events such as the September 11 attack and Hurricane Katrina, policymakers have emphasized the need to develop or upgrade law enforcement systems so that they are integrated across organizational boundaries and agencies can more effectively share mission critical information and collaborate. Currently there are many integrated criminal justice information system initiatives occurring across the United States, each with their own
technological architectures, organizational practices, and goals. To date, there is scarce and inconsistent empirical evaluation of the results of these efforts.
Chapter 3 The Social Informatics Perspective

Introduction

In this chapter I discuss the ontology that guides this dissertation. This task is important because theory and method choice derive from ontology – one’s theory about the nature of being\(^8\). How one perceives the nature of the world (both physical and social) defines the legitimate research problems, theories, and methods (Kuhn, 1996a, p. 10). This chapter, then, presents a brief but thorough discussion social informatics and how its ontological frame guides this research.

Social informatics is an approach to the study of ICT that attempts to account for both the agency of the material artifact (e.g., the actual ICT device, program, etc.) and the enabling and limiting influences of the broader social context within which the device is engaged. What this means is that the ontology undergirding social informatics research is one in which ICT are mutually constituted by the artifact and the social context within the artifact is embedded to the point where artifact and context are not meaningfully separable (Kling, McKim, & King, 2003). This premise of inseparability clearly has important epistemological and theoretical ramifications that are addressed later in this chapter.

I subscribe to the social informatics perspective over alternative views of technology such as the cognitivist view common to human-computer interaction literature or the social constructionist view found in much of the sociology of technology literature for two reasons. One, the social informatics perspective most closely aligns with my personal experience in the design and use of ICT in the work place. Two, the social informatics approach provides insight where other perspectives that tend to favor or ignore either the technical or the social provide

\(^8\) See http://www.merriam-webster.com/dictionary/ontology
incomplete understandings of the complex ways in which ICT intersect with social activity (Orlikowski & Baroudi, 1991; Orlikowski & Iacono, 2001).

In the remainder of this chapter I discuss social informatics research in detail, including its origins, principles, and challenges; and how a social informatics perspective conceptualizes the relationships between information, technology, and people. I then address the epistemological and theoretical considerations of social informatics research. I conclude this chapter by situting this dissertation as social informatics research.

**What is Social Informatics?**

Social informatics is more formally defined as the interdisciplinary study of the design, uses, and consequences of ICTs that takes into account their interaction with institutional and cultural contexts (Kling, Rosenbaum, & Sawyer, 2005, p. 6).” Less formally, social informatics can be accurately described as the social analysis of computing. The key feature of this definition, and what distinguishes social informatics research from other scholarly approaches, is the anthropocentric focus and emphasis on design, use, and consequences *in context*. Whereas a situated action theorist focuses on the emergent behaviors that arise from attempting to perform a particular task (Nardi, 1992), and a social construction of technology theorist examines the historical social choice-points that resulted in a particular technology (Bijker, 1995), the social informatics researcher focuses on the technology, its associated uses, and the broader current and historical context within which the technology is engaged by social actors. There are three characteristics of social informatics research that are indicated by the formal definition presented here.

First, social informatics research is inter- or trans-disciplinary. This means that social informatics in itself is not a scholarly discipline, but instead an approach that can be – and has
been – adopted by members of many different disciplines. For example, social informatics-like research has come from the disciplines of Information Systems (c.f., Markus & Robey, 1988; Orlikowski, 1992), from Science, Technology, & Society Studies (MacKenzie & Wajcman, 1999), and from Management Science (Barley, 1986; Barley & Kunda, 2001). Diversity of “membership” is both a source of strength and weakness for social informatics. Strength comes from the fact that an interdisciplinary approach to the studying of technology creates a fertile ground for multiple theoretical and methodological approaches to take hold. Weakness comes from the fact that such diversity can also be interpreted as a lack of paradigmatic coherence. The challenges facing social informatics as a scholarly movement are largely external to this dissertation; however it is important to note that the interdisciplinary nature of a social informatics has direct bearing on a key underlying principle of social informatics research to be discussed further on in this chapter.

Second, social informatics is fundamentally about the study of ICT. This emphasis on ICT distinguishes social informatics research from other forms of the social analysis of technology such as Social Construction of Technology theory and Science, Technology, and Society Studies in that both often engage in analyses of other types of technologies (such as nuclear power). Further, by making the ICT artifact the locus of interest, social informatics research privileges an ensemble perspective where artifact and context are mutually constitutive, while SCOT and STS often adopt a nominal perspective where technology is often simply a means to study some other phenomenon (such pay discrepancies among gender, the politics of globalization, etc.). As with the interdisciplinary character of social informatics, the focus on ICT informs a key principle –

---

9 I qualify the examples as ‘like social informatics research’ because the scholars who produced it reside in specific scholarly disciplines and likely consider the examples listed here as examples of research in those particular disciplines. That said, independent of how the authors would categorize their own work, as a practitioner of social informatics research I identify the cited articles as work representative of the social informatics ontology and the type of work I aspire to emulate.
the principle that social informatics is theoretically and methodologically independent – of social informatics research discussed later in the chapter.

Third, social informatics research seeks to account for the institutional and cultural context within which information and communication technologies are designed and used. Just as a focus on ICT distinguished social informatics from nominal approaches to the study of technology, the accounting of institutional and cultural context distinguishes social informatics from cognitivist or algorithmic approaches to the study of ICT such as Human-Computer Interaction (HCI) and Information Retrieval (IR). Whereas HCI research often tends to focus on individual computing activity in an experimental setting, and much of IR research tends to focus on the development of computational models and algorithms for retrieval of information and information management; social informatics research seeks to study ICT as they are engaged in a ‘real world’ context. Further, in social informatics research human actors are considered to be social actors with a variety of motivations, interests, and reactions to interactions with ICT; whereas in HCI and IR research the human component is often an abstracted, generalized entity useful for the purposes of developing formal laws.

The point here is not that the cognitivist / individualist approach that is common to HCI and IR is inferior to social informatics; rather that social informatics offers alternative insights to these fields when studying similar phenomena. So while HCI provides knowledge of human physical and cognitive limits as they apply to the design of ICT; social informatics research provides insights into the ways in which ICT impact and is impacted by real-world context.

**Information, Technology, & People**

Underlying the previous discussion, particularly the discussion of the differences between social informatics and other approaches to the study of ICT, is the way in which different
approaches to the study of ICT conceptualize the relationship between information, technology, and people. How this relationship is understood greatly informs the theoretical and methodological choices of the scholar, and therefore it is important to discuss in greater detail as part of a broader discussion of the ontological basis for this research.

A useful method for conceptualizing the relationship between information (I), technology (T), and people (P) is to render the relationship as a triangle with each corner of the triangle representing one of the concepts. Mapping the conceptual space in this manner allows us to visually locate different theoretical frames and research paradigms in terms of how they address all three phenomena.

Figure 3-1 Conceptualizing the domain.

Human-Computer Interaction (HCI) by definition focuses on human computing behavior in a manner that is oriented towards the level of individual cognition and the design of
technological artifacts to facilitate human physical, cognitive processes, and work activities (Carroll, 2003). Context, therefore, is limited to encoded information that can be applied to later use, or to design that allows for reaction to dynamic patterns of use (Dourish, 2007). Similarly, sub-genres of human-computer interaction that explicitly mention context, for example the area of distributed cognition, employ a very constrained conceptualization of context that is generally limited to a particular work task or goal, excluding from examination of larger contextual issues such as institutional and structural influences (Perry, 2003). Indeed, Dourish (2007) suggests that HCI research move away from a positivist-oriented definition of context in which context is information, stable, and separable, towards a phenomenological view in which context is considered to be relative, defined dynamically, spontaneous and associated with activity. A conceptualization of context in this manner would be consistent with the social informatics view of ICT.

In contrast to HCI with its generally socially-lean view of computing activity, many researchers engaged in the field Sociology of Technology employ theories such the Social Construction of Technology that privilege the social over the technological. Here, instead of a generic, generalizable “user,” it is the technology that is generic, abstract, a “black box (Winner, 1993).” The actual technological artifact is either only nominally accounted for, or absent altogether (Orlikowski & Iacono, 2001). Examples of this type of research include examining the impact of “The Internet,” conceptualized as a singular technology, on democracy (Kluver & Banerjee, 2005), health information seeking behavior (Burkell, 2004; Weisgerber, 2004), and as a public good (Stewart, Gil-Elguí, & Pileggi, 2004).
Social informatics research offers alternative insights to these two approaches in that the social informatics scholar attempts to account for both the material properties of the artifact and the broader social context in which the artifact resides while at the same time privileging neither. Computer users are social actors: socially complex, not primarily users of computers, and engaging computers in often unintended and unanticipated ways. At the same time, the material properties of the artifact—such as application feature sets and hardware performance capabilities—have a tangible impact on the ways in which humans can interact with the ICT; an impact that at one both enables and constrains human behavior (Leonardi & Barley, 2008; Tyworth & Sawyer, 2008). Guided by this view of the relationship among information, technology, and people, three social informatics principles have emerged from the growing body of social informatics literature.
Social Informatics Principles

Drawing on the three previously discussed elements of the social informatics approach – multi-disciplinarity, a focus on ICT, and an emphasis on both the artifact and social context – Sawyer (2005) identifies three main principles of social informatics research. One, social informatics research is motivated by problems not theory. Two, social informatics research is methodologically independent, though particular types of methods lend themselves more to social informatics research. Three, social informatics research challenges commonly-held assumptions about ICT.

What does it mean to say that social informatics research is driven by problems rather than theory? The social informatics scholar is interested in particular ICT problems to study rather than adherence to a particular theoretical orthodoxy. It is the phenomenon that is of interest to the social informatics scholar, and in this sense social informatics research tends to be idiographic. Theory choice is important, but not limiting: a social informatics scholar chooses from a range of theories to inform the research. Demonstrative examples of this principle include the application of neo-institutional theory to the study of ICT use in the real estate industry (Sawyer, Wigand, & Crowston, 2005) and agency theory to study the enabling role of IT in managed health care (Wickramasinghe & Lamb, 2002).

Given that social informatics research is theory-independent, it intuitively makes sense that social informatics is also method-independent for method choice often is a function of theory choice. Methodological independence is the second principle of social informatics. Social informatics research is neither driven nor constrained by adherence to any particular analytical method. However, given the emphasis on ICT in context, social informatics research tends to have a qualitative methodological orientation. The case study is a common
methodological technique employed in social informatics research, however other methods including content analysis and ethnography have been employed (Sawyer & Eschenfelder, 2002). This methodological flexibility distinguishes social informatics from other more methodologically-linked forms of research such as social network analysis (c.f., Granovetter, 1973; Wellman, 2001).

A critical orientation towards ICT is the third principle of social informatics. This means taking a critical perspective on a particular problem and challenging the commonly-held assumptions (George & King, 1991; Kling, 1999). This does not mean taking a critical theory orientation in which the focus is on class, power, and radical change (Farganis, 1975; Steffy & Grimes, 1986). Rather, a critical perspective or orientation in social informatics research means that the scholar eschews a tool view of ICT in which ICT is viewed as a static, neutral entity to which direct effects can be linearly traced in favor of the ensemble view in which ICT is complex, non-neutral and often results in unanticipated outcomes (Agre, 1999; Sawyer & Eschenfelder, 2002; Sawyer & Rosenbaum, 2000; Sawyer & Tapia, 2005).

<table>
<thead>
<tr>
<th>Social Informatics Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social informatics research is trans-disciplinary, drawing on research and insights from multiple academic and professional disciplines</td>
</tr>
<tr>
<td>Social informatics is problem- rather than theory-directed</td>
</tr>
<tr>
<td>Social informatics methodologically independent, though qualitative methods tend to be privileged</td>
</tr>
<tr>
<td><strong>Normative</strong> – social informatics research contributes to practice and future research through empirical insight</td>
</tr>
<tr>
<td><strong>Analytical</strong> – social informatics research generates new, or extends existing theory of ICT</td>
</tr>
<tr>
<td><strong>Critical</strong> – social informatics research challenges commonly held assumptions about the nature and impacts of ICT</td>
</tr>
</tbody>
</table>

Table 3-1 Principles of Social Informatics
Social informatics research, in addition to a critical orientation, often takes a normative or analytical form (Lamb & Sawyer, 2005). Normative social informatics research is oriented towards providing alternative recommendations or insights to practice and research through empirical analysis. Analytical social informatics research emphasizes generating new or extending existing theory of ICT. Kling et al.’s (2003) STIN-model and Lamb and Kling’s (Lamb & Kling, 2003) are examples of analytical social informatics research.

The research presented in this dissertation is both analytical and normative social informatics research. This research is normative in that it provides empirically generated insights that can be used to inform ongoing and future ICJS development initiatives; the analytical component of this research comes from the novel incorporation of boundary objects, social actors, and organizational identity theory to the study of ICT.

Challenges
As with all paradigms, approaches, frameworks, etc., there are challenges to doing social informatics research. Three challenges in particular stand out. One challenge is the premise that context and artifact is not meaningfully separable. For if artifact and context cannot be separated, what exactly is empirically observed when studying ICT? Is it even possible to study an amalgam of context and device?

This challenge misses the essence of Kling et al.’s assertion that artifact and context inseparable. Kling and his co-author are not arguing that the materiality of an artifact and the social context of its design, use and consequences are literally inseparable. This in fact, goes counter to the very basis of the social informatics approach in that ICT are context-dependent. The same artifact, for example the cellular phone, has different properties in different contexts. Rather, the argument Kling and his co-authors are making is that the artifact and context are not
meaningfully inseparable in the sense that one cannot truly understand the artifact without looking at the broader context within which it is designed and used, and one cannot truly understand the context of how an artifact is designed and used, without looking at the ways in which the properties of the artifact enable and constrain use. The purpose of such a claim is to challenge the technologically and socially determinist discourses on technology by emphasizing the need to capture both the social and the technical.

The second challenge for social informatics is the degree to which the materiality of the ICT artifact can be accounted for without falling into the trap of technological determinism. Or, in other words, to what extent can we assign agency (the ability to independently act) to the ICT artifact before that agency becomes determinant social outcomes? This challenge has been at the core of the debate over the validity of social informatics as a socio-technical approach (Grint & Woolgar, 1992; Kling, 1992).

The challenge of how much agency to assign the artifact can be represented along two orthogonal axes (Tyworth & Sawyer, 2008). On one axis is the tension between social structures (norms, values, regulations) and individual free will. On the other axis is the tension between the social actor (human, group, organization) and the ICT artifact. The salient issue is one of where causality lies (in physical objects or social constructions) and where agency lies (within humans or within social structures) (Leonardi & Barley, 2008). As Leonardi & Barley eloquently state, materiality and agency are often conflated and treated as synonymous when they should be treated as orthogonal.

To say that materiality matters is not to say that materiality determines in a predictable way our actions as humans. Rather it is to say that materiality serves to shape and constrain our
actions. We may choose to call a wooden door a window, but the view when looking through it remains lousy. However, that a rectangular piece of wood is used as a door in one context does not prevent us from using it as a ramp, or a raft, or a roof in another. Similarly, we have the free will to use ICT in ways not anticipated or intended by their designers but the range of uses we have to choose from is ultimately limited by the physical capabilities of the artifact and the prior choices of the designers. While we can use Microsoft Word to manage our digital photos, we cannot use it to analyze digital space photography.

The third significant challenge facing social informatics research is method and theory choice. As discussed earlier in the chapter, social informatics research is problem-driven rather than theory- or method-driven\(^\text{10}\) which exposes social informatics to the criticism of lacking theoretical or methodological coherence. While there is no single theory or method that drives social informatics research, there is coherence in the sense that in following the principles outlined above, the set of theories and methods available to social informatics research is restricted. These restrictions and their implications I discuss in the next section. The key point in this discussion is that because the choices of theory and method are limited when doing social informatics research, certain theories and method appear more frequently.

**Epistemological & Theoretical Implications**

Social informatics research focuses on studying ICT within institutional and cultural contexts and attempts to capture both the material properties of the artifact and the surrounding

---

\(^{10}\) By ‘theory- or method-driven’ approaches to the study of ICT, I mean fields or disciplines in which one primary theory or method serves as that which binds those who ascribe themselves as members of the community. An example of the former is those who employ Actor Network Theory (ANT). An example of the later is those who engage Social Network Analysis (SNA). While, there are ‘flavors’ of both, in general there are certain fundamentals that are common to majority and research in both domains exhibits certain commonalities (for example, tie-strength in SNA).
social context. This predisposes social informatics to certain theories and methods, while excluding others.

Theory-wise, social informatics research lends itself to those theories that address a level of analysis higher than the individual. The reason is simple: by definition ‘social context’ implies more than a single individual. Examples of theories that are appropriate to social informatics research include institutional theory (c.f., Avgerou, 2002), structuration theory (Orlikowski, 1992), and socio-technical theory (Friedel, 2007). Social-shaping of technology theory is also useful if there is adequate emphasis on the technological artifact. Alternatively, theories that exclude or ignore social context are clearly inappropriate for conducting social informatics research.

Certain methods of data collection and analysis are particularly useful for conducting social informatics research. Overwhelmingly, these methods are qualitative methods of data collection and analysis – e.g., case studies, field research, and ethnographies – because qualitative methods are expressly intended to capture contextual detail. Case studies, field studies, and ethnographies are not the only methods employed in social informatics research however. Action research has also been a method that has utility for social informatics researchers (c.f., Wood-Harper & Wood, 2005). Alternatively, methods designed to remove contextual variance, primarily the experimental method, are not useful to the social informaticist as they remove the very contextual detail the social informaticist is trying to unpack.

Methods such as case studies and ethnographies are well-suited for social informatics research for another reason: they provide for specific, empirically-based findings. Given that ICT are a product of artifact and specific context, generalized laws are not the purpose of social
informatics research; rather just the opposite: the purpose of social informatics research is often to point out that generalized claims about ICT do not stand up to empirical analysis.

This dissertation as social informatics research
In conducting the research for this dissertation, I sought to conduct a social informatics analysis. This dissertation was conducted in a manner consistent with the principles of social informatics research – it is problem driven, methodologically independent, and critically oriented. I have chosen to focus my research on a considerable problem facing professional practice: the design and use of integrated criminal justice information systems. I have, as will be discussed in Chapter 4, designed my study to employ multiple complimentary data collection and analysis methods that capture context and artifact properties. Inasmuch that there is a common wisdom about integrated criminal justice information systems, I adopt a perspective that challenges those claims that are made by demanding empirical evidence.

Consistent with prior social informatics research, the theories I employed to guide this research – organizational identity and boundary objects – are theories of social interaction. Both predispose that human actors are socially complex, motivated and influenced by multiple factors. My application of these theoretical lenses shed insight into IJIS design in two ways. One, using organizational identity, I identify one way in which the social attributes of an organization are manifested in the organization’s technology. Two, using boundary objects theory, I show how IJIS facilitate social interactions. Follow-up research will look at the ways in which identity characteristics embedded in ICT shape future ICT development.

Conclusion
In this chapter I discussed in detail the ontology that serves as the foundation for this research. This discussion has included a definition of social informatics research; why I choose
to do social informatics research; the principles and challenges and challenges of social informatics research; a discussion of how I conceive the relationship between information, technology, and people; and finally a brief discussion of how this research fits the social informatics model. Having established the ontological view of this research, I will now detail the domain of law enforcement of technology and the motivation to study integrated criminal justice information systems.
Chapter 4 Theoretical Framing

Introduction

In this chapter I review and synthesize the extant literature on organizational identity and boundary objects. The first half of the chapter covers organizational identity. I have chosen to study organizational identity and its influence on the design and use of organizational ICT for the following three reasons. One, both organizational identity and organizational technology are central to organizational life and therefore understanding the relationship between the two gives us important insight into organizational computing. A second related reason is that through the documentation and analysis of the relationship between an organization’s identity and its technologies, this research serves to contribute to the “unpacking” of the social context in which organizational computing is conducted. Three, this dissertation makes a much-needed empirical contribution to organizational identity research where prior work has been primarily theoretical in nature.

This chapter proceeds as follows. First, summarize how organizational identity has been defined in the literature, highlighting key issues in the ongoing debate over the nature of organizational identity. I then, briefly, discuss organizational identity’s conceptual relationship to organizational image and culture. I conclude the chapter proposing that organizational identity shapes the design and configuration of organizational ICT.

Organizational Identity

Organizational Identity Defined

What is meant by organizational identity? Fundamentally, organizational identity is the organization’s answer to the question “Who are we?”11 Organizational identity is a composite of the organization’s internal understanding of self, the organization’s distinct features and

11 ‘We,’ as used here, means the organizational collective.
attributes, and the organization’s actions. Organizational identity is tightly linked with both organizational culture (tacit understandings, values, norms) and organizational image (external perceptions of the organization); and organizational identity is understood to be a significant influence on organizational behavior and the behavior of organizational members (Hatch & Schultz, 1997, 2002). Beyond this basic understanding however, a review of the literature finds open debate over the precise nature of organizational identity and its impact as an organizational dynamic (Brunninge, 2005; Gioia, Schultz, & Corley, 2000; Ravasi & Schultz, 2006; Ravasi & van Rekom, 2003; Whetten, 2006).

Two main perspectives on organizational identity that have been identified are the social actor and social constructivist perspectives (Ravasi & Schultz, 2006). The former is grounded in Albert & Whetten’s (1985) seminal work on organizational identity which defines organizational identity as the claims (or shared beliefs) of what is central, enduring, and unique about an organization. The latter perspective treats organizational identity as negotiated, malleable and subject to external pressure (Corley & Gioia, 2004; Dutton & Dukerich, 1991; Hatch & Schultz, 2002). According to Ravasi & Schultz (2006) the difference between these two perspectives is one of ‘sensegiving’ versus ‘sensemaking.’

The social actor perspective treats organizational identity as a sensegiving mechanism; organizational identity helps organizational members to understand what differentiates the organization from others. The social constructivist perspective treats organizational identity as a sensemaking mechanism, organizational identity helps members to ascribe meaning to experience. However, recent work by Whetten (2006) indicates that these two perspectives may not be mutually exclusive.
Most scholars reference Albert & Whetten’s (1985) definition of organizational identity as that which is central, enduring, and unique (CED\textsuperscript{12}) about an organization (Corley, Harquail, Pratt, Glynn, & et al., 2006; Hogg & Terry, 2000). However, in responding to what he perceived as a lack of clarity in the organizational identity concept, Whetten (2006) argues that the lack of clarity in organizational identity theory is the result of an incomplete application of Albert’s and his original definition of organizational identity; that there are three components of an organization’s identity – the ideational, the definitional, and the phenomenological components; and that many scholars have treated the ideational (shared beliefs) component as the whole of the definition (See Table 4.1).

The ideational component of the organization’s identity is organizational member’s shared perception of who the organization is. The definitional component is comprised of the central, enduring, and unique features of the organization. The phenomenological component is comprised of the ways in which organizational identity is reflected in identity related discourse and action. In other words, an organization’s identity is simultaneously comprised of its self-understanding, its unique attributes, and the identity-related discourse by organizational members.

\textsuperscript{12} In the 2006 paper Whetten substitutes the word distinctive for unique. For the sake of brevity I treat these terms as synonymous and use Whetten’s own acronym of CED.
<table>
<thead>
<tr>
<th>Identity Component</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ideational</strong></td>
<td>The perception of who the organization is as collectively shared by its members.</td>
<td>The ideational component of organizational identity is reflected in statements of who the organization is. For example, “Google is an unconventional company,” is an ideational statement of organizational identity as is “Google does search.”</td>
</tr>
<tr>
<td><strong>Definitional</strong></td>
<td>Central, enduring, and unique characteristics of an organization.</td>
<td>The definitional component of organizational identity is the attributes that specify how the organization is similar to, and different from, other organizations. The attributes can be particular competencies, traits, or practices. For example, Google’s practice of providing on-site health and dental care to its employees is unique organizational attribute.</td>
</tr>
<tr>
<td><strong>Phenomenological</strong></td>
<td>Organizational identity reflected in organizational discourse.</td>
<td>The phenomenological component is organizational discourse related to how the organization must act in order to be consistent with who the organization is. Sticking with Google as an example, Google’s design principles are organizational discourse that guides organizational action to ensure consistency with who the organization is.</td>
</tr>
</tbody>
</table>

Table 4-1 Components of organizational identity.

---

13 See http://www.google.com/support/jobs/bin/static.py?page=about.html
15 See http://www.google.com/support/jobs/bin/static.py?page=about.html&about=top10
Defining organizational identity in this manner results in organizational identity being simultaneously institutionally and socially constructed. Whetten’s emphasis that the definitional component of organizational identity is central, enduring, and unique and difficult to change or act against indicates that organizational identity becomes institutionalized and existing, to some degree, beyond organizational members ability to enact it. At the same time the ideational component of organizational identity clearly is a social construction; existing only as it is enacted by organizational members. It seems clear then, that Whetten’s definition of organizational identity more closely resembles a structurationalist argument (DeSanctis & Poole, 1994; Orlikowski, 2000; Rose, 1998) – organizational identity is a socially constructed structure that in turn enables and constrains future organizational behavior. Indeed, Bouchikhi & Kimberly (2001, as cited in Brunninge, 2005, p. 19) make precisely this claim.

It seems clear that the social actor and social construction perspectives are encompassed by Whetten’s overarching definition of organizational identity; indeed this is the very point of Whetten’s follow-up commentary. Where the debate resides – and where Ravasi & Shultz’s two-perspective approach applies – is the degree to which organizational identity is primarily an institutionalized social property or is a malleable social construction that is regularly renegotiated. It is this debate that is reflected in the various forms of research on organizational identity. Prior to reviewing that research however, it is important to distinguish organizational identity from two related, but not identical concepts: organizational culture and organizational image.

Organizational Culture & Image
Organizational culture and organizational image are closely linked to organizational identity in the literature. Like organizational identity, the definition of organizational culture has
many components. In the IS literature, organizational culture is treated as the basic assumptions about values, relationships, behavior, and truth (Leidner & Kayworth, 2006). Organizational culture shapes organizational identity in much the same way the culture we are in as individuals shapes our individual identities. Organizational identity is, in part, an expression of organizational culture and also embeds itself in culture (Hatch & Schultz, 1997). In this model, organizations develop an identity out of their organizational culture and that identity serves to reinforce the culture.

Organizational image is how the organization is perceived by outsiders (Dutton & Dukerich, 1991; Gioia et al., 2000; Hatch & Schultz, 1997, 2002). Organizational image can relate to both brand management and to how organizational action is perceived by relevant stakeholder groups. Organizational image reflects the organizational identity, and organizations clearly have a vested interest in managing their image as evidenced by the vast resources companies dedicate to the establishment and maintenance of their brand. Prior research has shown that when an organization’s perceived external image is misaligned with the organization’s actual image, the organization is subjected to pressures to either modify itself into alignment with the actual image or to adopt strategies geared towards bringing the actual image in line with the organization’s identity (Dutton & Dukerich, 1991; Hatch & Schultz, 2002).

Organizational identity, image, and culture are highly related concepts. Indeed, there is significant conceptual overlap among the three, and the boundaries separating each are ambiguous, particularly between culture and identity, to the point where organizational identity, image and culture have been referred to as a “conceptual minefield (Hatch & Schultz, 1997).” Hatch & Shultz (1997) differentiate between organizational culture and organizational identity this way: Organizational culture is tacit, contextual, and emergent; organizational identity is
textual, explicit, and instrumental. In other words, organizational culture is often found in implicit assumptions while organizational identity is overtly stated.

Hatch & Shultz (2002) propose of organizational identity dynamics that is particularly useful for understanding the organizational culture—identity—image relationship. In their model culture and identity, and identity and image are conceived of as interlocking parts. Organizational culture is expressed through identity claims; and expressions of organizational identity embed themselves in the culture creating a recursive, self-reinforcing relationship. Organizational image is in part shaped by expressions of organizational identity (for example through advertising); and organizational identity is reactive (or mirrors) its external image.

**Prior Research on Organizational Identity**

Scholars have found the concept of organizational identity to have great utility in understanding organizational behavior. Organizational identity has been explored in terms of the degree to which members of an organization identify with an organization (Albert, Ashforth, &
Dutton, 2000; Ashforth & Mael, 1989; Berger, Cunningham, & Drumwright, 2006; Foreman & Whetten, 2002), brand management (Cornelissen, Haslam, & Balmer, 2007; Ullrich, Wieseke, Christ, Schulze, & van Dick, 2007), organizational reactions to identity threats (Corley & Gioia, 2004; Gioia et al., 2000; Gioia & Thomas, 1996; Ravasi & Schultz, 2006), organizational adaptation to discrepancies between image and identity (Dutton & Dukerich, 1991; Gioia & Thomas, 1996), and ambiguity in organizational identity (Corley & Gioia, 2004) and as a shaper of organizational strategy (Brunninge, 2005).

**Organizational Identity as a Shaper of ICT**

Despite the diversity of phenomena for which organizational identity has provided insight, technology remains conspicuously absent from the list. Information and communications technologies are ubiquitous in organizational life. Indeed, disciplines such as Information Systems are dedicated to the study of the design and uses of ICT for managerial and corporate benefit. The use of ICT is particularly prevalent in law enforcement organizations for which the use of technology is considered fundamental to organizational operations (Manning, 2003b). This makes law enforcement organizations a particularly enticing organizational type to study when examining organizational identity’s influence on organizational ICT.

As discussed previously in this chapter, organizational identity has been found to play a significant role in organizational behavior both in terms of internal organizational behavior and reaction to external forces. Organizational identity both guides organizational action and is embedded in the organizational culture. Given the prominence of ICT in organizational activity, it is reasonable to expect that organizational identity would both play a role in the design and use of organizational ICT and be reflected in the organizational ICT artifacts.
Proposition 1: Organizational identity will be reflected in the processes through which organizations procure, design, and deploy ICT.

Proposition 2: Organizational identity will be reflected in the ways in which organizational ICT are materially arranged.

Proposition 3: Differences in organizational identity will have corresponding differences in organizational processes and organizational ICT.

Table 4-2: Organizational Identity Propositions

To this end, we should expect that the processes by which organizations procure, design, and deploy their ICT will reflect their individual identities. This reflection should be both visible in organizational practices related to ICT (for example, design or administrative processes) and in the ways in which the ICT artifacts are materially arranged. For example, an organization with an egalitarian identity could be expected to employ Free/Libre Open Source Software. If indeed organizational identity shapes organizational ICT in this way, we should also expect that differences in organizational identity will be reflected in differences in process and in material arrangements (or conversely, organizations with similar identities should have similar arrangements). We should expect, for example, that a corporate library will design and deploy its ICT differently from a public library. In this research I look at the role of organizational identity in the design and use of integrated criminal justice information systems.

This concludes the portion of this paper dedicated to the discussion of organizational identity both in terms of theory and empirical research. I have presented a definition of organizational identity, outlined the open debates about organizational identity research, and presented the reasoning behind extending organizational identity theory to the design and use of organizational ICT. I will now present the second theoretical frame that informs this research: boundary objects.
**Boundary Objects**

I have chosen boundary objects as a theoretical lens to study integrated criminal justice information systems for two reasons. One, an IJIS is a complex ensemble of technological and organizational components created to facilitate communication and collaboration among heterogeneous groups and boundary objects theory attempts to explain precisely the process by which that communication and collaboration occur. Two, there is an opportunity to extend boundary objects theory by applying it to an organizational phenomena of interest when its application had previously been primarily limited to the study of small groups.

**Boundary Objects Defined**

Boundary objects theory is a theory of communication and collaboration among heterogeneous communities. The core concept of boundary objects theory is that there are artifacts that span the boundaries of communities – termed ‘social worlds’ – and through which communication and collaboration can be achieved (Fleischmann, 2006a, 2006b; Star, 1989; Star & Griesemer, 1989). A social world is a community organized around specific activities, concerns, and forms of communication (Covi & Kling, 1996; Fleischmann, 2006a, 2006b). Another term for social world is ‘community of practice,’ and indeed, the two terms are often used interchangeably in the boundary objects literature.

Police are an example of a social world. The police are organized around a specific set of activities (catching offenders, preventing crime, public relations, community service, etc.) and they employ specific forms of communication (criminal codes, policies and procedures, standardized forms). We, as the general public, are not members of that social world of police,
and as a result were police to communicate to us as they do to other police, we would likely have great difficulty in accurately receiving and processing the information being conveyed.  

Yet the police and the general public certainly have a need to communicate and collaborate. Boundary objects are one way the communities of the police and the public are able to communicate. An example of a boundary object that facilitates communication between the police and the public are most-wanted lists. Most-wanted lists are a vehicle for the police to convey to the public their high-value targets for detention and arrest and to inform the public that these criminals are at large among the citizenry. For the public, most-wanted lists are source of information about the community and, potentially, a tool by which the public can communicate information about wanted individuals to the police.

Boundary objects exist independently of any single social world but are negotiated by each individual social world that engages them (Fleischmann, 2006a; Gasson, 1999, 2005; Luna-Reyes, Zhang, Gil-Garcia, & Cresswell, 2005; Sandusky, 2003). This dichotomy requires that boundary objects be flexible enough to be interpretable by individual social worlds while rigid enough that they retain meaning independent of any one social world (Ackerman & Halverson, 2004; Star, 1989; Star & Griesemer, 1989).

<table>
<thead>
<tr>
<th>Type</th>
<th>Definition</th>
<th>Advantages</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repositories</td>
<td>Modular, indexed collections of objects</td>
<td>Modularity</td>
<td>Library</td>
</tr>
<tr>
<td>Ideal/Platonic</td>
<td>Abstracted objects eliminating local contingencies</td>
<td>Adaptability</td>
<td>Model Rocket</td>
</tr>
</tbody>
</table>

To illustrate this point, consider how policing is represented in popular entertainment. When an arrest is made, the cops never say “You are under arrest for violation of California criminal codes 481 and 187.” They say “You are under arrest for arson and murder.” This is because the general public is generally unaware of specific criminal codes but understands the terms ‘arson’ and ‘murder.’
In her seminal work on boundary objects, Leigh Star identified four ideal types based on the information joined to create the boundary object (Star, 1989). These four types of boundary objects are *repositories*, *platonic*, *terrain with coincident boundaries*, and *forms and labels*. Repository boundary objects are modular, indexed collections of objects – for example libraries. Platonic type boundary objects are objects that have been abstracted to a level that overcomes local specifics but are also locally interpretable; for example, model rockets which is a boundary object that spans the groups of aerospace engineers and enthusiasts. The terrain with coincident boundaries objects are those objects that have the same external boundaries but different internal content. Maps are example of this type of object: a map of Pennsylvania has the same boundaries (the state line) but can have different internal content (transportation, topography, weather patterns, etc.). Finally, the forms and labels type boundary objects are those objects that standardize language in order to facilitate communication. A field investigation (FI) report is an excellent example of this type of object. A standard FI form conveys information to the administrator responsible for monitoring the activities of his officer; to the detective investigating the crime; and to the crime analyst assessing crime trends in a particular neighborhood. All three individuals work within sub-communities of law enforcement and the report acts as the boundary object among them.\(^{18}\)

---

\(^{18}\) In the same way that a sketch of a car acts as a boundary object among engineers, marketers, and manufacturers.
Prior Research on Boundary Objects

Boundary objects have been particularly useful for understanding collaboration among groups using technology. Significant research has been done on boundary objects in the fields of Information Systems (IS), Computer-Supported Collaborative Work (CSCW), and Library and Information Sciences (LIS). Much of boundary objects research has focused on identifying boundary objects in practice. Examples include database records of aircraft maintenance requests (Lutters & Ackerman, 2007), digital dissection simulators for education (Fleischmann, 2006b), a call tracking database (Ackerman & Halverson, 1999), organizational information systems (Pawlowski, Robey, & Raven, 2000), sketches (Henderson, 1991), and process maps (Fenton, 2007).

There has also been research into identifying additional properties of boundary objects (Levina, 2005). Some types of boundary objects are better suited for spanning specific types of knowledge boundaries (Carlile, 2002). Boundary objects must be able to create common ground across communities in order to be effective (Bechky, 2003); and the trajectory of a boundary objects future use must be properly projected in order to be effective (Ackerman & Halverson, 2004).

In both streams of boundary objects research, the focus has been on the use and creation of artifacts in the process of work rather than the properties of the artifacts themselves. This has resulted in an emphasis on capturing the negotiations and understandings that occur around and through boundary objects. Some have even argued that the focus should be on ‘boundary negotiating artifacts rather than boundary objects (C. P. Lee, 2007). A consequence of this focus on process has been that boundary objects themselves remain largely underspecified and highly abstract.
IJIS as Boundary Objects

As interorganizational information systems, it seems clear IJIS act as boundary objects both within and across the agencies that participate in them, as well as between the agencies and other stakeholder groups (such as the public). I propose, therefore, that IJIS are ensembles of one more of the four types of boundary objects. What is not clear is what type of boundary object describes an IJIS. Through this research I seek to identify what type of boundary object describes IJIS most completely and to identify the social worlds the IJIS boundary object spans.

Conclusion

In this chapter I have presented a synthesis of the extant literature on organizational identity and boundary objects and outlined how these two theoretical frames inform this research. Organizational identity – the perceptions of who the organization; the central, enduring, and unique organizational features; and the organizational discourse on organizational action – has been show to play a significant role in organizational behavior. This research looks at how organizational identity shapes the design, configuration, and use of organizational ICT.

Boundary objects are a means of understanding communication among heterogeneous groups. By being both flexible enough to be negotiated and understood by individual groups, and rigid enough to exist independent of any particular group, a boundary object facilitates communication through standardization (standards and forms), abstraction (ideal/platonic), flexibility (terrain with coincident boundaries), and collection (repositories). This research seeks to identify the ways in which IJIS serve these functions.
Chapter 5 Research Design

Introduction
In this chapter I describe in detail the research design I employed for this dissertation. There were both ontological and pragmatic requirements that led to my choice of this research design. From an ontological perspective this research needed to capture both details of the artifact and details of the social context within which it is engaged. Pragmatically, this research had to be achievable within the constraints of limited access and limited resources. For this reason I have chosen to conduct case studies of two IJIS supported by secondary data and direct observation. This strategy allowed me to observe and analyze the micro-level context, the meso-level similarities and differences between the two cases, and understand the broader institutional context in which the two IJIS reside.

Rationale for Research Design

Design Requirements
Identifying and understanding the requirements of a design before embarking on its construction is critical. The need to know the requirements of a design remains true whether designing the cockpit of a fighter jet or a highly complex experiment. Requirements serve to define both the boundaries and the details of a project. As such, it is useful to outline the requirements that guided this dissertation and their relation to the research design here.

I identified two categories of requirement for this research design: paradigmatic and pragmatic. The former category contains the research design requirements that ontology, epistemology and theory choice present; for example, a strongly neo-positivist paradigm presents a number of methodological requirements including generalizability, replicability, and

---

19 I use the term paradigmatic broadly to describe the sum of my ontological, epistemological, and theoretical frame as a social informatics scholar. In practice, social-informatics may be pre-paradigmatic (Kuhn, 1996b).
falsifiability (A. S. Lee, 1991). Conversely, an interpretivist paradigm requires the method to capture the subjective perceptions of the researcher and the subject (Burrell & Morgan, 1979). Identifying the ontological, epistemological, and theoretical requirements of a research design is critical to establishing the *prima facie* validity of the subsequent research.

The latter category of requirement consists of the research design requirements that reflect the needs and constraints presented by real-world; for example, logistical and resource limitations, constraints on access, etc. Engaging in social science research through the application of field research methods mean that data collection is necessarily subject to external constraints. It is important to stipulate these constraints in order to help establish the limitations of the research. In what follows, I outline both paradigmatic and pragmatic requirements and their impact on this dissertation.

**Paradigmatic/Theoretical Requirements**

Three paradigmatic / theoretical requirements motivated this research design: (1) an organizational level of analysis; (2) the need to account for both the properties of the artifact\(^{20}\) and larger social context; (3) The need for a research design that facilitates elaboration of extant theory. These requirements are not isolated, but linked by ontology, theory choice, and research questions.

**Organizational Level of Analysis**

The phenomenon of interest and the choices of theory for this dissertation require an organizational level of analysis. I am researching IJIS using the theoretical lenses of organizational identity and boundary objects. As defined in Chapter 4, and to be further articulated in the discussion of the unit of analysis, an IJIS is a hybrid system comprised of both

---

\(^{20}\) When I refer to the ‘artifact’ I refer to the physical technological object or the properties and features of the software.
integrated organizational and technological elements. This hybrid-form is what distinguishes an IJIS from a “simple” off-the-shelf application or piece of hardware and from organizational collaborations among law enforcement that don’t contain an integrated ICT component.

I separately employed two theories – boundary objects and organizational identity – in this dissertation. Boundary objects theory can be applied at multiple levels – it is regularly used to study groups – so it presented fewer constraints on level of analysis. However, organizational identity theory clearly dictates an organizational level of analysis as it seeks to explain the collective identity of the organization. Even though it may be reflected in the actions and attitudes of individual members of the organization, organizational identity is an attribute of the organization as a collective. This means that the appropriate application of organizational identity as I applied it here was the organizational level of analysis.

Phenomenon and theory choice dictated that the research design must be appropriate to the collection and analysis of data that occurs at the organizational level of analysis. Common research designs for studying organizations include the case study (c.f., Markus, 1983; Orlowski, 1992), ethnography (c.f., Suchman, 1987), and action research (Baskerville & Wood-Harper, 1996; Baskerville & Wood-Harper, 1998). In contrast, the experimental method seemed difficult if not impossible to apply to an organization, particularly to real organizations in the larger world beyond a laboratory. For reasons that will be discussed in greater detail later in this chapter, I identified the case study as the appropriate methodology to structure my research design around.

The importance of capturing detail and context
In adopting a social informatics perspective I am driven to study an ICT-related problem in a way that accounts for both the material properties of the artifact and the surrounding social
context. Meeting this requirement precluded any research design that employs data collection and analytical methods that would fail to capture both. For example, it was clearly inappropriate for this dissertation to base my research design on an experimental or quasi-experimental method as both by definition seek to control for, rather than account for, social context. Similarly, to rely exclusively on deconstruction of secondary data would be inappropriate to this research because to do so would fail to capture important contextual details. Therefore, as with an organizational level of analysis, the requirement that I capture both detail and context led to my choice of qualitative methods of data collection and analysis.

**Theory elaboration and extension**
A third motivation for this research was to elaborate and extend extant theory. Theory elaboration is “the process of refining a theory, model, or concept through qualitative data analysis in order to specify more carefully the circumstances in which it does or does not offer potential for explanation (Vaughan, 1992).” The goal of theory elaboration is to refine or clarify theory rather than test theory. In theory elaboration case studies are analyzed and compared on some particular event, activity, or circumstance. As a result my research design included case studies.

**Pragmatic Restrictions**
There were two pragmatic restrictions that impacted this research design. One restriction was the issue of restricted or limited access to data. A second pragmatic restriction was the limited time and resources available to complete this research. Combined these requirements serve to limit the overall research design.

**Limited access**
Law enforcement is an enterprise that inherently involves sensitive information. People who have been charged with a crime or otherwise negatively involved with the criminal justice
system (as criminals or victims) generally do not want that information to be widely known. For example, witness the ongoing debates over the publishing of sex offender information. Even victims of crime often do not want their information to be viewable by the public, and so victims of domestic violence or sex crimes have their names withheld from the public. In general, the criminal justice domain has specific rules about what criminal justice data can be viewed by the public and it is often very limited.

There is also the issue of revealing too much to the public about police operations and systems may negatively impact policing operations by exposing weaknesses to those who would exploit them. Therefore access to individual systems was likely to be limited to surface-level presentation using fictional data. Data presented via publication from this research must be generalized enough to not risk breaching of operational secrets.

Finally, access was also limited by the availability of the organizations being studied. Providing access both to facilities, people, and artifacts is necessarily a time-consuming activity for organizations and one that is, at best, tangential to their overall organizational mission. Sawyer (2008) notes, method choice and research design are often determined by access to data, and so it is the case for this research. As a result, the design of this research was based in part on the anticipated access to the organizations studied.

**Limited resources**

The second restriction for this research was limited resources. This research was generously funded by grants from the National Science foundation. Resources were not unlimited however, and the amount of in-person data collection that can be performed in the course of this research was limited in part by the limitations of the funding from the NSF. This was particularly true for the case study of the ARJIS system which requires long distance travel...
in order to collect data in person. Where it was possible, remote methods of data access (telephone interviews, e-mail, video conferencing, etc.) were employed to compensate for this limitation. Finally, other professional obligations prevented me from pursuing more time-intensive data collection methods such as ethnography.

**Research Design**

The design employed for this research is three-tiered, consisting of micro-level detail, meso-level analysis, and macro-level context. Two in-depth case studies employing multiple data collection methods such as interviews and document analysis from multiple data sources were used to capture the micro-level detail. These cases provided a detailed understanding and thorough description of the interaction between organizational identity and the design and use of integrated criminal justice information systems.

The meso-level analysis consisted of a comparison of the theoretical propositions (See Table 4-2) against individual cases. The purpose of the meso-level analysis was to find similarities and differences among the individual cases using analytic induction; and to draw conclusions about those findings in terms of organizational identity and organizational computing at a more general level (Eisenhardt, 1989). Initial theoretical propositions were tested against the initial case, refined, and then tested against the second case. The results from the second comparison represent the findings of this research.

Macro-level context was derived from the collection and analysis of secondary and archival data. The purpose of analyzing macro-level data was to frame the cases-in a larger institutional context, identify common institutional and environmental pressures, and to generate macro-level insights about the design and use of integrated criminal justice information systems.
Micro-level detail: case studies

This research consisted of two individual case studies with a common unit of analysis: the integrated criminal justice information system. Multiple sources of evidence and analytical methods were employed within each individual case study and across all three studies. These case studies were used to collect rich detail about integrated criminal justice information systems and how organizational identity shapes their design and use.

I chose to conduct two case studies for the pragmatic reasons discussed above. One, the resources available for conducting this research made it unfeasible to conduct more than two case studies. Conducting in-depth case studies is resource-intensive enterprise fiscally, logistically, and temporally (Yin, 2003d, pp. 10-11). In order to complete the research in an acceptable time frame and to do so within the constraints of available resources, the number of case studies to be conducted had to be limited. It should be noted however that while increasing the number of cases studies would have served to increase validity of the findings, conducting only two case studies provides stronger findings than a single case study (Yin, 2003c, p. 53).

Definition of the case study

The case study is a research method used for the purposes of capturing holistic detail in natural settings. The case study method has been defined in a number of ways, and there is some ambiguity in, for example, how a case study differs from other qualitative methods such as ethnography and field studies\(^{21}\). However, a definition of the case study method that has been

\(^{21}\) The ambiguity of exactly how the case study method differs from other methods such as field study is evident in Darke, Shanks, & Broadbent’s (1998) guidance on how to successfully complete a case study in which they argue that the difference between case study and field research is the degree of \textit{a priori} knowledge held by the researcher while at the same time stipulating that the distinction is a “matter of degree” and “sometimes difficult to discern.” A thorough discussion of the differences in various qualitative methodologies is beyond the scope of this manuscript. For the purposes of this research, I defer that debate and accept the body of literature (e.g., Campbell (1975), Miles & Huberman (1984) Stake (1994), and Yin (1994)) that treats the case study as a unique qualitative methodology.
widely accepted and cited in qualitative research (c.f., Benbasat, Goldstein, & Mead, 1987; Flyvbjerg, 2006) is Yin’s (2003d, p. 13) definition:

A case study is an empirical inquiry that investigates a contemporary phenomenon within a real-life context, especially when the boundaries between phenomenon and context are not clearly evident. Fundamental to this definition is the premise that the basis for doing a case study is a need to observe the phenomenon of interest in situ. The emphasis on phenomenon-in-context is directly relevant to the selection of case study as a method for this research and will be discussed in greater detail later in the chapter. Prior to doing so however, the case study methodology needs to be described in greater detail.

The case study as a method is a valuable tool in at least four ways. First, the case study method is particularly appropriate for descriptive research in which the research seeks to identify how and why something occurs (Benbasat et al., 1987; Yin, 2003d, p. 5). Examples of descriptive case studies of information and communications technologies include Blanton et al.’s (1992) study of information technology organization and Majchrzak et al.’s (2000) case study of virtual teams. However, case studies are not limited to purely descriptive application. Case studies may also be exploratory and even explanatory (Yin, 2003d, p. 3). Action research and application description have also been identified as forms of the case study (Benbasat et al., 1987). Case studies are considered to be appropriate for theory development and extension, and even falsification (Benbasat et al., 1987; Darke et al., 1998; Flyvbjerg, 2006; Stake, 1978), providing further evidence of the case study’s utility as a method. With such flexibility of application, the case study is of great utility to the researcher.
When conducting a case study, the researcher often relies on multiple sources of evidence and analysis techniques. Typical sources of evidence relied upon in conducting case studies include documentation, archival records, interviews, direct observation, participant observation, and physical artifacts (Benbasat et al., 1987; Yin, 2003c, p. 86). The researcher uses as many of these sources of evidence as possible in an effort to gain as complete a picture of the phenomenon being studied as possible. This is called triangulation of data sources.

Triangulation of data sources or methods is a way of ensuring a complete picture of what is being studied, adapting for contingencies that emerge in collection and analysis of data, and confirming findings (Denzin & Lincoln, 1994; Jack & Raturi, 2006; Jick, 1979). The essence of triangulation is that the use of multiple, complementary components (e.g., data, method, theory) to compensate for the weaknesses of any individual method and thereby increasing validity of the findings (Jick, 1979; Lincoln & Guba, 1985; Yin, 2003a, p. 97). Jack & Raturi (2006) identify five basic types of triangulation: data sources, analytical method, observers, theory, and multiple (sources, observers, and theories). Triangulating data sources in this research serves to support findings of organizational identity as a collective perception rather than the idiosyncratic perception of an individual.

In addition to triangulation, the conducting and comparing of multiple case studies is also a preferred technique for increasing the validity and generalizability of the findings as well as theory development and testing (Benbasat et al., 1987; Yin, 2003c, p. 46). This is the process of analytic induction in which a priori theoretical propositions are tested against the empirical data.

---

22 In Yin’s discussion of sources of evidence, he distinguishes between direct observation and participant observation as a difference in the action of the researcher. In the former, the researcher is strictly an observer; in the latter, a participant in the case being studied.
of the case (Yan & Gray, 1994). When a hypothesis holds true across multiple cases, it can be considered conditionally generalizable to that phenomenon until a contrary case arises.

**Meso-level analysis: analytic induction**

For the meso-level analysis, the research design for this study will be a comparative case study; or, as Yin (Yin, 2003c, p. 40) terms it, an embedded multiple-case study. Multiple case studies are good for description and theory building (Benbasat et al., 1987), both of which are goals of this research. A comparative case study consists of conducting several individual case studies of similar / common units of analysis and then comparing the findings of each for similarity and variance (c.f., Barley, 1986 for a classic example and motivation). The unit of analysis is what defines the boundaries of the case (Yin, 2003c, pp. 22-26). The case studies are embedded because they move between multiple levels of analysis, e.g., organizational, individual, group, and system (p.40).

**Analytic induction as a method**

Conducting multiple case studies of similar phenomena, one can identify recurring patterns and make general propositions. This is called analytic induction. Analytic induction is a analytical method for testing and refining theory (Robinson, 1951). As a research method has a well established tradition in the social sciences (Cressey, 1950; Glaser, 1965; Robinson, 1951). There are six steps to the process of analytic induction:

1. A phenomenon is defined.
2. A hypothesis (or theoretical proposition) is formulated.

---

23 The unit of analysis is different from the level of analysis. As stated, the former is the phenomenon-of-interest that represents the boundaries of the case. The latter represents the level (e.g., individual, group, organizational, societal) at which the analysis is conducted.

24 The alternative form of case study is the holistic form with a single level of analysis (e.g., organizational).

25 I say similar because by definition – contextual phenomenon cannot be replicated in multiple instances. That said, the goal is to define the properties of a case in a way that each subsequent case is as close as possible to be identical to the previous cases.
3. The formulated hypothesis/proposition is evaluated against a case.

4. If the case evidence does not support the hypothesis/proposition, the hypothesis/proposition is revised or the phenomenon is redefined to exclude the case (e.g., the case was originally thought to be representative of the phenomenon and is discovered not to be).

5. Confirmation of the hypothesis/proposition from a limited number of cases results in ‘practical certainty’ of its validity\(^{26}\).

6. The hypothesis/proposition remains confirmed until a contrary case is found.

The outcome of these six steps is a finding that occurs across multiple cases and is generalizable beyond any individual case.

Some may argue that inductively generalizing from a single case study is epistemologically problematic and runs the risk of being easily falsified by a single counterexample (Benbasat et al., 1987)\(^{27}\). This argument is unpersuasive. The analytic induction process is a method for qualitatively testing a hypothesis and deriving improved hypotheses from those that fail. In other words, by identifying those hypotheses that fail the researcher narrows the possible hypotheses, closing in on the ‘true’ or strongest hypothesis. This predicting and observing of similar phenomena through multiple case studies is called “literal replication” in Yin’s terminology (p. 47) and the idea is that as successful test of a hypothesis is replicated, it is increasingly likely that it is true across most general cases. Conducting multiple

\(^{26}\) ‘Practical certainty’ reflects the concept that given a case that cannot be excluded as unrepresentative of the phenomenon, we can be practically certain that the hypothesized conditions follow. However, because the number of cases sampled is limited, any negative instance of a case that is considered representative nullifies the hypothesis (Robinson, 1951). For example, if the hypothesis is ‘patrol officers require mobility in the technology they employ in performing normal job activities,’ we can be practically certain of the truth of the hypothesis only until a counterexample arises. At that point, we either have to dismiss the counterexample as not representative of the phenomenon (e.g., the patrol officer was not performing normal job activity) or we must revise the hypothesis to account for the new data.

\(^{27}\) This problem – “The Problem of Induction” – is Karl Popper’s main criticism of the philosophy of Logical Positivism in *The Logic of Scientific Discovery* (c.f., Popper, 2002, pp. 1-7).
case studies is, in this case, similar to conducting multiple experiments on the same subject and revising the hypothesis each time to account for counterfactual results (Yin, 2003c, p. 47).

Analytic induction was appropriate to this research because the research starts with a priori theoretical propositions. As discussed in Chapter 3, I proposed that organizational identity shapes the design and use of integrated criminal justice information systems acting; and IJIS act boundary objects between the agencies that participate in them & other stakeholders. These initial hypotheses were tested using analytic induction against an initial case of an IJIS. Based on the analysis of the empirical data, I then revised the hypotheses to account for discrepancies. The revised hypotheses will were then tested against a second case of an IJIS. The resultant hypothesis provided a working theory of the relationship between organizational identity and the design and use of inter-organizational collaborative information systems.

In this summary of the case study method I have engaged the nature of the evidence a case study collects, the data sources relied upon in a case study, and the types of case studies that can been conducted has been discussed. I have shown how, using the procedure of analytic induction, generalizable propositions can be derived through the comparison of multiple cases. I now turn to a discussion of the theory development technique of analytic induction and its application to this research.

Consistent with the process of analytic induction, the comparison of propositions to case, and case to case was sequential. In other words, the initial set of theoretical propositions was evaluated against first case. Based on the findings of the first case the propositions were then revised, and then compared to the second case. Propositions that were confirmed in across both cases represent the findings of this research.
Macro-context: secondary data

To gain macro-level context, secondary and archival data was collected and analyzed. Examples of such data included census data such as the Bureau of Justice Statistics police census and sample survey (Bureau of Justice Statistics, 2000a, 2000b), commentary from the public and trade press, legislative records, and other publicly available data on integrated criminal justice information systems. The purpose of this tier of the research design was to frame the cases in a larger institutional context, identify trends in integrated criminal justice information systems as a whole, and identify common environmental pressures on integrated criminal justice system initiatives.

Phenomena of Interest

The phenomenon of interest to which each case study was bounded is the integrated criminal justice information system. Drawing on the discussion in Chapter 3, for an IJIS to qualify as the unit of analysis it needed to be: multi-organizational, multi-application, have its own governance structure, and be centered on law enforcement activity. Also an IJIS could not exclusively be an infrastructure or social agreement. In other words, as I defined it, an IJIS was not exclusively hardware and connectivity tools; nor is an IJIS simply an agreement between agencies to collaborate through a technological medium. Rather an IJIS was an ensemble of technical infrastructure, organizational infrastructure, and collaborative activities. Defining the phenomena of interest this way excluded single-agency systems such as the local police force implementing its own records management system from consideration.
<table>
<thead>
<tr>
<th>Criterion</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Multi-application &amp; multi-device</td>
<td>An IJIS has a suite of technological applications and devices; for example mobile terminals, back-end databases, hand-held cellular devices; A single COTS application does not qualify as an IJIS</td>
</tr>
<tr>
<td>2</td>
<td>Multi-organizational</td>
<td>An IJIS is multi-organizational in which member organizations participate in the design, governance, and support of the IJIS. There may be an additional separate organizational structure that represents the IJIS itself. For example, the organizational infrastructure may be a committee hierarchy, a governance document detailing bureaucratic procedures, and a dispute resolution system.</td>
</tr>
<tr>
<td>3</td>
<td>Governance structure</td>
<td>An IJIS has some governance structure in place to facilitate administration, operations, dispute resolution, development, and collaboration. For example this may be as “simple” as a contact, or as complex as a multi-level governance hierarchy including procedures and regulations.</td>
</tr>
<tr>
<td>4</td>
<td>Centered around law enforcement</td>
<td>The primary purpose of an IJIS is to facilitate law enforcement operations. This distinguishes it from other networked systems such as radio systems shared among all first responders.</td>
</tr>
</tbody>
</table>

Table 5-1 Defining the phenomenon of interest.

I defined integrated criminal justice information systems in this manner for the two reasons. One, this definition is consistent with how integrated criminal justice information systems have been defined in the prior literature (c.f., National Association of State Chief Information Officers (NASCIO), 2003). Two, bounding the cases this way ensures that when
conducting analytic induction the individual cases are as approximately similar as they can be because the properties of an IJIS narrow the possible case subjects significantly.

The phenomena of interest were measured at multiple levels of analysis. These levels included the organizational level – both of the IJIS organization and the participating organizations; the artifact or device level; and the contextual level. For example, data was collected on organizational identity at the organizational level – e.g., corporate statements of mission, practices, values; and at the artifact level – features or uses of the device that reflect organizational identity of the IJIS. Data for the contextual level included details about the contextual influences on what is being observed – such as institutional pressures (e.g., the government has mandated the system contain a particular feature) and environmental factors (e.g., the officer needed to keep her eyes on the suspect while using the hardware).

**Sampling**

This research used theoretical sampling to select the IJIS which will be studied. Theoretical sampling is sampling (site selection) based on the research questions being asked with the goal of replicating, extending, or filling gaps in existing theory (Benbasat et al., 1987; Eisenhardt, 1989). The sampling method is not random, but deliberate, based on the theoretical constructs guiding the research.

Theoretical sampling is recommended over population sampling for theory-building case studies (Eisenhardt, 1989). This is because unlike population sampling which is used with the goal of generalizing to a larger population from a random sample; theoretical sampling is used in order to generalize the results to the *theory*.

<table>
<thead>
<tr>
<th><strong>Criterion</strong></th>
<th><strong>Reason</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cases must be organizational</td>
<td>Theoretical frame is at organizational level of</td>
</tr>
</tbody>
</table>
Systems must be operational | The purpose of the study is to observe identity processes in ICT design and use; design and use cannot be contemporarily observed in inactive or non-operational systems

Organizations must be engaged in design of systems | Can be design-through-use but is ideally active participation in design decisions relating to the system

Technological infrastructure | IJIS are complex socio-technical systems of which the technological artifact is a key component

Multi-organizational & collaborative | For an IJIS to serve as a boundary object, it must reside amongst multiple organizations, through which the organizations collaborate

Centered around law enforcement | IJIS are fundamentally law enforcement ICT

Table 5-2 Sampling criteria.

The sampling for this research was determined by the research questions and the phenomena of interest (IJIS). Table 5-2 lists each individual criterion and the rationale on which the criterion has been chosen. In Chapter 1 I listed five specific research questions. The two research questions most relevant to the issue sampling are:

\[OI3: \text{How do the designs of organizational information systems, devices, and applications reflect their unique identity?}\]

\[BO1: \text{In what ways do organizational information systems serve the role of boundary object among various social worlds such as governments, publics, and systems?}\]

From these questions the following sampling criteria emerge:

1. Cases must be organizations – the IJIS must have its own organizational component distinct from any single member agency.
2. The IJIS must be operational – in order to study design outcomes there must be systems in place,
3. IJIS must be engaged in designing of their systems – in order to study design activity systems must be at a minimum configurable and as a best case – actively designed by the IJIS
The phenomena of interest results in the following sampling criteria:

1. Technological infrastructure – multiple applications and devices
2. Multi-organizational & collaborative – must be more than simple sharing agreements or informal negotiations.
3. Governance structure – must include institutional structures or processes
4. Systems must be used for criminal justice / law enforcement operations

These seven sampling criteria narrowed the possible sites for selection significantly. At the time of this research, only a few criminal justice IT integration initiatives met these criteria.

Establishment of Reliability

I used four methods for increasing the reliability of the findings. First, a detailed case study protocol was developed to structure the research and to help ensure that the data collected is appropriate to the research questions asked. The case study protocol included an overview of the project, detailed field procedures, case study questions, and procedures for formatting data, and performing analysis. Yin (2003b, p. 67) considers the case study protocol to be one of the major ways of increasing reliability in a case study because the case study protocol helps to ensure consistency of data collection in individual and multiple cases.

A second method for increasing reliability employed in this research is the construction of a case study database. A case study database is a detailed repository of data, investigator analyses, and information about the situation in which the data was collected (Yin, 2003a, pp. 99-107). The case study database provides a way of maintaining the “chain of evidence” allowing another individual to examine in detail the case study data and follow the logic of the analysis. For this research, a database was created for each individual case, for the comparative
study, and the secondary data collection using a combination of analog (e.g., paper records, files, etc.) and Microsoft Excel and nVivo.

Third I used the criteria developed by Brower, Abolafia, and Carr (2000) for improving qualitative methods in general that are applicable to this study. The criteria are split into two categories: data collection, analysis and presentation; and purpose and nature of research – adequacy of theorization. Three criteria comprise the first category: authenticity, plausibility, and criticality. Authenticity is described as conveying that the research as actually “been there,” and is obtained through “thick, rich descriptions” such as those common to ethnography (Bate, 1997). Plausibility deals with whether or not the findings make sense to the reader. Plausibility can be achieved through legitimizing research methods. Criticality refers to challenging readers assumptions. This criterion in particular is consistent with the both theories used in this paper as well as the social informatics perspective in general.

The second category has four criteria: purpose, research question, research design, and theoretical base. For the most part these criteria are self-explanatory and applicable to any study whether it be qualitative or quantitative or some combination of the two. As a result, they were useful for evaluating the proposed study.

<table>
<thead>
<tr>
<th>Brower et al. (2000) Criteria</th>
<th>Proposed Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the account seem authentic?</td>
<td>Uses ethnographic tools such as interviews, document analysis and “ride-alongs” provide data for thick descriptions</td>
</tr>
<tr>
<td>Does the account seem plausible to me as a reader?</td>
<td>By grounding results in theory, account should be plausible.</td>
</tr>
<tr>
<td>Does the account possess criticality in form and rhetorical style?</td>
<td>Theoretical basis of study adopts a critical approach.</td>
</tr>
</tbody>
</table>
Is the purpose descriptive, explanatory, or theoretical? | Descriptive.
---|---
Is there a formally stated research question? | General research questions are stipulated, some will be emergent consistent with the methodology.
Is the research design appropriate to answer the question? | Yes. Case studies have been used to demonstrate both theories.
Doe the conclusions contain theoretical explanations that the author relates to extant theory? | Yes. Conclusions are grounded in the theoretical basis for the paper.

| Table 5-3 Establishing validity. |

Finally, triangulation both in terms of triangulating data sources and data types served increase reliability by compensating for the weaknesses of individual data types and sources. Using a detailed case study protocol, a comprehensive case study database, Brower et al. (2000) criteria for assessing qualitative research, and triangulation will serve to ensure that the findings of the proposed research are reliable and stand up to independent review.

**Conclusion**

In this chapter I have presented the research design I used for this dissertation. The research design is grounded in the paradigmatic and pragmatic considerations attached to this research such as the need to capture context and limited resources. I chose to conduct and compare to case studies using the method of analytic induction. I chose to supplement the micro-level detail of the case studies with macro-level context obtained through analysis of secondary data.
Chapter 6 Data Collection & Analysis

Introduction

In this chapter I detail the collection and analysis of the empirical data for the ARJIS and JNET case studies. Overall, I conducted 14 interviews, analyzed 448 primary documents, and observed over 30 hours of organizational meetings across the two cases. To analyze this data I used a hybrid *a priori* / inductive coding scheme. Employing analytic induction, my findings from the first case study were used to revise and reformulate my initial hypotheses for comparison against the second case. The remainder of this chapter proceeds as follows. I begin with a discussion of the revised research design and subsequent collection of data. Each source of data (interviews, documents, observation) is discussed. The next section details the coding schema I used for analysis. I then conclude with a brief discussion of how I employed analytic induction across the two cases.

<table>
<thead>
<tr>
<th>Source</th>
<th>ARJIS</th>
<th>JNET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviews</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Documents</td>
<td>281</td>
<td>167</td>
</tr>
<tr>
<td>Direct observation</td>
<td>None</td>
<td>30+</td>
</tr>
</tbody>
</table>

Table 6-1 Sources of evidence.

Data Collected

Revised Data Collection Strategy

The actual collection of data varied from the original research design due to two issues that emerged during the course of data collection. One, it became clear almost immediately that validating the analysis of perceived organizational identity via a survey instrument would be inappropriate given the size of the organizations which in the cases of both ARJIS and JNET, are very small. I had initially planned to validate the statements of organizational identity that emerged in analysis using a survey instrument. In practice, initial interviews indicated that
neither ARJIS nor JNET was a large enough organization to warrant using the survey to validate qualitative findings. Sample-size would have been too small for both orgs given the limited number of organizational members. Surveys are useful for when there are a large number of respondents, which was not true of either ARJIS or JNET. As a result, the decision was made to member-check findings derived from the initial set of interviews. While in making this revision in data collection strategy I forfeited the ability to collect data from every member of the organization, I realized the additional benefit of allowing subjects to elaborate on their responses to my initial findings thereby providing greater clarity and substance to the findings overall.

Two, gaining access to conduct the ARJIS case study became increasingly difficult with time thereby limiting the amount of data I was able to collect via interviews and direct observations. The increased difficulty I had in maintaining access to ARJIS over time was largely attributable to the staff’s inability to divert time from other organizational priorities in part because of economic pressures.

**Interviews**

I decided to conduct interviews of key informants. The use of key informants is considered an appropriate method of data gathering when a survey is inappropriate and when the researcher would like the subject to generalize beyond their individual feelings, perceptions or behaviors (Kumar, Stern, & Anderson, 1993). An organizational member is considered a key informant when they are considered knowledgeable about the subject of the interview and willing to communicate their knowledge (Kumar et al., 1993; Tremblay, 1957).

In formulating my research design, I decided upon conducting semi-structured interviews of my key informants (see Appendices A & B for detailed descriptions of the interview guides). Semi-structured interviews have structure to provide a general flow to the interview and insure
important topics are covered during the interview; while at the same time leaving flexibility to pursue avenues of inquiry that emerge during the conducting of the interview (Berg, 1989). I chose semi-structured interviews because I wanted to be able to guide the interview but also be able to pursue interesting comments from the subjects (particularly those related to identity or boundary spanning) as they came up.

I also considered using structured and unstructured interviews for this research. In the end, I chose not to conduct structured interviews because a structured interview would have been too focused and thereby limiting of my ability to explore interviewee responses in greater depth. I chose not to conduct unstructured interviews for the opposite reason. I began this research with *a priori* propositions I wanted to explore and an unstructured interview provided no guarantees that those propositions would be explored during the course of the interview.

In both the ARJIS and JNET cases, initial contact was made with the top manager (Executive Director) of the organization. Prior to conducting this research I was already aware that the ARJIS Executive Director was to whom I should make initial contact. My original contact for JNET was no longer with JNET; having moved up to become the Deputy Chief Information Officer. My original contact directed me to meet with the current Executive Director of JNET and made introductions on my behalf. Initial contacts with ARJIS and JNET consisted of a one-hour semi-structured interview designed to elicit a general picture of the current status of the IJIS, to identify other key informants, and to elicit the top manager’s perceptions of the IJIS’ identity.

After making initial contact with the key informants a first round of one-hour semi-structured interviews was then conducted with other members of the organization. These
Interviews were designed to elicit details of the organizational structures and processes of the respective IJIS, the technological architectures of the respective IJIS, and the informants’ perceptions of the IJIS identity. Interviews were limited to one hour durations for three reasons. First, limiting the interviews to one-hour durations ensured that the data was collected in manageable amounts and thereby making tasks such as transcription from digital recording to text similarly manageable. Second, limiting the interviews to one-hour durations helped to manage the fatigue of both the interviewee and myself as the interviewer. Finally, because the interview subjects were taking time out of their normal workday, they had limited time with which to give me access. Interviews of longer duration would have likely resulted in a greater limitation of access.

Once initial analysis was complete of the first round of interviews (three for ARJIS, four for JNET), a second interview guide was created (see Appendix A for more detail) and a second round of interviews was conducted with the key informants in each case. These interviews were designed to confirm the initial analysis. In the interviews informants were read a statement of the IJIS identity that had been derived from the analysis and asked to rate the degree to which they felt that identity attribute described their IJIS using a five-point Likert scale. Informants were then given a chance to elaborate on their answer and to provide examples of how they saw that attribute reflected in the organizational practices and technical designs of the IJIS.

**ARJIS**

In the initial meeting the top manager identified two other key informants: the IT project manager and the lead project developer. She felt that these two informants would be able to offer the most insight into ARJIS as they were the staff members most connected to the organizational workings of ARJIS and the design of the ARJIS IT infrastructure. Both
informants had been at ARJIS for an extended period and were highly knowledgeable of ARJIS’ history and its organizational dynamics. Additionally, both informants were active in the design, use, and support of ARJIS technologies. One of the informants, the lead developer, was actually a contracted employee (in other words he is not paid by ARJIS), but for all intents and purposes he is considered to be a member of the ARJIS organization. His sole office is in the ARJIS office complex. He reports to the chief executive of ARJIS. He works for ARJIS exclusively; however he is not an employee of the city or state.

Three ARJIS employees were excluded from the interview process. Two were excluded because they serve administrative roles not involved in the design of ARJIS – one is the office administrative assistant and the other writes grant proposals. The third was excluded because at the time of data collection he had just begun his tenure at ARJIS and therefore was not in a position to provide insight into the ARJIS identity or design of the systems.

JNET

The top manager at JNET identified three key informants to speak with about JNET’s design and identity. These three informants were the lead project manager, the communications director, and the architectural manager. The top manager believed these informants would be good informants because they were the most connected to both the organizational and technological processes of JNET.

These three informants were particularly well-suited for this study as their organizational responsibilities represented the majority of organizational activities JNET is engaged in. The architectural manager’s responsibilities are to oversee the management of information systems.

---

28 During the interview of another member of the ARJIS organization, when asked about this member, the subject stated “He’s paid by someone else, but he’s part of ARJIS.”
development and design. The communications director oversees communications with the user community, JNET stakeholders, and participating agencies. The lead project manager’s responsibilities are to manage and oversee ongoing development projects at JNET.

Two of the three informants (the communications director and lead project manager) came to JNET initially as contractors before transitioning to full members of the JNET organization. The third informant came to JNET from another position within the Commonwealth government.

**A note about the number of interviews**

The number of subjects interviewed, and the number of interviews conducted in both cases is a relatively small number. However, these numbers are appropriate to this research for three reasons. One, both organizations are very small organizations, consisting of only a few full-time organizational members. For example, at the time of data collection ARJIS had five employees and so interviewing three informants represented 40% of the organizational membership (60% if the contracted developer is counted as a member of the organization – which the other organizational members do). Further, the informants interviewed represented 100% of those that could speak to the design of ARJIS technologies and the organizational processes related to ARJIS as an integrated criminal justice information system.

Similarly, JNET as an organization had only six full-time organizational members and relied on contracted employees for technical services. The interviewing of four employees represented 66% of the organizational membership and 80% of the organizational membership that could speak to the identity of JNET and technological design. In sum, the number of subjects interviewed was sufficient to obtain a broad representation of the organization with insight into the subjects of the interview.
Two, in both cases, I began to experience saturation of the data by the second interview. The second interviews offered minimal new theoretical insight, but provided clarification and evidences supporting the analysis of the first round of interviews I determined that the probative value of a third round of interviews was outweighed by the high associated costs of conducting the interviews for both me and the subjects.

Three, during the course of the ARJIS case study I experienced a reduction in the level of access to the site. Interviewees at ARJIS became increasingly difficult to reach and schedule for interviews. In some cases, an interview would be scheduled but the subject would fail to be available at the appointed time. Multiple efforts were made to address this challenge including phone calls, e-mails, and letters to the primary informant. Ultimately I decided to go with the data I had already collected, which was substantial, rather than force the issue of access and potentially poison the relationship with the subject permanently.

**Document Analysis**

Primary documents proved to be a significant source of data for both cases. For the ARJIS case study 281 documents (4,284 pages) were coded and analyzed. For the JNET case study 167 (4,285 pages) documents were coded and analyzed. In total, 448 documents totaling 9,313 pages were coded and analyzed for this research. I summarize the collection of documents analyzed in both cases in Table 1.

<table>
<thead>
<tr>
<th></th>
<th>ARJIS</th>
<th>JNET</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● Business and Wireless</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Design Documents</th>
<th>Governance Documents</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Network Diagrams</td>
<td>● ARJIS Joint Powers Agreement</td>
<td>● Consultant-produced organizational and technological assessments</td>
</tr>
<tr>
<td>● Entity-Relationship (ERD) Diagrams</td>
<td>● California Law Enforcement Telecommunication System (CLETS) regulations</td>
<td>● ARJIS public and private presentations</td>
</tr>
<tr>
<td>● Data Dictionaries</td>
<td></td>
<td>● The ARJIS public website</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Network diagrams</td>
<td>● JNET Management Directive</td>
<td>● Presentations given at the JNET Quarterly Integration Meeting by JNET and member agencies.</td>
</tr>
<tr>
<td>● Interface design layouts</td>
<td>● JNET Executive Order</td>
<td>● JNET public and private presentations.</td>
</tr>
<tr>
<td>● Project selection scoring matrix</td>
<td></td>
<td>● JNET public website.</td>
</tr>
</tbody>
</table>

**Table 6-2 Detailed breakdown of documentary evidence.**

**Direct Observation**

I used direct observation to buttress my understanding of JNET as an organization.

Because I had already engaged in extensive direct observation of the ARJIS system as part of prior research, I felt that my understanding of the organizational dynamics of ARJIS was sufficient for this research. However, JNET remained largely unfamiliar and therefore it was critical to observe the JNET organization *in situ* in order to understand the JNET design processes.

<table>
<thead>
<tr>
<th>Observed Event</th>
<th>Number Observed</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff Meetings</td>
<td>2</td>
<td>2 hours</td>
</tr>
<tr>
<td>Steering Committee Meetings</td>
<td>2</td>
<td>4 hours</td>
</tr>
<tr>
<td>Quarterly User Meetings</td>
<td>2</td>
<td>28 hours</td>
</tr>
</tbody>
</table>

**Table 6-3 Detailed breakdown of direct observations.**

As part of my JNET case study, I was able to attend JNET organizational meetings in order to gain better insight into how JNET engages in design at an organizational level and to how JNET is governed. I attended two JNET staff meetings. JNET staff meetings are run by the
Executive Director. At JNET staff meetings, project status updates are provided, resources are allocated, and key technological and organizational issues related to JNET technologies are discussed. I also attended two JNET Steering Committee meetings. The Steering Committee meetings were useful because they provided insight into how JNET is influenced and responsive to the various institutions that govern its operations. Finally, I attended two Quarterly Users Meetings. These meetings are where users are updated on JNET’s status in terms of issues, new services being deployed, costs of service, and communicate their feedback to JNET in general sessions and working group sessions. Attending and observing the Quarterly Users Group meeting was particularly useful because it allowed first hand insight into how JNET presents itself to its external stakeholders. In total, I was able to engage in over 30 hours of direct observation at these meetings. At all the meetings, I was able to take detailed notes which were then digitally transcribed.

Secondary Data

There were two components of the secondary data analysis. First was the reading and analysis of articles related to ARJIS, JNET, and IJIS in the popular, trade, and academic press. The purpose of this component was to familiarize myself with what was to become informed about ARJIS and JNET and to stay abreast of current practices and outcomes in IJIS development in general. This proved particularly useful for the ARJIS case study as Mitretek published a detailed summary of the ARJIS system in 2006 as part of NIJ-funded project (Mitretek, 2006).

The second component was the use of statistical demographic data to obtain facts and figures about the regions ARJIS and JNET operate in, and in the case of ARJIS, the agencies that participate in the system. In particular, I made extensive use of the Bureau of Justice Statistics’
Law Enforcement Management Statistics (Bureau of Justice Statistics, 2007) and Census of State and Local Law Enforcement Agencies (Bureau of Justice Statistics, 2003). These statistical databases capture data demographic information of both law enforcement agencies and the communities they serve and are an excellent resource for gathering key facts about IJIS.

Analysis of Data

In order to maintain conceptual and analytical clarity I chose to analyze the collected data for each case in five phases (See Figure 5). The first phase consisted of analyzing and synthesizing the available secondary data to generate an initial understanding of the ARJIS and JNET systems and the institutional environment they resided within.

The second phase consisted of coding the first round of interviews, primary documents, and field notes using a set of high-level *a priori* codes derived from the theoretical framework of this research. In total there were five *a priori* codes employed: three empirical and two theoretical. Three of the codes empirically described the data in terms of dimensions of the IJIS:

- Organization: organizational details, features, structures, design practices, and processes.
- Technology: organizational technology, functionalities, features.
- Governance: relating to the governance of the IJIS.

The remaining two codes – organizational identity and boundary spanning – linked the data at an abstract level to one (and occasionally both) of the theoretical frames.

There were three purposes for engaging in this phase. One, by coding the data in this manner I was able to organize the data both theoretically and empirically. Two, the initial coding transformed the data from a single anomalous pile to a set of ordered piles thereby facilitating later more detailed data analysis. Three, coding the data in this manner provided a
foundation for exposing relationships and patterns within the data and for linking identity and boundary spanning to features of the IJIS.

![Figure 6-1 Analytical process.](image)

In the third phase I inductively coded for specific organizational identity attributes. For both cases I coded the initial round of interviews to generate a set of identity statements about the IJIS using in vivo language. I then grouped these codes based on conceptual similarity, occasionally combining codes when there was a high degree of overlap and little discriminatory power was gained from keeping the codes separates.

The fourth phase consisted of coding the interview transcripts and primary documents for types of boundary objects, the social worlds they spanned, and the flow of information. The types of boundary object codes were derived from the literature. Codes for social worlds and flows of information were inductively generated. As with phase four, codes were then
categorized and codes having a high degree of overlap were combined and redundant codes were eliminated.

The sixth phase consisted of coding the second-round interviews and the identification of the links and relationships between the statements of organizational identity and examples of boundary objects with the three features of the IJIS I coded for in Phase 2. Two examples illustrate the latter process.

A core element of the ARJIS identity to emerge from the data was center for regional collaboration. I therefore created the code collaboration and assigned it to examples of collaborative activity or statements espousing collaborative action within the text of the interviews and documents. The following is an example of a statement that received the code ‘collaboration’ from minutes of an ARJIS Management Meeting:

*Over the next two months, crime analysts, investigations, patrol, and administration will be surveyed regarding requirements gathering and needs assessments for Enterprise ARJIS. It is critical that the system meet user needs and be designed from the ground up.*

Here ARJIS management is stating that they will approach design collaboratively, bringing in all types of users to formulate the design requirements for their Enterprise ARJIS application.
A second example comes from JNET. Because I wanted to understand how JNET functioned as a boundary object, I coded examples of the data of JNET acting in a boundary-spanning capacity. Then, I went through and coded each item coded-boundary spanning with codes for the any of the boundary objects that applied (e.g., indexed, modular). For example, I coded JNET’s notifications application as ‘boundary spanning’ because it is an application that JNET provides to users across agency boundaries with real-time notifications of changes to data. I then coded the application ‘autonomous’ because users employ the system independently, ‘common referent’ because the purpose of the system is to connect users through an interest in common data, and ‘different internal content’ because the displayed data is customized to each notification. The combination of these codes led me to draw the conclusion that the notification system had the properties of a terrain with coincident boundaries object.

**Analytic Induction**

The process of analytic induction consists of forming a general hypothesis, comparing the hypothesis to the empirical data, and then revising the original hypothesis to account for any
discrepancies between the original hypothesis and the facts of the case. Prior to starting the first case I formulated two general hypotheses. One, that organizational identity shaped the design of IJIS organizational and technological architectures. Two, that IJIS acted as boundary objects among different groups of individuals.

I then proceeded to collect and analyze data on the first case. Based on my analyses I revised my original hypotheses to account for new facts. In both cases the hypotheses became more specific. I now hypothesized that organizational identity shapes IJIS technological and organizational architectures through governance, design, and organizational practices; and differences in these practices among different IJIS would be reflected in different organizational and technological outcomes. For my second hypotheses, I now hypothesized that IJIS not only acted as boundary objects among different user groups, but among different organizations and different institutions.

Once the hypotheses were revised, I then proceeded with the second case. Following data collection and analysis, I then revised my hypotheses a second time to account for new facts. These new revisions are the findings I present in the next two chapters.

**Conclusion**

In this chapter I have summarized the data collected and the analytical methods used in the conducting of the ARJIS and JNET case studies, and the use of analytic induction for within-case and cross-case comparison. Though there were some challenges posed by limited access, the quantity and quality of the data is substantial. I used a hybrid *a priori* / inductive coding scheme to organize the data and to identify links between organizational identity, design practices, and design outcomes. I relied on multiple analytical methods and multiple types of
data to increase the validity of the findings. In the following two chapters I present my empirical findings.
Chapter 7 – Case Study: Automated Regional Justice Information System (ARJIS)

Introduction

In this chapter I describe the Automated Regional Justice Information System (ARJIS). I start with the origins of ARJIS as an IJIS. I then describe ARJIS as an organization focusing on ARJIS’ organizational structures and governance processes. The third and final section of this chapter deals with ARJIS technical architecture. ARJIS’ hardware, software, networking, architecture and security are described in detail.

What is ARJIS?

The Automated Regional Justice Information System is a regional-level IJIS in the San Diego county metropolitan region in the state of California. Initially only a mainframe system operated by a single agency, ARJIS now is one of the most established, advanced, and complex IJIS in the United States incorporating eighty member and ex-officio agencies and providing access to eleven separate information systems.

Origination of ARJIS

The ARJIS system originated in the early 1970’s through funding from a U.S. Department of Justice grant. The ARJIS system began as an IBM mainframe database funded by the U.S. Government and developed by the San Diego Police Department (SDPD). Technologically, ARJIS’ early history was primarily as a records management system for the SDPD. In the late 1970’s a move was made to make ARJIS more of a regional asset to the various law enforcement agencies operating in the broader San Diego metropolitan region.

In 1980 an initial arrangement, called a Joint Powers Agreement (JPA), was formed to add an organizational component to the ARJIS mainframe system (Mitretek, 2006). A JPA is a contract between entities in which the signatory parties agree to share services and power as
outlined in the agreement. Analysis of the ARJIS JPA shows that it established the core governance and organizational structures of ARJIS and provided the organizational foundation upon which ARJIS would develop into the IJIS it is today. In particular, two governance mechanisms were established that were critical to ARJIS development as an IJIS.

One, the JPA established a funding mechanism through which each member agency contributed dues to the operation of ARJIS. The amount of dues each member agency is responsible for is proportional to their size. Smaller agencies contribute less while larger agencies contribute more. In establishing this funding mechanism the JPA had three key effects.

First, the establishment of member funding the JPA created a path to long-term sustainability by freeing the ARJIS organization from having to depend on grants for sustainability. ARJIS does continue to seek and employ grants as tools to enhance and expand the existing system but it is not reliant upon grants to remain operational. Second, by assigning member obligations proportionally, the JPA facilitates encouraged participation among smaller agencies by allowing them to stay within their fiscal limitations while also allowing the larger agencies to offload some of the cost of operating ARJIS to their partners. Third, by establishing a dependence on the member agencies for funding, the JPA also has the implicit effect of ensuring that ARJIS designers attempt provide a return on investment for the member agencies by designing and implementing functionality the member agencies need.

The second mechanism the JPA established was governance. Specifically, the JPA established that each member agency would have equal standing in the governing of ARJIS.

---

29 ARJIS ability to not have to rely on grant funding to maintain sustainability has been placed in some doubt in the summer of 2009 when the SDPD informed ARJIS management their membership dues will not be paid this year. At the time of writing this issue was still unresolved, and so as of this date, ARJIS still does not rely on grant funding to operate.
Each member agency appoints a single representative – usually the chief executive of that agency – to the top-level governing committee (initially termed the Management Committee). As with the funding mechanism distributing governing authority equally among member agencies has had a critical effect on the ARJIS organization.

Distributing power equally across the member agencies prevented, and continues to prevent, the larger agencies from dominating the ARJIS organization and agenda. With a proportional funding model, a reasonable expectation is that the agencies that contribute the most dollars to the funding of ARJIS (the two largest member agencies) would exercise the most influence over ARJIS. Such an outcome would clearly have a negative impact on the level of collaboration among the member agencies as the smaller agencies simply would not have the influence to have much effect on ARJIS as a system.

Instead what has happened is that by distributing authority equally across member agencies; the design and governance of ARJIS has become an exercise in consensus building and collaboration. While the larger agencies can exercise at least indirectly, greater influence on the design of ARJIS, no one agency can attempt to impose its will on ARJIS. Further, because smaller agencies have a stake in the governance of ARJIS they are incentivized to continue participating. As will be shown, this distribution of power has played a major role in maintaining ARJIS sustainability.

In 2004 the JPA was revised and ARJIS was consolidated into the San Diego Association of Governments (SANDAG): a regional government planning agency (Gallegos, 2003; Mitretek, 2006). For the most part the incorporation of ARJIS into SANDAG gave ARJIS the ability to capitalize on the administrative expertise and infrastructure that existed at SANDAG.
The Executive Director revealed during interviews that the most significant change brought about by the consolidation with SANDAG was primarily to give ARJIS access to SANDAG administrative capabilities, and the revision of the JPA was to expand and rename the ARJIS Board of Directors. The Board of Directors was renamed to Public Safety Policy Advisory Committee (PSPAC) to more appropriately reflect the mission of ARJIS within the SANDAG organizational structure. The membership of the PSPAC was expanded to include public elected officials from each of the four sub-regions of San Diego County, the county, and the city governments. The PSC retained oversight of ARJIS through SANDAG.

The ARJIS Organization

Organizational Structure

The ARJIS organizational structure consists of a hierarchy of committees organized around a business process loop and a technical process loop. At the top of the hierarchy is the SANDAG Public Safety Policy Advisory Committee (PSPAC) a committee comprised of senior public administrators and elected officials. The PSPAC serves two primary functions. The PSPAC retains all powers afforded the ARJIS organization, but its primary function is to serve in an advisory capacity.
The second level of the ARJIS organizational hierarchy is the Chiefs Management Committee which is comprised of the chief executives of all the ARJIS member agencies. The Management Committee is where de facto operational control of ARJIS resides. The Management Committee effectively renders the final decisions on organizational and technical questions for ARJIS. The Management Committee also can delegate proposed changes to the ARJIS system to the lower committees to evaluate and propose action.

There are three committees (which they call working groups) that make up the lowest level of the ARJIS hierarchy. They are the Business Working Group, the Technical Working Group, and the Analyst Working Group. Each working group is populated by representatives from all the member agencies. The chair of each working group rotates among the member agencies. Additionally the Executive Director of ARJIS sits on all three committees serving primarily in a reporting, advisory, and facilitating capacity.
The Business Working Group is responsible for evaluating proposed changes to ARJIS for alignment with ARJIS strategic business goals. The Business Working Group also addresses and legal, ethical, or regulatory issues attached to any proposed design change. Working in parallel with the Business Working Group, the Technical Working Group evaluates proposed changes to the ARJIS technical architecture from a technological standpoint and reports the results of their analysis to the Business Committee. Together these two working groups continually produce a set of recommended additions or changes to the ARJIS system for the Management Committee to attach their final approval.

The ARJIS Analysts Working Group handles the management of ARJIS data standards. This working group resolves issues related to the ARJIS database, in particular the establishment of new data codes and the enforcement of compliance with the data dictionary by member agencies. A typical task of the Analysts Working Group is to review and to either accept, reject, or modify a proposed change to the data dictionary. For example, a member agency may propose revising a code for ethnicity (e.g., ‘Asian’) to be more precise (e.g., Pilipino, Korean, Japanese, Chinese, Thai, etc.). As will be shown in the next chapter, the enforcement of compliance is one of the highly collaborative aspects of ARJIS governance.

The ARJIS management team is a part of the SANDAG Technical Services division. Headed by an Executive Director the ARJIS management team serves three primary roles. One, the ARJIS management team serves as advocates for ARJIS to both internal and external stakeholders. Two, ARJIS management provides both technological and organizational guidance to the business and technical decision making processes occurring in the committees. Three, ARJIS management acts an honest broker among the various member agencies, maintaining member buy-in, resolving disputes and coordinating activity.
ARJIS Governance

The JPA is at the core of ARJIS governance as it determines criteria for membership, basis for participation, and how ARJIS will be funded. Full membership is limited to agencies within San Diego County. All of the member agencies are law enforcement agencies which clearly represents the law enforcement focus of ARJIS. As stated before, each member agency gets a single vote. However, there is mechanism for conducting a weighted vote where large agencies carry more voting weight though it is rarely used.

Analysis of financial data\(^{30}\) contained in Management Committee Meeting minutes shows that ARJIS is funded primarily by the fees assessed member agencies, member-affiliated agencies, and ex-officio member agencies. Member agencies contribute the largest portion of the fees to operate ARJIS; paying in 8 times as much as member-affiliated agencies, and 10 times as much as ex-officio agencies. The member agencies are assessed fees to fund ARJIS proportionally based on the size of the population they serve. The largest two agencies – San Diego Police Department (SDPD) and San Diego Sheriff’s Department (SDSD) – are the primary funding sources for ARJIS; contributing approximately 77\% of all member-assessed fees. The annual budget of ARJIS has averaged $6.8 million and has grown at an average rate of 17.5\%.

<table>
<thead>
<tr>
<th></th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARJIS Budget</td>
<td>$4,862,202</td>
<td>$4,039,802</td>
<td>$5,969,249</td>
<td>$7,496,706</td>
<td>$8,310,806</td>
<td>$9,983,811</td>
<td>$40,662,576</td>
</tr>
<tr>
<td>Salaries &amp; Benefits</td>
<td>$188,853</td>
<td>$256,680</td>
<td>$323,995</td>
<td>$656,848</td>
<td>$806,232</td>
<td>$1,153,100</td>
<td>$3,405,712</td>
</tr>
<tr>
<td>Direct Costs</td>
<td>$137,149</td>
<td>$197,000</td>
<td>$628,677</td>
<td>$231,362</td>
<td>$250,996</td>
<td>$699,225</td>
<td>$2,144,409</td>
</tr>
<tr>
<td>Contract Employees</td>
<td>$598,200</td>
<td>$563,210</td>
<td>$998,487</td>
<td>$642,922</td>
<td>$615,020</td>
<td>$0</td>
<td>$3,417,839</td>
</tr>
<tr>
<td>Contract Services</td>
<td>$1,586,000</td>
<td>$1,022,912</td>
<td>$3,798,710</td>
<td>$4,629,386</td>
<td>$5,713,829</td>
<td>$7,927,492</td>
<td>$26,678,329</td>
</tr>
<tr>
<td>Materials &amp; Equipment</td>
<td>$2,318,000</td>
<td>$50</td>
<td>$219,376</td>
<td>$1,336,188</td>
<td>$904,729</td>
<td>$263,793</td>
<td>$5,042,086</td>
</tr>
<tr>
<td></td>
<td>$9,692,409</td>
<td>$8,081,610</td>
<td>$11,940,505</td>
<td>$14,995,420</td>
<td>$16,623,621</td>
<td>$20,029,431</td>
<td>$81,350,951</td>
</tr>
</tbody>
</table>

\(^{30}\) Management Committee Meeting Minutes 3/6/05, 3/1/06, 4/4/07, 4/2/08, 5/6/09

Figure 7-2 ARJIS operating budget 2005-2010
Many individual projects are funded by grant monies from federal agencies such as the Department of Homeland Security (DHS), the National Science Foundation (NSF) and the National Institute of Justice (NIJ). For example, DHS has funded Project Bordersafe through which ARJIS provided mobile access via handheld devices; as well as the State, Regional, Federal Enterprise Retrieval System (SRFERS) a project to integrate systems in western states, and the NIJ has funded a pilot project comparing COPLINK to existing crime analysis tools.

**Figure 7-3 ARJIS project budget 2005-2010.**

In terms of annual outlays, the majority of ARJIS budget outlays are towards ongoing maintenance and support of the ARJIS mainframe (37%) and projects (39%). These outlays primarily go to contracted services – hosting and support for the mainframe, contracted application programming, etc. Since 2007 the expenditures on maintenance and support have remained relatively steady, while expenditures on management and enhancements have declined, and expenditures on projects have risen sharply.
Membership in ARJIS is determined through a committee vote in which only member agencies are allowed to participate. Ex-officio agencies and member-affiliated agencies are allowed to participate in ARJIS governance meetings, but retain no voting power or other ability to effect ARJIS operational decisions.

The ARJIS Technical Architecture

Hardware

ARJIS technical schemata and presentations show that the centerpiece of the ARJIS technical architecture is an IBM mainframe. This mainframe is COBOL based and contains two high-availability disk drives totaling approximately 580 gigabytes of disk space. The ARJIS database grows at a rate of approximately ten percent per year due to retention of records, the addition of new transaction and data types (as mentioned in the discussion of the Analysts

---

Working Group), and report entries from participating agencies. Records from the database are purged based on age.

The mainframe is operated and maintained by the San Diego Data Processing Corporation – a public non-profit organization that handles most of the government IT for San Diego County\textsuperscript{33}. The cost of operating and maintaining the mainframe is increasingly expensive as hardware and programming expertise become scarce. As noted above, almost 40% of ARJIS’ annual expenditures are towards maintenance of the ARJIS mainframe database. The estimated cost of upgrading the mainframe in 1996 was estimated at approximately $17.1 million\textsuperscript{34}. The legacy mainframe is augmented by Windows NT servers that run middleware and front-end applications. The cost prohibitive nature of continuing to operate this legacy system is a key factor in ARJIS development efforts. Specifically, ARJIS management’s long term strategic goal is to develop the infrastructure and applications to eventually move off the ARJIS mainframe completely.

\textsuperscript{33} See http://www.sddpc.org/
\textsuperscript{34} Report prepared for ARJIS Management by Garner Consulting (1999)
For all intents and purposes, ARJIS does not employ client hardware. Instead the ARJIS applications are piggybacked onto existing client hardware (such as MDTs, MCTs, laptop computers) owned and operated by the participating agencies. The exception is wireless devices. ARJIS provides wireless devices to clients for use in accessing the ARJIS wireless application. Originally ARJIS used Compaq iPAQ Pocket PCs but found that the devices delivered unacceptable performance. The iPAQs had poor battery life, connectivity, and usability. Since that time ARJIS has employed multiple types of PDAs and now currently has three different types in the field: the Palm Treo 700w, the Verizon XV 6700 and XV6800.

Software

A review of ARJIS technical documentation reveals that ARJIS’ primary application is its Global Query 2 application. Initially deployed in 2003, Global Query 2 is a federated query...
(a single query of many databases) of multiple back-end databases including the legacy ARJIS mainframe (see Appendix C for a detailed list of ARJIS applications). The Global Query application accesses over 63 databases at all levels of government. The major systems that Global Query is attached to include booking photos, Department of Motor Vehicles drivers’ records, court information, wants and warrants, wanted persons, local incidents, and federal crime info. A user connects to the Global Query 2 application through a firewall and queries a name.

The Global Query 2 application then queries each of the attached systems and returns results aggregated by individual name. For example, an officer queries “John Doe” and all matching records from all the attached systems are aggregated under the name John Doe. The benefit to the user is that she only has to enter information once in order to search all of the available systems and the returned data is organized by suspect name rather than by system making the results much easier to read and interpret.

To able to connect to so many heterogeneous systems ARJIS designers chose to employ a middleware solution. Middleware applications facilitate connectivity among other applications. ARJIS uses IBM’s Websphere MQ middleware. MQ Series middleware allows the global query app to connect to multiple heterogeneous systems by acting as a messaging bridge between the Global Query application and the back-end servers. MQ Series middleware supports both single-to-many and many-to-single connections, and ARJIS employs the software in order to provide a single point of entry to multiple data sources.

In addition to Global Query, ARJIS provides numerous other applications. ARJIS acts as an agency-specific records management system (RMS) that includes such features as document
and evidence management, case management, FBI mandatory reporting functionality, and laboratory analysis. ARJIS provides officer notification service (ONS), a system by which officers are notified when flagged data that is relevant to them is queried by other users. Finally, ARJIS provides a host of regional applications such as COPLINK, crime mapping, crime analysis, data mining, crime statistics, crime link analysis, and offender notification.

ARJIS also provides applications to the public that access a limited set of ARJIS data. These applications are accessible through the public website. The two applications that ARJIS provides that directly access ARJIS data are crime statistics and crime maps. The crime statistics application allows users to query data about crimes committed in the San Diego region for a given time period. Once the results are retrieved, users can graph individual crimes in order to see how the rate for the specific crime breaks down per month. The crime map application is much more robust. After reading a page describing the application in detail as well as providing relevant disclaimers, users can map crimes based on location, time period, and type of incident. A map is generated based on the selected criteria and users can then navigate around the map, click on a particular incident to see its details, and print out a PDF of their map.

ARJIS most significant software development project currently is the development and eventual deployment of Enterprise ARJIS. The Enterprise ARJIS project is intended to be the system that replaces the ARJIS mainframe as the core ARJIS system. The Enterprise ARJIS project is expected to cost between twelve and twenty million dollars to complete. Enterprise ARJIS is currently in development and ARJIS management is expected to deploy the application sometime in 2009.
Networking

ARJIS employs a mixed network infrastructure to deliver connectivity and access. Most devices connect to ARJIS over System Network Architecture (SNA) protocols using Ethernet, Fast Ethernet, Token Ring, and Peer-to-Peer leased lines. The use of SNA by ARJIS is unsurprising given that SNA is a protocol stack developed by IBM in the 70s and can be commonly found in the financial industry and the government sector (Gilbert, 1995). Many of the member agencies participating in ARJIS have moved to Wide Area Networks (WANs) in recent years. The SDDPC provides a WAN to the region called SANNET. Standard TCP/IP protocol is used for the ARJIS Intranet.

---

37 Presentation given to Public Safety Committee 5/19/2006


**Architecture**

Network diagrams display the routing of ARJIS traffic through two main paths. One path routes traffic to the ARJIS legacy database (RMS), Automated Field Reports (AFR), and external systems such as the California Law Enforcement Telecommunication System (CLETS), the Joint Terrorism Task Force (JTTF) system, the National Crime Information Center (NCIC), and Department of Justice systems through a data distribution center (DDC). The DDC manages queries, validates distribution rules, and links to state and federal applications and data. The second path routes traffic through a data warehouse where regional applications and validation standards are housed. Users of ARJIS connect to the DDC and the data warehouse via the ARJIS interface using a local client desktop, a mobile computer, or a handheld device.

**Security**

Security of information and access is a critical component of the ARJIS system. The ARJIS security center has been designed to be the cornerstone of the entire suite of ARJIS applications and was the first major component of the modern ARJIS. The ARJIS security center is an enterprise-distributed application that makes use of the Lightweight Directory Access Protocol (LDAP). Like the use of MQ Series middleware, the use of LDAP allows ARJIS designers to implement a security scheme that can interface with multiple heterogeneous systems. The design of the security center allows ARJIS to employ a single-sign-on mode of authentication greatly reducing the burden of authentication for the users. Users only have to remember a single set of credentials and only have to authenticate a single time to access all of the ARJIS features.

**Conclusion**

This chapter has presented a detailed description of ARJIS as an organization and as a technological architecture. Key to the ARJIS organizational structure is the Joint Powers
Agreement which established a funding model and governance model that facilitates sustainability and participation. The technological architecture is highly complex, built around an aging legacy mainframe but migrating towards more modern technologies. ARJIS primary application, Global Query, allows ARJIS users to query multiple heterogeneous databases with a single query and receive the aggregated results in one application. This single-to-many design rationale permeates both the ARJIS network infrastructure and the security design.
Chapter 8 Case Study: Pennsylvania Justice Network (JNET)

Introduction

In this chapter I describe the JNET integrated criminal justice information system. JNET is an IJIS that serves all levels of government within the Commonwealth of Pennsylvania. From its origins in an executive order signed by then Governor Tom Ridge, JNET has grown to a massive system serving 34,000 users and providing access to 19 different data sources. JNET has been recognized repeatedly as an exemplar of IJIS, receiving numerous awards for achievement such as NASCIO’s 2008 Recognition Award for Data, Information, and Knowledge Management ("NASCIO Recognizes 10 State IT Initiatives for Outstanding Achievement," 2008).

Origination of JNET

Two aspects of Governor Tom Ridge’s first term in office provided the impetus for the creation of JNET. One was the 1994 Improve Management and Cost Control Task Force (IMPACCT) charged with findings ways for the Commonwealth government to operate more efficiently and save fiscal resources (IMPACCT, 1996). IMPACCT produced over 400 recommendations including a reexamination of policies prohibiting inter-agency information sharing, increasing the operational efficiency of the state police, consolidating the state’s responsibility of drug enforcement, and privatizing prisons and reflected an overall policy goal of increased efficiency and reduced operating costs for the government (Sawyer, Hinnant, & Rizzuto, 2008). One outcome of IMPACCT was the Office of Information Technology (OIT), an executive branch agency, was made the location for strategic information technology planning and governance.
A second aspect of Governor Tom Ridge’s first administration was a political focus on crime in the Commonwealth of Pennsylvania. One action taken by Governor Ridge was to call for a special session of the General Assembly which ultimately produced 34 signed pieces of legislation related to criminal justice, the judicial system, victims’ rights, and law enforcement (States News Service, 1995a, 1995b, 1995c). In combination, the administration’s emphasis on the control and prevention of crime, and in generating more efficiency from the Commonwealth’s use of IT created the institutional environment from which JNET emerged.

The next step in the creation of JNET was the Integrated Justice Project. The Office of Administration – a cabinet-level office – launched the Integrated Justice Project in 1996 through its OIT (Rendell, 2003). The goal of the Integrated Justice Project was to develop a strategic vision for information exchange between justice and justice affiliated agencies. The strategic vision that emerged from the Integrated Justice Project served as the basis for JNET. JNET was to help the Pennsylvania criminal justice system “solve cases faster, apprehend and identify suspects, and to lead to reduced costs with criminal justice information processing.”
JNET formally began as a project in 1997 with the formation of the Steering Committee by the Governor’s office. The Steering Committee developed the initial blueprint for JNET’s governance structure and mission. In 1999 JNET was officially established as an agency in Governor Ed Rendell’s Executive Order 1999-4. Executive Order 1999-4 formally created the JNET governance structure to include the JNET Executive Council, the JNET Steering Committee, and the JNET Office. In addition to establishing these governance bodies, the executive order defined the mission of the governance structures, the list of participants, some of the responsibilities of the JNET Executive Director, and the physical location of the JNET Office.
Office. More will be discussed about the details of these governance bodies and their roles later in this chapter.

Since its inception as an IJIS, JNET has experienced a high rate of growth both in terms of functionality and number of users. Documents provided by JNET management show that the JNET system has grown from a single system (the JNET messaging infrastructure) to a system that provides access to nineteen different systems. At the same time, the JNET user base has grown from 100 users in 1999 to over 35,000 individual users in 2009. The JNET system is connected to all 67 counties in Pennsylvania, 750 municipal police departments, 54 state agencies, and 42 federal agencies.

Figure 8-2 Growth of JNET user base over time.
The JNET Organization

Organizational Structure

The organizational structure of JNET is four-tiered. The top tier is the Executive Council. This council is comprised of chief executive officers from Commonwealth criminal justice and information technology agencies and is chaired by an appointee of the Governor. The Executive Council serves in the role of a board of directors; it meets biannually for the purposes of setting overall policy for JNET and providing a strategic vision. Providing strategic vision includes the setting of budget priorities and proposing JNET’s overall annual budget; ensuring JNET’s actions are consistent with Commonwealth plans established by the Governor; and giving final approval to the JNET project plan developed by the JNET Executive Director with input from the Steering Committee.

![Figure 8-3 The JNET governance structure](image)

The Steering Committee is the second tier of the JNET organizational structure. The Steering Committee is comprised of mid-level representatives from many of the state agencies.

---

39 Source: JNET Overview Presentation
that sit on the Executive committee with one exception: there is less representation of the Governor’s office. The chair of the Steering Committee is appointed by the Executive Council and the Office of Administration. Meeting on an as needed basis, on a broad level the Steering Committee establishes the tactical (operational) plan for the deployment of JNET functionality and establishes JNET system and information system requirements. What this means is that the JNET Steering Committee directs the development and implementation of JNET systems; ensures compliance with Executive Council directives; sets policy, performance standards, and delivery dates; and ensures JNET compliance with statutory requirements and standards set by the Governor’s office.

The third tier of JNET’s organizational structure is comprised of the JNET Agency Advisory Subcommittee (JAAS) that is charged with analyzing specific issues and making recommendations to the Steering Committee, the Senior Policy Team which is an oversight team charged with monitoring overall JNET Project compliance with established statewide policy, budget, and information technology standards and initiatives, and the Office of Information Technology which provides organizational oversight.

<table>
<thead>
<tr>
<th>JNET Executive Council</th>
<th>JNET Steering Committee</th>
<th>JNET Senior Policy Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Governor</td>
<td>Office of the Governor</td>
<td>Governor’s Office of Administration</td>
</tr>
<tr>
<td>Juvenile Court Judges Commission</td>
<td>Office of Information Technology</td>
<td>Office of the Budget</td>
</tr>
<tr>
<td>Department of Corrections</td>
<td>Administrative Office of the Courts</td>
<td>Governor’s Policy Office</td>
</tr>
<tr>
<td>Department of Transportation</td>
<td>Department of Corrections</td>
<td>Governor’s Office of General Counsel</td>
</tr>
<tr>
<td>Board of Pardons</td>
<td>Department of Public Welfare</td>
<td>JNET</td>
</tr>
<tr>
<td>PA Board of Probation and Parole</td>
<td>Department of Transportation</td>
<td></td>
</tr>
<tr>
<td>Office of the Budget</td>
<td>PA Board of Probation and Parole</td>
<td></td>
</tr>
</tbody>
</table>

40 The meeting frequency of the Steering Committee is significant and will be shown to be emblematic of the overall evolution in JNET’s organizational identity.
The JNET Agency Advisory Subcommittee employs work groups and action teams comprised of representatives from the JNET Office and from individual agencies who are involved with a particular issue. For example, JAAS formed a work group to study the prospects of implementing a system that tracks pre-sentencing information. The work group was comprised of a representative from JNET, representatives from the Pennsylvania Board of Probation and Parole, and a county representative. The work group report was then presented at the Steering Committee for consideration and action.

The Senior Policy Team is comprised of Deputy Secretary for Budget, the Deputy Secretary for Information Technology, the Governor's Policy Office Director, a designated Deputy Counsel from the Office of General Counsel, the Executive Director of the JNET Office, and the JNET Steering Committee Chairperson. The role of the Senior Policy Team is to provide guidance about legal or policy issues as they pertain to JNET activity and to ensure that JNET’s operational and strategic plans align with that of the governor’s administration.
The bottom level of the JNET organizational structure is the office level headed by JNET’s Executive Director. The Executive Director is the senior manager within the JNET organization and maintains control of JNET’s daily operations. In this role, the JNET’s Executive Director oversees the managing of Commonwealth employees working in JNET, contractors, vendors, and service providers; implements policies established via the Executive Council and Steering Committee; develops an annual project plan consistent with directives from the Governor’s Office of Information Technology; as well as being responsible for compliance with security standards, developing outreach initiatives, and preparing the annual report.

In practice, JNET’s Executive Director is managing the development, maintenance, and growth of JNET. He (for so far only men have served in the role of Executive Director) assigns responsibilities among his senior management team; determines priorities and allocation of resources, and coordinates activities among vendors. Finally, the Executive Director acts as the primary public face of JNET; networking with other IJIS executives, receiving awards on JNET’s behalf, and pursuing funding opportunities such as federal grants.
Internal budget data shows funding for JNET as based on two sources: allocations in the annual Commonwealth budget and grants from funding agencies such as the NIJ and NASCIO. The total budget for JNET has averaged $11.3 million annually. Since 2001, JNET’s allocation from the state government has decreased from a high of $15.3 million to a low of $5.5 million for the 2008-2009 fiscal year. During the same period, JNET has received an average of $1.3 million in grant funding which also peaked in 2001 at $2.5 million and has since dropped to $566,355 for the 2008-2009 fiscal year. Over the ten-year period of JNET’s history, state funding has declined an average of 5.21% while grant funding has declined an average of 11.7%. Two effects of this long term pattern of decreased funding has been a transition from growth to stabilization of JNET as a technical system, and increased percentage of the organizational

Figure 8-4 JNET operating budget 1999-2009.
membership comprised of Commonwealth employees (which generally cost less than their counterparts in the private sector).

![Percent Change in JNET Funding by Year](image)

**Figure 8-5 JNET operating budget trends.**

**JNET Governance**

During interviews it was revealed that as an organization, JNET is governed primarily by two entities: the JNET Steering Committee and the Office of Information Technology (OIT). The JNET Steering Committee is the body most directly involved in the governance of JNET activities. It is to the Steering Committee that JNET’s Executive Director goes to receive guidance on exceptionally difficult operational decisions. The JNET Steering Committee must give its approval to any projects that the JNET management team proposes.
Today, the primary function of JNET Steering Committee meetings is to update members on the current status of JNET. JNET management attributes this to a general stabilization of JNET as an organization requiring less direct oversight from the committee. The reduced role of the Steering Committee in the daily management of JNET is reflected in the reduced frequency of meetings of the Steering Committee from a monthly meeting schedule to a bi-monthly and occasionally quarterly meeting schedule. Early in JNET’s history however this was not the case and the Steering Committee played a much more active role in shaping the daily operational activities of JNET.

The Office of Information Technology provides a different type of governance for JNET. Specifically the OIT functions as JNET’s parent organization within the executive branch of the Commonwealth government. The OIT established the standards, policies and procedures related to information technology services in the Commonwealth government that JNET must comply with. For example, as will be discussed in greater detail in the next chapter, the OIT periodically produces the *Keystone Plan* which establishes the Commonwealth’s strategic IT goals and to which JNET management must comply.

**The JNET Technical Architecture**

**Hardware**

The JNET architecture initially consisted of servers physically located in multiple counties throughout the Commonwealth of Pennsylvania connecting to the central office; but in an effort to reduce the costs of purchasing and supporting the hardware, JNET has converted to a virtual server platform that allows them to run all their application environments (development, test, production, and backup) on many fewer computers. Today the JNET hardware
infrastructure is comprised of Windows servers and IBM Datapower appliances. IBM Datapower appliances are purpose-built network devices used to accelerate web services within the system.

**Software**

Weblogic and Oracle webserver software provide the foundation for JNET’s software environment. JNET applications are browser-based and written primarily in the Java programming language and JavaServer Pages scripting language (see Appendix E for a detailed list of JNET applications). Additionally, JNET has some legacy applications that are written using Active Server Pages scripting language. Recently, some newer applications have been written using Microsoft’s .NET scripting language.

Two middleware suites are used by JNET to integrate the various system components. JNET’s enterprise portal application is built on Software AG’s webMethods application. The webMethods application is a Service Oriented Architecture (SOA)-based middleware application that allows JNET to connect to heterogeneous data sources and to make services available to multiple partners. Also used by JNET is IBM’s MQ-series middleware application in conjunction with Sun Microsystem’s Java Messaging Service (JMS) to run its messaging system.

The JNET system provides access to a suite of 25 applications (see Appendix D for more information) accessed through the main JNET application – the JNET enterprise portal. These applications serve various functions including connectivity, communication, search, statistical analysis, and informational (e.g., sentencing guidelines). The majority of these applications are interfaces provided by other agency systems that the JNET connects to (for example the
Pennsylvania State Police’s CLEAN system). The enterprise portal and the notifications application are the two most prominent internally developed applications JNET provides.

The notification system, more formally referred to as the JNET Messaging Infrastructure is based on the Java Messaging Service (JMS) specification, an application programming interface (API) that uses applications written in the Java programming language to handle the creation, sending, and receiving of messages. The JNET Messaging Infrastructure allows users and agencies to be notified when flagged data within the system is accessed or changed.

**Networking**

JNET’s network architecture is designed to facilitate connections from client devices and workstations to the appropriate back-end information systems via the JNET enterprise portal. Users connecting with a mobile device can either connect over the public safety wireless spectrum or through the Internet using a virtual private network client and a smart card (these two components provide security and are discussed in the next section). Workstation users connect to JNET primarily through points of access residing in county agencies – often Sheriff’s offices or County Jails – throughout Pennsylvania. The county local area network then connects to the JNET system which in turn routes the traffic through a series of frame relay switches to the appropriate back-end system. For example, an officer in a squad car needing driver’s license information connects to the county LAN through the MCT in the car which routes the request to the JNET system which then routes the request to the PennDOT system attached to JNET. The query is run and the results are returned via the same steps in reverse.
Security

Information security is applied to both the server-side and client-side of the JNET network. On the server-side, there are firewall applications running between the clients and the county local area network, the county local area network and the JNET network, and between the JNET network and the CLEAN system (PSP network). Client security consists of encryption and identity verification using Public Key Infrastructure (PKI) digital certificates. User digital certificates are stored on e-tokens (small hardware devices with the user’s credentials and digital certificate stored on them), and physical and virtual smart cards (similar to credit cards). These digital certificates are used to establish the user’s identity and create a secure virtual private network (VPN). The VPN is an encrypted connection from the client through the firewall to the back-end systems that prevents unauthorized access to the transmitted data.

---

41 (JNET, 2009)
Conclusion

In this chapter I have detailed the JNET integrated criminal justice information system. JNET is a commonwealth agency, established by executive order and governed by a powerful Steering Committee. As a system, JNET has grown substantially both in the systems it provides access to and the number of users who make use of JNET’s services. JNET’s growth and stabilization as an organization has resulted in a reduced role for the Steering Committee in the governance of JNET’s daily operations. At the same time however, JNET has seen a steady reduction in funding both from the Commonwealth and agencies providing grant funds which has forced JNET to minimize organizational costs in order to maintain development and growth.
Chapter 9 Collaboration vs. Brokerage: How organizational identity commitments shape IJIS design.

Introduction

In this chapter I describe the organizational identities of the ARJIS and JNET organizations. I then discuss in detail how the identities of ARJIS and JNET are reflected in both their organizational and technological designs. What this discussion will show is the differences in these two organizations in terms of both their organizational and technological components can be explained, in part, by the differences in their organizational identities.

ARJIS

Given that the ARJIS system has been in operation in varying forms since the late 1970’s is it unsurprising that there is a well-established organizational identity. The organizational identity of ARJIS has three main elements. One, members of the ARJIS organization view ARJIS as a center of regional collaboration where regional problems are addressed and solved. Two, members of the ARJIS organization see ARJIS as a service and technology provider to regional criminal justice agencies and the public. Three, members of the ARJIS organization perceive ARJIS as an aid to the regional criminal justice user community. A term that best describes these three components in combination is that of collaboratory. A collaboratory is a network form of organization built around shared ICT and process, modes of communication, norms, values, and regulations (Cogburn, 2001). This definition captures both the form of ARJIS as an organizational and technological ensemble and ARJIS’ emphasis on collaboration.

These three main elements of ARJIS’ organizational identity are reflected in the organizational design and practices of ARJIS, the ICT products ARJIS develops and integrates

---

42 Note: When referring to members of the ARJIS organization I refer to employees of ARJIS as distinguished from member agencies (agencies that participate in ARJIS) or employees of those member agencies.
into its ICT architecture, and the organizational artifacts ARJIS creates. ARJIS employs a governance structure that emphasizes collaborative decision making, representation of participating agencies, and achieving shared goals and outcomes. The ARJIS system has been built to serve as a central location for regional criminal justice data. New system components are collaboratively chosen and micro-level design detail decisions are often made between ARJIS developers and one or more member agency representatives. Finally the overriding design criteria employed by ARJIS is whether or not the feature, application, or information will help the end user engaged in policing activity.

<table>
<thead>
<tr>
<th>Element of Identity</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center for regional collaboration</td>
<td>Democratic decision making; equal representation; fostering relationships and working together to solve common goals; rooted in institutional culture of the region</td>
<td>Negotiation of data entities, definitions, and attributes among representatives from participating agencies to ensure standardization.</td>
</tr>
<tr>
<td>Provider and facilitator of regional criminal justice IT</td>
<td>Providing technology services to member agencies; connecting existing ICT infrastructures; collective representative of member agencies in contracting of services and procurement of equipment.</td>
<td>ARJIS negotiated the contract with Verizon on behalf of member agencies to provide wireless access to the ARJIS system.</td>
</tr>
<tr>
<td>Criminal justice tool</td>
<td>Serving police and enhancing criminal justice operational capabilities; providing mission critical information to law enforcement practitioners</td>
<td>Designed Global Query application to provide accurate, detailed information quickly to cops in the field.</td>
</tr>
</tbody>
</table>

Table 9-1 Elements of ARJIS’ organizational identity.

“ARJIS is a center for regional collaboration”

Members of the ARJIS organization see ARJIS not just as a location of shared ICT, though that is a key component of the ARJIS system, but also as vehicle for shared communication among partners, shared values of public safety, and shared processes for
development and design. For the ARJIS organization collaboration is core to its conception of itself as an organization, to successful organizational action and to what distinguishes ARJIS from other IJIS.

Members of the ARJIS organization see ARJIS as a place of collaboration among regional law enforcement and public safety agencies. This collaborative activity is highly prized by ARJIS staffers and is seen as a validation of the organization’s efforts. As the Project Manager states:

*I think ARJIS fosters participation, cooperation. I think we foster relationships between agencies. My understanding is, compared to other regions in the country, we like to think that our users cooperate more, you know, I feel like cooperation breeds cooperation in that, you know, the more we have our business committee meeting and our technical committee meeting, we have our task forces, you know, we pull user groups together and then--well, I just love seeing a detective from National City, no matter if we came together for some other reason, I like the after chat, the detective from National City talking to the detective from Carlsbad, that frankly they might not have ever crossed paths if they hadn’t come to some ARJIS-sponsored, whatever, function.*

The types of interactions the manager speaks of – detectives serendipitously engaging in collaboration in ways that would otherwise be unavailable but for ARJIS – are one of the critical outcomes ARJIS organizational members strive for. She goes on to state that the members of the ARJIS organization are actively engaged in encouraging this type of interaction and that collaborative leadership is critical:

*I believe that we foster cooperation at a, you know, almost sort of a personal level, probably more so than other regional groups, I think especially at the chiefs’ level, and I go to the occasional chiefs’ meeting, I kind of see it.*

*So really for me, the one reason why we have been so successful is because of our governance and because of the strong executive leadership that is so collaborative, sheriff, all of them, the thing that they’ve all agreed on is that they leave their egos and attitudes in the closet, they go into a room and they are all equal. Once again that same*
equal thing, they're -- each agency is just as important no matter what it is, they continue to embrace that.

It is worth noting that the quoted manager expresses a view that not only is it cooperation and collaboration that are key to who ARJIS is as an organization; but that it is the emphasis of these identity characteristics that differentiate ARJIS from other IJIS. That which makes an organization unique is a key element of the organizational identity concept.

Organizational artifacts such as the ARJIS vision statement repeatedly emphasize the collaborative purpose of ARJIS. The ARJIS vision statement is statement of who ARJIS is and who ARJIS aspires to be as an organization in the future, and the vision clearly presents ARJIS as a collaborative enterprise serving regional needs. The document is riddled with language such as “coordination with community partners,” “cross-jurisdictional access,” and “regional cooperation and collaboration.” The ARJIS vision statement also emphasizes the external image of ARJIS as a collaboratory:

We are internationally recognized for leadership, collaboration, and information sharing, and regional acquisition of effective information technology. We use community partnerships and regional information technology to address and anticipate public safety issues and to improve quality of life.

For members of the ARJIS organization acting as locus of collaborative government and being recognized as such is of critical importance.

Institutional Roots of ARJIS Identity

It is perhaps unsurprising that ARJIS has developed the collaboratory identity given the institutional culture from which it emerged. Just as our individual identity is in part a product of our culture, so organizational identity is in part a product of the larger culture in which it exists. The San Diego region is a community of cities and suburbs. As one member of ARJIS stated, “San Diego is a city of cities.” While each individual city has its local governments, services,
and infrastructures, there is a high degree of regional collaboration among the individual cities. Going back to at least 1966 with the formation of the Comprehensive Planning Organization (CPO) which later evolved into the San Diego Association of Governments (SANDAG), local governments within the greater San Diego region have created a culture of collaboration among local partners (San Diego Association of Governments, 2008). This is the environment in which the ARJIS organization emerged and its identity reflects, at least in part, the broader institutional culture.

“ARJIS is a provider and facilitator of regional public safety technology”

The second major element of the ARJIS identity is that ARJIS serves as a provider and facilitator of regional public safety ICT. As articulated in the vision statement, ARJIS is the “convening agency for regional information technology.” ARJIS managers understand that the different member agencies have different and often competing technology needs and resources. The larger member agencies both have extensive ICT infrastructures and budgets. ARJIS management and developers cannot hope to replace these highly entrenched ICT infrastructures so they adopt an identity of facilitator to them; seeking ways to enhance large agency information systems through complementary technologies and applications (such as wireless).

At the same time ARJIS acts as a provider of ICT services to the smaller agencies that cannot for fiscal reasons, or choose not to for political reasons, develop their own ICT architecture and support infrastructure. ARJIS personnel have to balance these competing perspectives in their approach to ICT development. The Lead Programmer comments:

---

43 For example, in the proposed budget of the San Diego Police Department – one of ARJIS’ largest member agencies – for fiscal year 2010 is $409,325,900, approximately forty times larger than ARJIS’ FY09 proposed budget; and the SDPD’s FY2010 proposed budget for information services is $15,961,225, over $5 million more than the total ARJIS budget.
Oh, gosh, that Agency really wants to become the IT leader for all of San Diego County. Across most of California, that type of agency is the anointed network distributor of data. That's not so historically in San Diego. Agency X would very much like to become that; and it's largely a political issue. That would mean replacing ARJIS in a lot of ways. A lot of the agencies don't want that. They don't want, you know, they're on a peer-to-peer level with Agency X right now and they don't want to become subservient to them; so there's a political push the other direction to not let that happen. That's a whole political thing that we stay out of but we have to be aware of it.

The duality of this identity trait is reflective of the broader institutional environment that is policing in the United States. As discussed earlier, policing is a highly fragmented activity with authority and resources residing with individual agencies. Serving police, and more broadly public safety, ARJIS has to be able to accommodate this institutional reality.

By being both a facilitator and provider of technology and services, ARJIS is able to accommodate the existing institutional barriers to regional cooperation (different agencies with different interests) and simultaneously maintain buy-in for all the disparate partners by fulfilling their needs to the degree required by each member agency.

A description of ARJIS that came up repeatedly in interviews was of ARJIS as a service provider. ‘Service provider’ perfectly describes this dual role in that ARJIS is providing different levels of service based on individual member agency needs. Large member agencies that only want to share data with ARJIS while retaining the ability to develop and maintain their own ICT architectures are able to do so. For example, one member agency relied on ARJIS primarily as a data source; choosing to implement its own cutting-edge record management system and even test voice-activated patrol car controls. Smaller member agencies that want to rely on ARJIS not just for data but for ICT hardware and software applications are able to achieve that level of service.
“ARJIS is a criminal justice tool”

The third core element of ARJIS’ identity is that of a criminal justice tool. Consistent among all interviewees was the perception that ARJIS was there to serve users engaged in public safety and criminal justice. At ARJIS significant value is placed on developing systems that have a great amount of utility for the patrol officer, investigator, and criminal data analyst. ‘What is in it for the user?’ is the dominant design question. ARJIS’ lead programmer, the person most directly involved in the physical building of ARJIS applications, states:

_We have a lot of projects going on, and as you see we are not a very big place. And so I guess really my first question is, do my users want this, I mean is this useful, is it appropriate, is it relevant, is somebody already doing this smarter than we are?_

The Project Manager echoes his point:

_The technology is secondary to the functionality, but I mean we’re pushing some functional issues that, more common in the internet and business, law enforcement has not necessarily caught up with nationally, so we’re trying to bring in that functionality for our users, so that tends to be what pushes our technology more than anything else I think._

For ARJIS employees serving the user trumps serving any particular member agency. This is in part due to ARJIS’ top manager being a former police officer; an experience that provides her with first-hand insight into the needs and mentalities of her user community – she “thinks like a cop.” ARJIS’ top manager knows, and has conveyed to her staff members, that ARJIS features will go unused if they are perceived as trivial, awkward, or useless. Further she understands the potentially catastrophic consequences of a system that is ineffective or difficult to use for the police officer out in the field. ARJIS serves cops and those who help cops such as criminal data analysts.
This emphasis on user-driven design is perceived as a feature that distinguishes ARJIS both technologically and organizationally from other integrated criminal justice information systems as the Lead Programmer’s comments make clear below:

*I think the ARJIS system is different because it is so based on user requirements, user requirements and a business case established up front, the users are involved in the annual work plan of ARJIS and any and all applications that are developed from the beginning all the way through the end.*

For ARJIS staffers, ARJIS is different from other IJIS because of the way in which they engage the user at all levels of the design process.

**How do ARJIS organizational and technological infrastructures reflect ARJIS’ identity?**

**The organizational architecture of ARJIS facilitates regional collaboration and partnership in governance and design**

Two key features of ARJIS’ organizational architecture reflect its identity as a center of regional collaboration. The first feature is ARJIS’ governance mechanism, a Joint Powers Agreement (JPA) which legally established ARJIS as an organization and established the rules by which agencies would participate. The second feature is ARJIS’ collaborative approach to design – both organizational and technological. Each member agency participates in the technological and business design process giving each agency a chance to shape the final design outcomes.

**Joint Powers Agreement**

Fundamental to ARJIS’ collaborative identity is its governance mechanism – a Joint Powers Agreement among participating agencies. The JPA is a relatively simple but highly effective legal agreement that establishes the rules for membership, participation within the ARJIS system, and the governance hierarchy. Funding of ARJIS is achieved through the
payment of dues by member agencies; larger agencies such as the San Diego Police Department and the San Diego Sheriff contribute more than smaller agencies such as Chula Vista’s police force. A committee populated by chief executives of the member agencies and elected politicians retains final decision making authority for all ARJIS business and technical decisions.

Most importantly, and where ARJIS’ collaborative identity is most-clearly visible, is in the voting mechanism established by the JPA. Each member agency has equal standing in the decision making process with one vote. Therefore the respective size of the agency is made irrelevant in ARJIS decision-making. Though a massive agency like the San Diego Police Department may pay over forty times ($1,731,898 for fiscal year 2008) more than a small agency like the Coronado Police Department ($39,419 for the same time period) both agencies retain the same voting power. Further, by distributing power equally among member agencies, the JPA serves to prevent ARJIS from falling under the sway of any single agency. Discussing ARJIS governance, the Executive Director notes:

*I consider ARJIS very democratic, you know, our one agency, one vote model at the -- for instance, at our chiefs' level, I think that helps balance the playing field between the large agencies and the small agencies.*

The one agency/one vote model permeates the entire ARJIS governance structure and design process, and it serves to reinforce and maintain ARJIS’s identity of collaboration. It is not just the JPA that reflects ARJIS identity of collaboration. The manner in which ARJIS has constructed its organizational processes for decision making does as well.

**Collaborative Decision Making**

ARJIS employs a hierarchical governance structure where business and technological decisions work their way through a bilateral committee process. A ‘Technical Committee’ makes institutional-level design decisions pertaining to the ARJIS ICT infrastructure.
Committee members address questions of technological feasibility and requirements pertaining to any proposed system design change. A ‘Business Committee’ handles the business concerns related to both the ARJIS organization and technological architecture. This committee evaluates the business case for any proposed modification to either the technological architecture or organizational practice. Each of these committees is populated by an individual representative of each member agency, often mid-level managers (such as sergeants) and expert users. Decisions are made within an individual committee and then sent to the other committee for evaluation and approval. Once a design decision is approved out of both committees it is brought to the Public Safety Committee, which is populated by chief executives of the member agencies and elected representatives from regional government, for final approval.

Figure 9-1 ARJIS’ governance structure reflects its collaborative identity.

The organizational architecture is designed to facilitate collaboration not just across agencies but across hierarchical levels of the organization. Anyone who has seen a police drama understands that the needs and interests at the top of the police hierarchy (chiefs, high ranking
officers) can often vary from those at the bottom (e.g., patrol officer). The ARJIS committee structure allows these needs to be communicated and evaluated both across agency boundaries and hierarchical levels. Talking about how ARJIS approaches the decision on whether to add a new component to ARJIS, the Project Manager states:

*I think the chiefs -- it's your view of what you're doing, the crime analysts kind of have this feeling they want to help the people and then the chiefs look more at it from a liability and a business case. So it's really interesting to see the different perspectives; that's why we have so many committees because everybody looks at it with a different viewpoint and then the recommendations made up to the chief.*

Similarly:

*We take it pretty seriously. We really kind of, you know, analyze it to death and look at all sides of the issue: really get the input from the analysts' side, from the technical side, from the chiefs' side, from the elected official, and then the ultimate say is really the chief. But we do a lot of research. So we don't do it haphazardly or quickly, we really put a lot of analysis into it which probably makes for a better product; and we have the attorneys also who get involved for appropriateness.*

Collaboration at ARJIS is extensive and includes technical and non-technical institutional actors. The varying, and sometimes competing, perspectives matter to ARJIS as an organization, and making organizational and technological decisions that satisfy as many of the competing interests as possible is a priority organizational goal.

As will be shown later in this chapter, this high level of collaboration in the management of the ARJIS organization and the design of ARJIS’ ICT is a differentiating characteristic of ARJIS. ARJIS varies greatly from JNET in the degree to which the governance and design processes are integrated across agency boundaries and levels of the organizational hierarchy.

**ARJIS designs and employs ICT that reflect its organizational identity**

ARJIS’ organizational identity is not only reflected in its organizational design and practices, but in its ICT artifacts. The systems, hardware, and applications designed and
employed by ARJIS reflect their organizational identity in three key ways. One, ARJIS’ approach to design is collaborative resulting in ICT architecture whose features and functionality represent an outcome negotiated by multiple constituents. Two, ARJIS’ ICT are overwhelmingly designed to serve as an aid to police, investigators, and criminal justice data analysts. Three, the ARJIS ICT architecture is designed to centralize data and maintain ARJIS position as the central resource for regional criminal justice information.

How does ARJIS’ organizational identity get inscribed in the technologies ARJIS implements? The answer is ARJIS’ identity shapes these technologies indirectly through its organizational values and practices. The three components of ARJIS identity constrain and direct the decisions made in the committees and by the organizational leadership regarding the design of the system. The collaborative element of ARJIS’ identity means, at a minimum, all strategic system design decisions must be negotiated by, and benefit, the member agencies who participate in ARJIS. The ICT-provider component of ARJIS’ identity means that, in ARJIS, management is looking for features, components, and applications to add that increase ARJIS’ standing as the regional IT resource for law enforcement; again, this plays a critical role in the overall configuration of the ARJIS technical architecture. Finally, the criminal justice tool component means that when deciding on and configuring pieces of hardware, an application, or information, ARJIS designers are first and foremost thinking about how the design will benefit the cop on the street. ARJIS’ organizational identity guides its organizational behavior related to ICT design which determines the end-design of ARJIS’ ICT.
Design of ARJIS ICT is collectively negotiated by member agencies

ARJIS approaches the design of its ICT as a collective process through which member agencies negotiate their individual needs into the final design. This negotiated design occurs at both a macro level through the Business and Technical working groups and the Management Committee, and at a micro level where technical experts from individual agencies decide on the technical particulars of a system.

All the member agencies are represented on the Business, Technical, Management, and Public Safety Committees. Through these committees, individual member agencies can propose requests for functionality, access, or other requirements for the ARJIS system. Chiefs of the various member agencies often propose new functionality or modifications to the existing technological architecture. The proposal is negotiated among the other committee members and if ratified, the proposed system change is delegated to the ARJIS working groups for action. The
ARJIS Security Center (a suite of authentication and encryption applications) provides an
illustrative example of this process in action. The Project Manager explained the system to me:

We have a new authentication system. This is where all of our users, usernames and
passwords are kept. We call it the ARJIS Security Center and each agency has an
administrator that has been trained to go in and reset a password or create new users or
delete this cop who retired. So, one of the things the chiefs asked for was specifically, the
Chula Vista chief, could the users be warned before their passwords expire and not let
them expire and then notify them. So we went to our programmers and they implemented
a feature from the Security Center that has an e-mail component.

So, we crafted up a little e-mail, and what happens now, is we watch their passwords and
send them a courtesy e-mail that notifies them their password will expire in 15 days. It
provides them a link to click to change their password. If they ignore that e-mail they get
another in 7 days with a link. And finally they get one that notifies them their password
has expired and provides a link. They have never had such proactive alerting on their
passwords before. That came from a chief, and we turned it around and put it into
production.

More often, a member agency may make a request at either the Business or Technical working
groups where if approved, is then sent to the other committee for approval; upon approval by
both committees, the proposed design change works its way up through the Management
Committee and then Public Safety Committee for final approval.

In either case, the design process is highly collaborative resulting in a design outcome
that reflects an amalgamation of the various member agencies design requirements. Consider for
example the ARJIS data dictionary. New codes are continually added to the ARJIS data base to
account for new types of crime, changes in criminal law, and agency needs. ARJIS proposals for
new codes are made in committee where through negotiation the final form of the code is
defined. These new data codes are then incorporated into the ARJIS database and all the
member agency systems to ensure conformity.
Because the design of the data standards is shared among the member agencies, there is an additional peer pressure among the member agencies to ensure compliance with the data standards and code definitions. When an individual agency fails to comply, their representatives often receive kindly intended, but undesired, derision from their peers. This social interaction among the member agency representatives serves as an informal mechanism for ensuring compliance with collaborative design and is so effective that more formal mechanisms for ensuring compliance are often not employed.

The design of the ARJIS system implicitly reflects those design recommendations that were rejected. For example, in 2007 the Management Committee decided not to make a field capturing document status mandatory because it was viewed as overly burdensome and not returning much investment. Similarly, in 2008 a member agency proposed tracking pawn slips in the ARJIS system, but the proposal was rejected in committee by other members who did not have pawn shops in their jurisdictions and did not see the value of the investment.

Facilitating police use of information is overriding design rationale
A second dimension of ARJIS’ organizational identity is that of serving police and facilitating their use of information in order to perform their jobs more successfully and safely. ARJIS’ public relations materials talk about how “cops use ARJIS to solve crimes, identify suspects, and enhance officer and public safety.” In assessing the BORDERSAFE project to provide access to ARJIS in the field via handheld devices, “positive impact on field operations” is listed as the primary benefit. ARJIS goals are to “…solve crimes, identify offenders, link cases across jurisdictions, and alert officers.”

44 “Document status” refers to the current political language of referring to whether or not a person in is the United States legally or illegally. The political language no longer refers to individuals in the country as ‘illegal aliens’ but as ‘undocumented workers.’ Given San Diego’s proximity to the border of U.S. and Mexico, the problem of undocumented workers is a continual one.
This identity of serving cops is a very prominent and powerful component of ARJIS’ overall identity and is manifested in the design of ARJIS’ systems in a myriad of ways. For the ARJIS technical and business working groups, the “benefit to agencies and officers” is one the four priority criteria used to decide the worthiness of a potential project. Here is what the Lead Programmer stated about ARJIS’ approach to system design:

*I mean we can't lose sight of the fact of who our customers are and what we do for them. That has to stay core and actually we have to be careful, as exciting as some of the new technologies and some of the national things are, we can't lose sight of the main goal of ARJIS is providing data to officers and investigators in the field.*

In discussing the ARJIS Global Query application, the Project Manager echoes this view:

*But the whole goal for the system was keep it simple. Make it easy for the cops; give them a quick hit with valuable returns. Don't make the query or the returns too complicated. I think it was just user simplicity.*

This identity of serving cops, making it easier for them to be effective and to be safer has had material consequences for the ARJIS system.

The aforementioned Global Query, obviously, is one example of how the identity of “serving cops” has been translated into material features of the ARJIS technology infrastructure. Police officers in the field cannot afford to be distracted by having to form complex queries or decipher query results in an unfamiliar format. So ARJIS designers built the Global Query interface to allow officers to query by filling in pre-defined form fields such as first name, last name, data of birth, and driver’s license number – information officers are familiar with and likely to have access to. Similarly, the results returned by Global Query are formatted in a way police officers are familiar with, and labeled using every day language (e.g., race, sex, height) in order to make them more easily understandable.
ARJIS’ wireless access project also demonstrates how their identity as an aid to police shapes their design process and ultimately the systems that materialize from their design process. The top priority in designing the new system was that the system had to be useful for cops. This meant that it the system had to be reliably accessible in both urban and rural areas of San Diego County45. The ability for the police in the field to connect reliably was more important than data transmission speed or price. This was particularly true in the early phases of the project as the test users were to be U.S. Border Patrol agents working on or near the U.S. – Mexico border which is essentially desolate outside of the border-crossing areas. For this reason, ARJIS designers ended up choosing Verizon over the primary wireless provider in the area (Qualcomm) because Verizon provided better coverage in rural areas even though Qualcomm had better bandwidth and may have offered a better subscription rate.

What we see in these two examples is evidence of how one dimension of ARJIS’ organizational identity – that of an aid to police in the field – shaped the design process and the technological outcomes that process produced. When ARJIS designers and managers consider adding data, creating a new application, or introducing a new device, the utility of the new addition for police officers working in the field is a top consideration.

ARJIS ICT are strategically oriented towards making ARJIS the central regional resource for criminal justice information

A third component of ARJIS identity that is reflected in the design of its ICT is the identity of central regional resource for criminal justice information. Members of the ARJIS organization see their ARJIS as being, or becoming, the primary point of access for criminal justice data in the San Diego County region. ARJIS designers and managers want police and

45 San Diego County encompasses approximately 4,200 square miles of terrain, most of it rural, unincorporated land. See U.S. Census Bureau (http://quickfacts.census.gov/qfd/states/06/06073.html).
other public safety officials to rely on ARJIS for their criminal justice data. Here is how the Lead Programmer at ARJIS described it:

Well, ARJIS is a clearinghouse for data, law enforcement data in the San Diego region. We take in virtually every piece of paper that an officer touches or creates and we pull it into a central database, that other agencies can then turn around and access so that if a car is involved in a bank robbery in Oceanside, that officer that stopped a car in El Cajon will find out that it matches the suspect's description. That in a nutshell is what ARJIS does. We bring that kind of information to the individual officers and investigators and other people that have need of it, and it kind of crosses those boundaries. That was the original purpose of ARJIS. San Diego is -- for a very long time has been a community of cities, you know, kind of all merged together so the boundaries that make up the cities don't really apply to -- in practice to how we use the data. In more modern times, especially post-9/11, it's kind of a national imperative to start sharing data, that's for a long time been, I think even predating that, the goal of ARJIS is to start bringing outside information in, that's kind of been our purpose.

Similarly, the ARJIS Project Manager states:

We are the single repository in the region for law enforcement data. There isn't another ARJIS.

This is one reason why ARJIS houses all its member-agency data within its legacy mainframe rather than simply acting as a connection relay among the distributed member agency data sources. By storing as well as providing access to the data, ARJIS managers can ensure that the data is high quality, standardized, and centralized. ARJIS designers can also, then, standardize the interface to the data ensuring that the data serves regional needs rather than local ones.

ARJIS’ organizational identity as the central resource for criminal justice information impacts their system design in another way. ARJIS as the central criminal justice information provider grows the technological architecture through activities such as obtaining grant funding and negotiating information sharing agreements. The wireless project mentioned previously is an excellent example of how this occurs. ARJIS obtained the funding to build and test wireless
access to the ARJIS system from the National Institute of Justice, and through this funding added new technologies (handheld devices, cellular networking) to the ARJIS infrastructure as well as new sources of data (the Tucson, AZ Police Department) obtained through information sharing agreements negotiated by ARJIS. In other words, members of the ARJIS organization see ARJIS as the central location for criminal justice data. Consistent with this identity, ARJIS seeks opportunities to reinforce their role as criminal justice information provider resulting in new components, functionalities, and sources of data being added to the ARJIS system.

**JNET**

Like ARJIS, JNET’s organizational identity has important consequences for JNET’s organizational and technological design. However, as detailed below, the differences in identity between JNET and ARJIS are evident in the differences between these two systems relative to their organizational and technological design. Analysis revealed two main elements of JNET’s identity: JNET as a Commonwealth agency; and JNET as a broker of information among various public safety agencies. These two elements of JNET’s identity shaped both its organizational and technological features. For instance, JNET’s governance structures and strategic planning processes have been developed to serve the interests and needs of Commonwealth agencies over other stakeholders such as municipal police and local or regional governments. As an information broker, JNET designers and managers have deliberately eschewed taking ownership of systems or data in favor of designing an information system that provides point-to-point connectivity to existing individual systems.

**What is JNET’s Identity?**

JNET first and foremost identifies itself as a Commonwealth agency: a member of Pennsylvania’s state-level administrative machinery. Second, JNET sees itself as a broker for other Commonwealth agencies, providing organizational and technological connectivity to
achieve Commonwealth public safety goals. JNET’s identity is not that of a collaboratory, but rather more similar to that of a matchmaker: JNET identifies or is approached by with the need to share information and builds the connection between them and incorporates that connection into the JNET suite of applications\textsuperscript{46}.

<table>
<thead>
<tr>
<th>Element of Identity</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commonwealth agency</td>
<td>Commonwealth agencies primary clients; Representatives from Commonwealth agencies dominate JNET governance</td>
<td>In prioritizing which projects to take on, a project for a Commonwealth agency receives greater weight than a project for a municipal agency.</td>
</tr>
<tr>
<td>Information broker</td>
<td>Providing access to through the building of connections to individual systems; no ownership of data or systems</td>
<td>JNET connects to each system individually and minimal federation of queries or results.</td>
</tr>
</tbody>
</table>

Table 9-2 Elements of JNET’s organizational identity.

\textit{JNET as a Commonwealth agency}

JNET is first and foremost an agency of the Commonwealth government. This element of JNET’s identity makes sense given JNET’s institutional location within the executive branch of the government. This dimension also makes sense given that JNET’s primary governing body is overwhelmingly comprised of representatives of Commonwealth agencies.

The members of JNET who I interviewed repeatedly stressed the centrality of the Commonwealth to JNET’s identity. JNET’s Executive Director, for example, repeatedly emphasized the focus on Commonwealth needs and interests in JNET decision making and technology design. The Executive Director of JNET commented on how switching from a growth mode to a stabilization mode has affected JNET organizationally:

\textsuperscript{46} I use the term ‘matchmaker’ to convey the idea of JNET as a third party bringing two separate entities with a common information need together.
We've built a lot of dependencies in JNET that were never part of the original mission. And we're able to not just discuss but demonstrate the return that the Commonwealth has made on investing in this agency.

Discussing how the organization vets what projects to take on, the Executive Director adds:

*Part of that vetting process for a project is 'who is going to benefit from it?' I'll be honest if a local cop's going to benefit from it and the state police have no interest, it may not occur.* But I would say that, looking at our user base, it's pretty equal across the board. Local, county, and municipal government is as essential to me and our success as state government. *The difference is they don't sit our governing committee.*

Notice in the second quote how even though the Executive Director states that his own personal interest is serving users at all levels of government, he readily admits that organizationally, JNET serves the Commonwealth first.

The other JNET employees I interviewed echoed these sentiments. For example, when discussing how JNET had been stabilizing as an organization, JNET’s Architectural Manager also emphasized the importance of the JNET’s place within the Commonwealth government:

*When I say operationalizing, even though there's a operations arm that handles firewalls, server site and that kind of stuff but operationalizing JNET, more of getting into a stable platform where our level of our maturity within Commonwealth government is more attached because, again, when we first started we were actually, actually worked for state police, now we're Office of Administration so being here in that move as well, when we shifted organizations within Commonwealth.*

The Application and Development Manager for JNET emphasized the potential benefit of JNET’s adoption of state-of-the-art technology to the Commonwealth once other agencies caught up. In the first interview, the JNET Executive Director commented:

*The Commonwealth tends to be behind the public sector when it comes to technology. I believe once the other agencies catch up, I hope that JNET becomes a service provider of web services to other agencies within the public safety arena. Even if we have the web services right now which we actually do have several that have gone into production,*
other agencies aren't ready to consume them. So we're a little bit ahead of the curve and once they catch up, I think that could become of major benefit to the Commonwealth.

JNET’s organizational membership sees the Commonwealth government and its constituents as their primary client and the primary beneficiary of JNET’s services. When presenting JNET to outsiders, JNET management describes JNET as “the Commonwealth’s information broker,” and “the collaborative effort of 16 state agencies.”

In the future, JNET’s identity as a Commonwealth agency is likely to become stronger. Beginning in 2007, JNET began replacing contracted employees with employees of the Commonwealth government in order to reduce the costs of retaining vendor-based contract employees. In that year, JNET replaced 12 contractors with 12 Commonwealth employees. JNET management’s long term goal is a “fully staffed Commonwealth complement.” One result that seems likely to occur from greater percentage of JNET’s staff coming from within the Commonwealth government is that JNET’s identity as a Commonwealth government agency is likely to only increase and become more entrenched.

**JNET as Pennsylvania's public safety information broker**

The second element of JNET’s organizational identity is that of a public safety information broker. Unlike ARJIS who saw their organization and system as a source for public safety information and technology, the JNET organization sees itself as a provider of access to public safety information. For the organizational membership of JNET, mantra is access, not ownership. Statements from three different organizational members help make this clear. The Executive Director emphasizes JNET’s role as a broker rather than collector of information:

*When I look at JNET versus any other private or public sectors out that there that are claiming to be integrators of public justice data, there are two major differences. First one is, we don’t store, we don’t retain, we don't maintain data and I think a lot of other agencies are collectors of data and providers of that same data that they're collecting.*
Sometimes fee for service, sometimes not, but we do not collect, store, or maintain data. We are simply a hub on that giant wagon wheel. The other piece of that is we are developers of the systems that need to be -- that are used to broker that information.

When asked how they would present JNET to outsiders, the JNET Architectural Manager and Project Manager both invoke the broker identity:

*I would say JNET is the broker for multiple data sources within the justice community in order to increase public safety and sharing that information.*

*JNET I think is, as we're pretty much supposed to be, we're the facilitator of all of these, you know, the other providing agencies that provide data and input, so forth, we’re the facilitating organization which should know what's going on and be able to keep everything rolling and spinning.*

The brokering of information, and providing connectivity to public safety data sources, is a driving motivation within the JNET organization, particularly for their technical staff. This aspect of JNET’s identity traces back to the organizations origins.

**Institutional Roots of JNET's Identity**

JNET’s identity as a Commonwealth agency and a broker of information is rooted in the institutional environment from which it emerged. As noted in above, JNET was founded as an agency as a result of an executive order signed by Commonwealth government’s chief executive. JNET is organizationally located within the larger government organizational hierarchy. JNET management is responsible to representatives of the Commonwealth government both directly via the Office of Administration and indirectly via legislation, and requests for service by government agencies and its governance structures.

The broker identity was formed during the early stages of JNET’s development as both an organization and as a suite of applications. There were many institutional barriers to getting access to criminal justice information. In particular, JNET managers had to overcome extreme
reticence by the PSP to relinquish any control over access to their data. As the Project Manager noted:

Probably the biggest accomplishment that JNET has achieved is getting agencies to play well in the sandbox together. If you've grown up in the IT world, we've always been told to keep our data, protect our data, and don't share your data. And that's just how we grew up, you know, this is my data, nobody else can have it and then justice, you got to take that times a hundred, say this is my data and I can't share it, so I think their biggest barrier and biggest achievement was being able to break down those barriers and get agencies to share data, get the courts to share data with parole, share data with police. But because they did it in increments, and you can imagine, okay, they went to AOPC they said, come on, can we do this, let's try this pilot, so went one little silo, went to PSP, here went another silo so just through the evolution of the organization, these silos were built, pulled more people in and more people in, and we grew and we grew and we grew and we continue to grow. o it was just a natural evolution that occurred, had they tried to do the big bang theory and say let's get everybody in a room and let's take all this data, it would have never worked.

The method JNET management used to get past the institutional barriers that inhibited the sharing of data was to build connections to individual systems in isolation. This strategy allowed JNET management to negotiate data sharing arrangements specific to each system and to retain control of the data with the individual agencies that operated the systems. This strategy also allowed JNET to be a facilitator of technology for Commonwealth public safety agencies.

JNET’s Executive Director comments:

The other thing that the ESB does for us is we expose web services off of them, we have one web service now that's available for warrant searches and kind of the vision of Chad Firestone at the time when he started this project was let's get JNET to the point where JNET is being used as a service but it interacts with legacy systems to help enhance them, the users don't know that JNET is powering them so it's kind of like the police records management system XYZ powered by JNET. And what would happen there is police records management could consume this web service for warrants, they're doing their entries for an incident and in the background our web services is presenting them, making them part of their case.
Organizationally, JNET was adopting a broker identity whose purpose was to connect previously unconnected agencies by overcoming or bypassing preexisting institutional barriers. Technologically, JNET ended up with a hub and spoke design which each spoke connecting to an individual system in isolation.

To summarize, JNET’s identity is that of public safety information broker for the Commonwealth of Pennsylvania. JNET’s primary client is the Commonwealth government. JNET connects rather than owns data sources. JNET continually seeks opportunities to employ new technologies in its overall design. Let us now explore the impact of JNET’s identity on its organizational processes and its technologies.

How do JNET’s organizational and technological infrastructures reflect JNET’s identity?

JNET’s identity is reflected in its organizational structures and processes

JNET’s organizational features and processes reflect, primarily, JNET’s identity as agency of the Commonwealth government. Structurally, JNET’s governance – both direct and indirect – is dominated by Commonwealth actors and interests. JNET’s identity as a Commonwealth agency also plays a key role in shaping the organization’s strategic planning processes.

Governance structures

A review of JNET’s website and primary documents provided by the JNET staff shows that JNET is governed directly by its Steering Committee. When the Executive Director needs resolution to a thorny problem, he looks to the Steering Committee to make the final decision on the matter. Through the Steering Committee JNET is governed by representatives of agencies in the Commonwealth government. And, in both cases, there is effectively no representation of
stakeholders outside the Commonwealth government such as the counties, municipalities, or federal agencies\textsuperscript{47}.

For example, both direct observation and analysis of the minutes of Steering Committee meetings revealed that JNET leadership is focused on issues related to the state government and public safety, as these dominate the meeting agendas. During the year 2007, the only mentions of the counties in the minutes are in the form of providing status updates for projects (e.g., “We’ve deployed to five more counties this month,”). Conversely, the same analysis reveals that meeting topics focused on pending legislation that may impact JNET, discussion of what various state agencies are engaged in, JNET status updates and status updates for various individual agency systems. What this evidence indicates is that the only parties that have a place at the JNET governance table are those associated with the Commonwealth government. Parties from the local, county, or federal levels of government simply have no say in the governance of JNET.

The Steering Committee’s role in JNET governance has changed over time. As JNET has stabilized as an organization, the Steering Committee’s role has been reduced to primarily one of oversight rather than active management. Still, the Steering Committee’s influence remains strong on JNET’s identity and organizational practices. Early in JNET’s development, the Steering Committee took a lead role in forming JNET policy and shaping JNET day-to-day decision making. The executive order that mandated the creation of JNET established this role for the Steering Committee. In recent years, JNET has begun to stabilize as an organization and require less oversight from the Steering Committee. As a result, the Steering Committee’s role has primarily shifted to an oversight role ensuring that JNET takes actions consistent with the

\textsuperscript{47} In 2003 the JNET Steering Committee voted to add 3 at-large members, at least one of which would be representative of a county. However, none of the three at-large members would have voting rights so the net effect of their addition to the Steering Committee on JNET’s governance was negligible.
policies, guidelines, and values established earlier. Even though the Steering Committee’s role has changed, its influence remains strong within JNET’s management culture, reinforcing the Commonwealth orientation of JNET’s identity.

**JNET Governance processes**

JNET’s identity as a Commonwealth agency is also reflected in its strategic planning process. JNET is an agency within the Commonwealth government. When forming the agency’s strategic plans, JNET management creates plans consistent with the goals and policies established by the Commonwealth government. JNET’s strategic planning process starts with the Keystone Plan – a document produced by the Office of Information Technology detailing the high-level goals and objectives for a five year period. For example, the goals established in the 2006 Keystone Plan included ensuring IT investments align with business objectives, leveraging existing IT investments, documenting business and technical relationships, assessing projects by their ability to reduce IT costs, reallocate redundant resources, efficiency, and improved services levels, and, developing a Commonwealth IT workforce.

The JNET management team, lead by the Executive Director, then develops a five year strategic plan based on the Keystone Plan requirements and goals and JNET’s internal technological goals. Then, each year, JNET management produces a one-year business plan that outlines all the projects JNET will do for the year. Because the five year strategic plan and annual business plans are all derivative of the Keystone Plan, all projects JNET takes on are, in effect, products of the Keystone Plan. Conversely, as the Executive Director’s comments indicate, any proposed project that does not align with the one-year, strategic, and Keystone plans, does not get done:
The Keystone Plan was published, and then we developed a five-year strategic plan. Once that plan was completed, and we had to go through and make sure everything we wanted to do as an agency aligned with the Keystone Plan. Then we develop an annual business plan that has to align with the strategic plan. Each year, every project has to tie back to the strategic plan and the Keystone plan. If we can't, there's no value in completing that project.

For JNET management there is no value in working on projects that do not conform to the goals and policies established by the Commonwealth government. It is easy to see how JNET using a Commonwealth-oriented strategic planning process makes sense from a practical perspective: JNET management, particularly the Executive Director, must act in accordance with the wishes of their superior managers.

Using a Commonwealth-oriented strategic planning process also makes sense from an organizational identity perspective. Central to JNET as an organization is its location within, and purpose of serving, the Commonwealth government. Being part of the Commonwealth government, and partnering with other agencies within the government is core to who JNET is. As a result, it would be inconsistent with JNET’s identity of itself as an organization to employ a strategic planning process that did any other than align with the goals and policies of the Commonwealth government. What will be shown in the next section of this chapter is how this identity as a Commonwealth agency is directly manifested in the design and configuration of JNET’s ICT.

JNET’s identity is reflected the design and configuration of its ICT

Project Selection: For and by commonwealth representatives

The process by which JNET management selects and then prioritizes technical projects reflects both the ‘Commonwealth’ and ‘technologically progressive’ dimensions of JNET’s identity. JNET uses a weighted scoring matrix to evaluate proposed projects and to assign
resources. Proposes (and later accepted) projects are scored on 11 dimensions such as alignment with strategic goals, number of users impacted, and whether or not the project can be successfully realized with existing JNET resources. Projects are assessed using the 11 dimensions and receive a weighted score which is then used to rank the project priority among other possible or ongoing projects.

<table>
<thead>
<tr>
<th>PROJECT TITLE:</th>
<th>Enter the Project Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sponsoring</td>
<td>Enter Sponsoring Agencies Names</td>
</tr>
<tr>
<td>Rater's Name:</td>
<td>Enter rater name(s)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Prioritization Criteria</th>
<th>Weight</th>
<th>Select</th>
<th>Decision Weight</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alignment – How well does this initiative support JNET’s Mission and Goals?</td>
<td>20%</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Provide a platform for improved public safety</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resolve integration issues</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Deploy emerging technologies</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pursue more aggressive means to ensure protection of data</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Explore cost-effective solutions</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strategic Goal 1 - Transition from collaboration to integration</td>
<td>5</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strategic Goal 2 - Primary Public Safety information broker</td>
<td>5</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strategic Goal 3 - Transition from a Technology-centric focus to Customer-centric focus</td>
<td>5</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strategic Goal 4 - Highest quality of service (i.e., eliminate or reduce bags)</td>
<td>5</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Urgency - Is there a funding time limit, or regulatory compliance date that must be met?</td>
<td>10%</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Does it require additional funding from the JNET Operating Budget?</td>
<td>10%</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Figure 9-3 The JNET project scoring matrix.

The properties of the scoring matrix itself reflect the Commonwealth and technologically progressive aspects of JNET’s identity. The matrix weights projects more heavily if they “deploy emerging technologies.” A project that impacts a Commonwealth agency – particularly the Pennsylvania State Police or the Association of Pennsylvania Courts – also is weighted heavily. The potential costs savings of a project are evaluated in terms of cost savings to the Commonwealth the project will provide (as opposed to a specific agency or region).
The outcome of weighting potential projects this way is that the designs of JNET technologies reflect their broader identity as a technologically progressive Commonwealth agency because the projects that are selected and receive the most resources are those projects that serve Commonwealth agencies and use modern, cutting-edge technology. Projects that only benefit a local agency or group of agencies are passed over for projects that benefit the Commonwealth overall or Commonwealth agencies in particular. Projects that allow JNET to procure new technology or upgrade the system are prioritized over those that make use of old or obsolete technologies.

JNET uses point-to-point rather than federated connectivity

JNET’s broker identity is reflected in its system architecture, user interface, and messaging application. As noted previously, early in the development of the JNET system JNET management chose a strategy of building isolated connections to the specific system of the Commonwealth agency with whom they were partnering. JNET designers chose to build their system in this fashion because true integration and collaboration among multiple agency partners was seen as too complex and too difficult a process, and JNET managers critically needed to get “buy-in” to the new system. The result of this approach is a hub and spoke system architecture consisting of numerous single connections from the JNET hub to distributed systems rather than a single global connection to numerous distributed systems as found in ARJIS.
The decision to establish access to systems individually and in isolation had consequences for the user interface (UI) as well. Unlike ARJIS’ Global Query application where users can retrieve data from multiple databases with a single query, JNET users have to connect to each system individually from the portal. For example, take the scenario where a patrol officer has stopped a motorist and wants to find out if the person has a criminal record, is the subject of a restraining order, or on probation or parole. Assuming the officer has the appropriate privileges, after accessing the JNET portal, he first follows a link to the Commonwealth Law Enforcement Assistance Network (CLEAN) to see if the motorist has a rap sheet in Pennsylvania or otherwise. The officer then returns to the JNET portal and follows the link to “Justice Data” from which the officer can access the Protection from Abuse database and the Flexible Search application to find out of the motorist is a parolee or probationer or subject of a restraining order respectively.
To summarize, JNET’s broker identity is a byproduct of JNET being created in an institutional environment in which the agencies JNET was to establish connections with were highly protective and controlling of their data, thus precluding JNET from attempting to centralize and take ownership of the data. Thus, JNET management decided to establish connectivity to each source system separately, and each with its own query application. The result was a hub-and-spoke network architecture, with a comparatively (to ARJIS) non-integrated user interface.

A third way JNET’s broker identity is reflected in its technological architecture is the JNET messaging system JNET has deployed. Specifically, as the central connector of many disparate databases, JNET built a messaging infrastructure and interface to notify uses and agencies when data had been entered, queried, or modified. JNET highlights the brokering aspect of the messaging system in its public relations materials:
JNET serves as the messaging broker between county jails and the DOC, county probation departments and the PBPP, and between the AOPC, PSP, and county records management systems. JNET brokers’ information between agency systems in real-time scenarios, and in many cases, fulfills the needs of data reporting requirements inherently delayed by resource, personnel, and technology constraints.

As with other aspects of the JNET ICT architecture, the retention of data ownership by individual agencies is a key feature of the messaging system:

This data exchange and event messaging model provides stakeholders with the ability to maintain ownership and control of their data systems, and has elevated county and state agency data availability.

Architecturally, the JNET messaging system is setup similar to that of the JNET system overall. The JNET messaging infrastructure sits among systems from the courts, counties, state police, and the Pennsylvania Commission on Crime and Delinquency. When a watch list triggers a notification (e.g., something on the match list is matched within a system) the message is sent from the host system to the JNET hub, and then relayed through the JNET messaging infrastructure to the recipient system or client. The messaging infrastructure, in essence, is a distribution center for data related messages.
The messaging system built by JNET is the example that best demonstrates the broker aspect of JNET’s identity. Fundamental to its design is a principle of relaying notifications about data rather than collecting and centralizing data.

**Conclusion**

In this chapter I have described the organizational identities of the ARJIS and JNET integrated criminal justice information systems, and detailed how those identities are reflected in their organizational structures, practices, and technological designs. There are three main elements to the ARJIS identity – that of a regional center for collaboration, a regional provider of criminal justice ICT, and a tool for public safety personnel. Two main elements make up JNET’s organizational identity: JNET as a Commonwealth agency and Pennsylvania’s public safety information broker. The identities of ARJIS and JNET formed in the way they did in part because of the institutional environments within which both IJIS emerged. The San Diego region has a long history of inter-governmental collaboration at the regional level. The agencies
in the Commonwealth of Pennsylvania government are highly protective and controlling of their agency data.

<table>
<thead>
<tr>
<th>IJIS</th>
<th>Element of Identity</th>
<th>Impact on Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARJIS</td>
<td>Regional center of collaboration</td>
<td>Collaborative governance, design, aggregated data and federated access to data</td>
</tr>
<tr>
<td></td>
<td>Regional provider of IT</td>
<td>Provides IT services and hardware to member agencies</td>
</tr>
<tr>
<td></td>
<td>Tool for public safety</td>
<td>Design and configuration of IT is expressly purposed to serve public safety personnel</td>
</tr>
<tr>
<td>JNET</td>
<td>Commonwealth agency</td>
<td>Commonwealth agencies receive priority in JNET governance and technological design processes and decisions</td>
</tr>
<tr>
<td></td>
<td>Pennsylvania’s public safety broker</td>
<td>JNET system functions as a gateway to individual agency systems rather than aggregating data centrally</td>
</tr>
</tbody>
</table>

Table 9-3 Differences in identity are reflected in design differences

The differences in the identities of ARJIS and JNET can be seen in the organizational and technological differences between them. Consistent with its collaborative identity, ARJIS has developed a highly collaborative organizational structure and design process. Its member agencies, all with equal standing, all contribute to the design and management of ARJIS. Technologically, the ARJIS system is designed to aggregate data from its member agencies, and applications such as Global Query provided a single point of federated access to multiple data sources. Consistent with its identity as a provider of IT to the region, ARJIS is a provider of both IT services and hardware to its member agencies. Finally, the applications and devices ARJIS builds and deploys are chose and configured expressly for the purposes of being of maximum utility to regional public safety personnel.
Conversely as a Commonwealth agency, JNET’s organizational processes are geared almost exclusively to serving Commonwealth clients. Commonwealth agencies enjoy priority in JNET business and technical considerations. As a broker, instead of aggregating information, JNET has been designed to act as the bridge that provides connectivity to different data sources. JNET designers have deliberately chosen not to aggregate data instead built JNET as a gateway to other agencies’ data sources.

To conclude: identity matters. Identity shapes organizational behavior and through that behavior the design of organizational technologies. This finding has implications for both theory and practice which I discuss in Chapter 11.
Chapter 10 Terrain with Coincident Boundaries: IJIS complexity and the spanning of group, organizational, and institutional boundaries.

Introduction

In this chapter I describe my findings on how integrated criminal justice information systems (IJIS) act as boundary objects. I begin with a brief review of boundary objects and social worlds in order to refresh the concept in the reader’s mind. I next make the case for IJIS as boundary objects drawing on empirical examples to support my argument that IJIS are terrain with coincident boundaries type boundary objects. That is, they have a commonly defined border among the communities they span, but the internal content of an IJIS varies by the community spanned. I then propose that the terrain type of boundary object is at a more abstract level than the other ideal types and conceptually subsumes those types.

A brief recap of boundary objects

The boundary object concept is drawn from theory of social worlds – communities centered on a common activity and forms of communication. In an effort to gain a more ecological view of how different groups collaborate, Star & Griesemer (1989; 1989) argued that boundary objects – objects spanning the borders of social worlds provided the mechanism through which different social worlds communicate. For example, a clay model of an automobile prototype might be a boundary object situated among the communities of engineers, designers, and marketers engaged in the work of bringing a new automobile to market. Boundary objects, such as the example above, are adept at facilitating communication across social worlds (or communities of practice) because they are simultaneously rigid enough to retain their own identity and malleable enough to be independently interpreted by individuals in the different social worlds (Ackerman & Halverson, 1999; Carlile, 2002; Fleischmann, 2006a;
Levina & Vaast, 2005; Star, 1989; Star & Griesemer, 1989). Boundary objects create common understandings, ensure reliability of communication, and create information integrity.

<table>
<thead>
<tr>
<th>Type of Boundary Object</th>
<th>Properties</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>Ordered piles of objects that are indexed in a standardized fashion (e.g., library, database)</td>
<td>Modular, able to deal with heterogeneity in units of analysis</td>
</tr>
<tr>
<td>Ideal/Platonic</td>
<td>Abstracted from all domains, adaptable to local site, serves as a means of communicating symbolically (e.g., social networking diagrams)</td>
<td>Adaptable</td>
</tr>
<tr>
<td>Terrain with Coincident Boundaries</td>
<td>Common objects with the same boundaries but different internal content (e.g., a map of the state of Pennsylvania)</td>
<td>Work can be conducted autonomously but cooperating parties can work on the same area with the same referent Resolution of different goals</td>
</tr>
<tr>
<td>Forms and Labels</td>
<td>Methods of communication across dispersed work groups (e.g., driver’s license)</td>
<td>Local uncertainties are removed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can be included as part of repositories</td>
</tr>
</tbody>
</table>

Table 10-1 Types of boundary objects.

Four idealized types of boundary objects have been identified: *repositories, terrain with coincident boundaries, platonic objects, and forms and labels* (Star, 1989). Repositories are modular collections of standardized objects; ideal/platonic objects are abstracted objects; terrain with coincident boundaries are objects with the same boundaries but varying internal content; and forms and labels are standardized forms of communication. These four idealized types are each ideally suited to particular contexts of boundary-spanning, but also share characteristics. Individuals in a social world learn to translate, negotiate, debate, triangulate, and simplify these types of boundary objects in order to fit them to their needs. As a result, the boundary object can be understood coherently, but differently, when standing between members of different social worlds. In this way they provide a boundary that also serves as a structure to jointly negotiate.
To summarize all boundary objects exhibit the following properties. One, the boundary object spans the boundaries of multiple social worlds or communities. Two, the boundary object facilitates communication and collaboration among the social worlds it spans. Three, the boundary object is rigid enough to exist on its own, but flexible enough to be uniquely interpreted by each of the social worlds it spans.

**IJIS as boundary objects**
Integrated criminal justice information systems exhibit the properties of boundary objects. IJIS as inter-organizational information systems, by definition, span the boundaries of multiple communities of practice engaged in criminal justice for the explicit purpose of facilitating communication among them. These communities of practice – to include law enforcement, the government, and the general public – collaborate on the work of criminal justice. Typical of boundary objects, IJIS exist independent of any particular community that engages the IJIS. At the same time, the ways in which different communities interact with and make use of the IJIS can vary from community to community.

<table>
<thead>
<tr>
<th><strong>Properties of Boundary Objects</strong></th>
<th><strong>Boundary object properties in IJIS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Span the boundaries of multiple social worlds (communities, groups, etc.)</td>
<td>IJIS span the boundaries of organizations, institutions, and user communities</td>
</tr>
<tr>
<td>Facilitate communication and collaboration among heterogeneous groups</td>
<td>Different user groups, communities, and institutions communicate and collaborate through the technological and organizational systems that comprise the IJIS</td>
</tr>
<tr>
<td>Rigid enough to exist independent of any single social world, but flexible to be interpretable by each social world.</td>
<td>IJIS exist as individual entities, but the forms of interaction vary with different communities.</td>
</tr>
</tbody>
</table>

Table 10-2 Properties of boundary objects.

**IJIS span communities of practice engaged in criminal justice**
Analysis of ARJIS and JNET revealed that IJIS act as boundary objects among multiple public and private communities of practice. The communities of practice that engage ARJIS and
JNET include the various user groups such as patrol officers, analysts, detectives, investigators, etc; and institutional domains such as vendors, policymakers, the general public, funding agencies, and researchers. The collaboration that occurs among these various communities can be direct or indirect. For example, JNET’s messaging system allows individuals in different user communities (e.g., investigators, patrol officers) and different organizations to collaborate on common issues by allowing the users to flag data and then be notified when that data is accessed or modified. This is an example of direct collaboration among different communities of practice.

![Diagram showing the ARJIS and JNET boundary objects.](image)

Figure 10-1 The ARJIS and JNET boundary objects.

An example of indirect collaboration is the collaboration of funding agencies and law enforcement agencies through ARJIS. This collaboration occurs bi-directionally. Funding agencies such as the National Institute of Justice contact ARJIS about developing a system or application for evaluation in the field. For example, in 2005 the Department of Homeland Security approached ARJIS about submitting a proposal for $500,000 to use technology to improve collaboration and interoperability in the region. Conversely, ARJIS management may also approach funding agencies on behalf of their members to get funding for a desired project.
For example, in 2009 the Management Committee asked that ARJIS submit on behalf of the member agencies to receive funding from the American Recovery and Reinvestment Act.\textsuperscript{48} In these examples, one community – funding agencies use ARJIS to achieve their goals (research, evaluation) and member agencies use ARJIS to achieve their goals (obtain more operational dollars, new technology)\textsuperscript{49}.

**IJIS facilitate communication among different communities & groups**

Integrated criminal justice information systems are organizational and technological ensembles created to facilitate the communication of criminal justice information among government, criminal justice agencies, and other interested communities through the integration of heterogeneous information systems. There are many different communities involved in the work of criminal justice and their work is distributed, idiosyncratic, and asynchronous. For example, when a patrol officer responds to a call or otherwise interacts with the civilian population, she completes a Field Investigation (FI) report documenting the interaction that gets entered into the ARJIS mainframe database. At some later point crime analysts will use the data within the ARJIS mainframe (including the data from all the FIs) to identify and analyze trends in crime for their local jurisdictions. The reports produced by the crime analyst are then used by operational planners to allocate resources (such as the patrol officer). And, a concerned citizen may see the incident captures in the officer’s FI on a crime map of their neighborhood generated on the ARJIS public website.

\textsuperscript{48} See http://www.recovery.gov/

\textsuperscript{49} It has been suggested by members of my dissertation committee has suggested that this example may not be appropriate because boundary objects can work horizontally across social worlds. My review of the literature does not support that argument. Further, there are certainly social worlds that are connected vertically – management and labor for example. Even if one accepts the position that boundary objects only operate horizontally, the example in the text is still valid because the member agencies of ARJIS and the funding agencies, though at different levels of government, are not vertically linked in any way. In other words, the National Institute of Justice does not have authority over Carlsbad Police Department to any degree beyond that which is instantiated in specific funding contracts into which both parties enter voluntarily.
Different communities interact with IJIS in different ways

IJIS exhibit the rigidity/plasticity characteristics of boundary objects. IJIS exist independent of any particular community that interacts with them; while at the same time the different communities that interact with the IJIS can do so in ways unique to that particular community. ARJIS and JNET both exist as agencies. However the ways in which particular institutions varies. For example, the public interacts with ARJIS in different manner than the law enforcement community; and because they can do so, the two communities are able to communicate and collaborate through ARJIS. This example and others are discussed in greater detail later in the chapter. For the moment, it is important only to understand that IJIS exhibit the duality characteristic of boundary objects.

IJIS: Terrain with Coincident Boundaries

The type of boundary object that best describes integrated criminal justice systems is the terrain with coincident boundaries object (hereafter referred to as the terrain type of boundary object) because the content of the IJIS can vary for each community that intersects with the IJIS. Specific components of IJIS can, perhaps, be better described by one of the other types of boundary objects. For example, the ARJIS mainframe is clearly a repository type of boundary object. However, only the terrain type of boundary object is abstract enough to capture the essence of an IJIS in its entirety.

The terrain type of boundary object also is the type that most describes an IJIS for two reasons. One, an IJIS facilitates both autonomous work and collaborative work using the same referent. For example, robbery detectives make regular use of ARJIS as part of their investigatory duties. These detectives, working autonomously, use the ARJIS mainframe and other data sources to query stolen property, similar crimes, and victim information. They also work collaboratively, sharing information about their cases on a robbery detective electronic
mailing list. Using the mailing list provided by ARJIS makes it much easier for robbery detectives to collaborate on overlapping cases.

Two, an IJIS allows the resolution of different goals among the different communities of practice. For example, the JNET system itself facilitates the resolution of different goals for policymakers and law enforcement practitioners. For policymakers, when JNET contributes to the successful resolution of a criminal justice matter or draws positive attention to the state, they are able to tout JNET as evidence of their positive work, or as support for further policy goals as demonstrated by this press release:

"The impact [of cutting the JNET budget] would be real and disastrous and would only help criminals," said the Governor. "Police officers would not be able to get real-time information about outstanding warrants, stolen property, or protection from abuse orders. When responding to domestic violence calls, for example, this lack of information will put troopers and victims' lives in danger.

"Cyber security activities would be crippled and citizen data would be at unacceptable risk of hacking. Criminals who have been arrested or have outstanding warrants could slip through the cracks because troopers would not have in-car, real-time intrastate information. This is of particular concern in Philadelphia where the metro area makes it easy for criminals to flee across state lines.

"Additionally, honest and innocent people would be affected," added the Governor. "People with names that match those of wanted criminals could be subject to false arrest because troopers may not have ready access to PennDOT photographs or they could be detained longer than necessary while their fingerprints are processed. And the background checks that many rely on for jobs, doing volunteer work, and buying guns for hunting or self-protection could be delayed."

For law enforcement practitioners, JNET facilitates the resolving of normal operational goals (e.g., catching criminal, performing investigations) but also strategic goals such as improving

officer safety in the field. Though different, JNET facilitates the achieving of both the policymaker’s and the law enforcement practitioner’s goals.\(^{52}\)

I have outlined how IJIS exhibit the properties of a *terrain* type of boundary object. I will now discuss how ARJIS and JNET exhibit these same properties in greater detail.

**ARJIS**

Two elements of ARJIS – the ARJIS mainframe\(^{53}\) and the ARJIS governance structure – are particularly demonstrative of how ARJIS exhibits the properties of a *terrain* type boundary objects. Both the ARJIS mainframe and the governance structure allow law enforcement, government, and the general public to work autonomously while also providing a common referent for collaboration.

**The ARJIS Mainframe**

The ARJIS mainframe database is an element of ARJIS that spans the boundaries of government, law enforcement and the general public. The ARJIS mainframe has the same boundary for all three communities the system itself. External to the boundary are the communities, internal to the boundary is the content contained within the system – and that is where the variance occurs for these three communities as they engage the mainframe.

For the various member and non-member criminal justice agencies that use ARJIS, the ARJIS mainframe database is the primary regional resource for criminal justice data. All

---

\(^{52}\) I note that both policymakers and law enforcement practitioners have multiple sets of goals. I have only chosen the two sets discussed in the example to demonstrate how different sets of goals by different communities are able to be resolved through an IJIS. I also note that though these two sets of goals are different, they are at least implicitly mutually supportive. When law enforcement practitioners are able to successfully achieve their operational goals such as preventing or solving crimes the result gives political prestige to policymakers who can claim that their policy actions led to the successful results in the field.

\(^{53}\) The ARJIS mainframe database is also, of course, a prototypical *repository* type of boundary object as well. What I will argue later in this chapter is that the *repository* type of boundary object is a subset of the *terrain with coincident boundaries* type of object with its own unique properties (indexed, modular) but also inheriting the properties of the super-class.
criminal justice data from the member agencies are entered into the ARJIS mainframe. However the ARJIS mainframe database fulfills different needs both within and across the different agencies. The ARJIS mainframe database itself allows for the resolution of the different goals of the different agencies. For some member agencies, the ARJIS mainframe database acts as their only records management system. These agencies store all their data in ARJIS and the ARJIS system is their singular tool for criminal justice data storage and retrieval. For other member agencies, and for non-member agencies, ARJIS is a supplementary resource to be used in conjunction with their own internal records management systems. For these agencies, ARJIS is source of data from other localities which can be used to extend their own internal resources and a location to share their own data for mutual gain.

The information housed within the ARJIS mainframe database satisfies different informational needs for different user types. For patrol officers, the ARJIS mainframe is a source of information that they can access while in the process of responding to an incident. For the criminal analyst, the ARJIS mainframe database is a source of information for identifying crime trends in order to facilitate the formation of operational strategies (e.g., increasing patrols in an area that has seen an increase in burglaries). For investigators, the ARJIS mainframe database is a resource for making connections across cases such as identifying a common modus operandi or a vehicle that was reported in separate crimes.

As noted before the ARJIS mainframe database also provides the basis for collaborative work among these different user communities. Crime analyst reports are used both by management in operational and strategic planning, and by investigators trying to ascertain trends in crime related to their investigations. Similarly, investigators in different jurisdictions can query the ARJIS mainframe for similar crimes in other jurisdictions.
The ARJIS mainframe database is also an information resource for the general public; providing regional criminal data to the public citizens, but in manner fundamentally different from that of law enforcement. The public only has limited access to the data housed within the mainframe. The public accesses the mainframe from the ARJIS public web site and can generate tabulated crime statistics and maps of crimes within the region. However, the data is “scrubbed” to make it consumable by the public. The public cannot see the specific locations of where crimes occurred. They cannot access the victim’s name, or the reporter of the crime, nor are they provided the exact time of the crime. Instead, public is only presented cursory information about particular crimes – what types of crime are most common in particular areas, what areas crimes most often occur in, timeframes of crimes, and general locations of crimes. The data is different in another fundamental way: the jargon of the California criminal code is removed and crimes are listed in abstracted common language. For example, the California Penal Code has nine codes for the various types of sexual assault54. The crime mapping application gives lists two: ‘rape’ and ‘other.’

54 See http://law.justia.com/california/codes/pen.html
The public uses the data from the ARJIS mainframe differently from law enforcement as well. Unlike law enforcement agencies that use the data for strategic and operational purposes, the public uses the data to inform themselves about the region. Examples include the use of ARJIS data by the news media to supplement reports (Arner, 2006a), real estate agents using ARJIS data to demonstrate the attractiveness of a property they are selling (Fjellestad, 2009), and buttress arguments made in letters to the editor (McElroy, 2007).

The information the general public gets from the ARJIS mainframe can also be the basis for public communication to government about local concerns and vice versa. For example, newspaper reports that have relied on data from the ARJIS mainframe have spurred the public to

---

55 This is a crime map representing crimes committed in within 1 mile of the San Diego Zoo during the period of April 1, 2009 to May 31, 2009. The San Diego Zoo is a major tourist attraction for the city. Notice that, perhaps unsurprisingly, the majority of crimes committed in this area are theft-related (e.g., robbery – orange diamond, theft – yellow circle, vehicle break – green oval, and vehicle theft – purple square).
express their concerns about the level of crime in Chula Vista (Branscombe, 2005) and a law to prohibit some sex offenders from being classified as transient (Arner, 2006b).

Local and regional government bodies make use of the ARJIS mainframe as well. For government, the ARJIS mainframe is both an analytical tool and a communication tool. Working in conjunction with ARJIS another division of SANDAG – the Criminal Research Division (CRD) – analyzes data contained within the ARJIS mainframe, and from other resources such as the National Crime Information Center, to produce reports. These reports serve at least two functions for SANDAG. One, these reports serve to inform and guide public policy. Members of SANDAG are able to use the reports to form law enforcement/public safety strategies to be applied to their own jurisdictions and to coordinate activities on shared problems. Two, SANDAG is able to use the reports to communicate to the public information about crime in the San Diego region and where possible, emphasize SANDAG’s effectiveness in combating crime.

For example, in April, 2009, the CRD released a report analyzing and summarizing crime trends for the prior 25 years ending in 2008\(^56\). In addition to a detailed discussion of regional trends in different categories of crime, the report also stresses the benefit of the ARJIS mainframe data to tout the benefits SANDAG provides for the citizenry. The introduction to the report states:

\textit{SANDAG is the only local entity to compile these statistics across the 18 incorporated cities, as well as the unincorporated areas of the county, making this information some of the most frequently requested from SANDAG’s Criminal Justice Clearinghouse. These data are useful to local law enforcement, policy makers, and the community in tracking}

\(^56\) The timeframe of the report roughly coincides with the time the ARJIS mainframe became operational and began housing criminal justice data for the region.
public safety over time, as well as the effectiveness of prevention and response efforts on regional crime rates.

Note how this paragraph emphasizes the benefit of the ARJIS mainframe data to both the public and to government. The latter is stated outright. The former is implied by stating that the data is some of the most requested information from the Clearinghouse. Of course, the report is also useful for informing the public about current crime patterns within the region and for, where possible, emphasizing decreases in crime or increases in law enforcement effectiveness.

**FAST FACTS**

- In 2008, both the violent and property crime rates for the San Diego region decreased and were at 25-year lows (4.09 and 28.79, respectively, per 1,000 residents).
- There were 90 homicides in the San Diego region in 2008, the third lowest number in the past 25 years.
- After five consecutive increases, the number of robberies decreased eight percent in 2008, compared to 2007.
- While the number of burglaries that involved entry through an open or unlocked door or window declined in 2008, the number involving forced entry increased 12 percent from the previous year.
- Motor vehicle thefts decreased 18 percent from 2007, more than any other property crime. However, thefts of motor vehicle parts increased 9 percent.
- Firearms were used less frequently in both robberies and aggravated assaults in 2008, compared to 2007.
- According to preliminary statistics, there were 118 hate crime events reported to local law enforcement in 2008.

*Figure 10-3 "Fast facts" from a report generated using ARJIS data.*
To summarize, the ARJIS mainframe serves the needs of multiple constituent groups. Different types of criminal justice agents and organizations, the government, and the general public all use the ARJIS mainframe to work autonomously to solve their own goals. The ARJIS mainframe acts as a common referent upon which to base collaborative work among the different communities.

The ARJIS mainframe is one component of ARJIS that allows ARJIS to function as a boundary object. Another is ARJIS’s governance structure through which different communities are able to communicate and collaborate on common goals.

**ARJIS Governance**

For the member agencies of ARJIS, the ARJIS governance structure serves multiple purposes. At the working group level, the ARJIS governance structure is mechanism for resolving competing and complementary technical and business needs such as differences in crime codes or needs for specific applications. As discussed in Chapter 7, representatives from the ARJIS member agencies participate in these working groups to resolve the technical issues and business needs of ARJIS and to present their own internal needs to ARJIS for consideration.

For senior law enforcement executives of the member agencies and for the ARJIS staff, the Management Committee is a location to collaborate on regional problems, politically network, and engage in oversight of ARJIS. Examples of the types of activities engaged in at Management Committee meetings include: resolving budget issues, receiving comments from the public, receiving status updates on current initiatives and programs, coordinating grant writing, receiving updates from the working groups, and providing guidance on system development. The November 3, 2004 committee meeting provides an excellent example of how senior executives collaborate and engage in oversight of ARJIS:
Assistant Sheriff [SDSD] believes the more the better on the law enforcement side. He is not sure what purpose of giving the call for service information on the public side.

John [SD DA’s OFFICE] stated the more information given to the public to explain what the police are doing is helpful.

Assistant Sheriff [SDSD] stated that a call for service does not mean a substantiated crime.

Chief [CORONADO PD] wanted to make sure no addresses were given on the public side.

Chief [CARLSBAD PD] agreed with Chief Hutton in not giving out addresses. He feels that this just hands over information to the bad guys.

Julie [SD DA’S OFFICE] explained that the idea of calls for service was to inform the community what the police are doing and stopping unnecessary calls to the department.

Pam [ARJIS DIRECTOR] stated that ARJIS has not had a legal opinion provided yet on calls for service being made available to the public. Pam Scanlon stated that the law enforcement side would be done first. At a later date, a filter could be done if some selected call for service information was approved to be released to the public side.

Chief [OCEANSIDE PD] stated that no one in Oceanside seems to want this information (on the public side). If asking for ARJIS-wide, he would say no.

Chief [CORONADO PD] wants more discussion on this. He feels it puts pressure on other departments if one department does and one doesn’t.

Upon a motion by Chief [OCEANSIDE PD] and a second by Chief [CARLSBAD PD], the Management Committee unanimously approved to table the issue of sharing information on the public side and to bring back for a vote at the next meeting.

In this example the senior managers are discussing how the public crime-mapping application should be developed. The chiefs are advocating for both their individual jurisdictions and as law enforcement agents with a common mission. For example, the chief of Oceanside PD states “Nobody in Oceanside seems to want this [information].” And the chief of Coronado PD, the chair of the Management Committee, is concerned that providing certain information only helps “the bad guys.” Through the same discussion, the ARJIS staff communicates their design rationale and the current status of the design process as well as future design options. The result
is that both senior managers and ARJIS staff become aware of each other’s views on the design of the public crime mapping application.

The public also receives information from law enforcement and the government via the Management Committee and Public Safety Advisory Committee meetings. Schedules, agendas, and minutes are published on the SANDAG website. The PSAC publishes a newsletter – the *PSC Dispatch* – that highlights key PSC activities and accomplishments on the public’s behalf; and this is also made available digitally via the SANDAG website. To summarize, through civic participation and digital communication, the public is able to communicate with law enforcement practitioners and policymakers via the top-level committees in the ARJIS governance structure.

The government interacts with the ARJIS governance structure through the PSAC. The PSAC is both a component of the SANDAG governance structure and the top-level authority in the ARJIS governance structure. The PSAC fulfills a number of informational needs for members of government. One it allows policymakers to be apprised of current ARJIS activities and critical issues and to resolve any outstanding matters of ARJIS policy. For example, at the March 16, 2007 PSC meeting policymakers were informed of the following:

- ARJIS committee members and legal advisers were reviewing the potential impact of the California Public Records Act on ARJIS operations and policies
- ARJIS had received an additional grant from the Department of Homeland Security to extend the State, Regional, and Federal Enterprise Retrieval System project
- ARJIS is working to resolve privacy issues in interstate information sharing

Committee members are not passive recipients of the status updates from ARJIS. Rather committee members regularly inquire about particular issues related to the topic or make
recommendations based on their policy interest. The March 20, 2008 meeting of the PSAC gives us an example of this process:

Pam [ARJIS DIRECTOR] stated that ARJIS has accomplished several deliverables such as the needs assessment, business case and architecture for Enterprise ARJIS, network upgrade, and several web-based applications such as crime stats and crime maps. ARJIS is working with the Sheriff’s Department with generic interfaces which will allow us to get information into ARJIS as near real time as possible. All this work has enabled our technical team and participating agencies to become familiar with products and technologies that are out in the market and see how these technologies meet and enhance our business needs. We need to ensure we meet our objectives. The technologies rolling out will support our agencies for officer and public safety. Pam introduced Robert (ABC Consulting). Robert presented an overview of the work completed to date and the upcoming deliverables for 2009.

David [COUNCILMEMBER - NORTH COUNTY COSTAL] inquired on the timeline and funding challenges, if any.

Pam [ARJIS DIRECTOR] stated ARJIS is doing quarterly and/or every six months roll out components. The critical dependencies will be tied in. The first piece is the portal which will be presented today. ARJIS is working with the Sheriff’s Department on mapping all data and learning the business processes. ARJIS provides all the mandated Uniform Crime Reporting (UCR) FBI recording. This is done in components and ARJIS will be coming back to the committee upon every phase completion. The funding available is the $11.6 million in reserves that is dedicated for this project. The consultants have informed ARJIS that $12 to $17 million may be needed, so we are leveraging existing infrastructure as much as we can with the funds available.

Robert [ABC CONSULTING] noted the six month increment is critical so we can gauge how to move forward with the most effective services. As we hit the funding limit, ARJIS should have 80 to 90 percent of Enterprise ARJIS completed.

David [COUNCILMEMBER NORTH COUNTY COASTAL] replied that it is building as you go verses buying something on the shelf. He inquired if other counties, federal, or state levels are doing it this way?

Pam [ARJIS DIRECTOR] stated ARJIS is using all state and federal standards. ARJIS is the standards bearer for this region and is working closely with the FBI and the Department of Justice. Where we can, we are going off the shelf. We want to limit the customization as much as possible. We are on the forefront. ARJIS is the first in the
nation and continues to be the model. ARJIS is using open-source software and hardware.

Vice Chair [CORONADO PD] stated that since there are new members on this committee today that perhaps Ms. Scanlon could describe how long we’ve been on the current platform and how long we’ve been working towards the new generation.

Pam [ARJIS DIRECTOR] stated the core system has been on the mainframe since 1981. It is the same mainframe that the City of San Diego is using. It is critical for ARJIS to get off the mainframe and have throughout the years been pulling pieces off and using the Web. It is all Web-based. ARJIS is using FBI, National Crime Information Center (NCIC), and all Cal DOJ standards. ARJIS has a strong team and strong participation from all participating agencies that make up the Core Working Group. ARJIS has eight different committees with heavy involvement with police officers, investigators, and support staff to make sure what we have is what we can use. ARJIS also has oversight from the Chiefs’/Sheriff’s Management Committee.

Robert [ABC CONSULTING] commented that the solution that is being built relies on the off-the-shelf tools. The things that ARJIS needs to build are the things that represent the business knowledge that are specific to ARJIS and the stakeholders here. That’s a key element of the justice reference architecture.

David [COUNCILMEMBER NORTH COUNTY COASTAL] asked if privacy standards have been established that only the right people get access to the information.

Pam [ARJIS DIRECTOR] stated that ARJIS is one of the first to do a Privacy Impact Assessment (PIA). ARJIS is working with the General Counsel at SANDAG regarding the handhelds we are using and Information Data Sharing MOU. ARJIS is very conscious regarding privacy from both the public records requests and types of data and how it is protected.

Theresa [COUNCILMEMBER NORTH COUNTY COASTAL ALTERNATE] asked if the system will need to be down for any period of time while data is transferred and if the end user will know when it is happening.

Robert [ABC CONSULTING] stated it will not be down. That is one of the key roles of the middleware product. It will continually move information real-time. We want to get away from nightly downloads, etc. The end user won’t see it happening.

The informational flow within the PSC is not only between government representatives and ARJIS or from the public to the government, but also between members of the government from different jurisdictions. PSC meetings regularly serve as a location for representatives of different
jurisdictions, or from different levels of government to communicate their specific issues to the other policymakers on the committee. At the May 19, 2006 meeting, for example, a representative of the federal government addressed the PSC:

"Bill from the Congressman’s office addressed the Public Safety Committee regarding the utilization of military assets in conjunction with emergency preparedness of the County. A meeting will be held in August with attendance encouraged from every major command in San Diego including Pendleton, Miramar, and North Island, as well as public safety agencies throughout the region to develop an emergency preparedness protocol in San Diego as it relates to military support."

This example shows how policymakers from different levels of government are able to communicate through the PSC medium and coordinate their efforts in preparing for emergencies. Another example demonstrates how members of different local jurisdictions use the PSC forum to communicate about issues of common relevance:

Chris, a staff member for Assemblyman of District 77, provided information related to Assembly Bill (AB) 4, which proposes to increase the hours of operation and coverage of the transportation District 11 office in San Diego. The Mayor requested a copy of AB 4 for review and recommended that it be forwarded to the SANDAG Board for review. Diane [SANDAG Deputy Director] indicated that she would have the legislative staff carry it through the legislative process here at SANDAG.

In this example we see how a member from on jurisdiction is able to communicate and collaborate with a member of another jurisdiction about an issue of common interest while third policymaker communicates how SANDAG will administrate the process.

I have shown how different facets of the ARJIS technological and organizational infrastructures serve in a boundary-object capacity to facilitate communication between the regional government and law enforcement, the regional government and the public, and law enforcement and the public. Additionally I have show how the organizational structures
specifically allow for bi-directional information flow among the different communities. I will now highlight the ways in which JNET exhibits similar properties.

**JNET**

The JNET system is comprised of many components, but one component, more than any other, reflects JNET’s boundary spanning properties: the enterprise portal. The enterprise portal is the entry way to all the JNET applications and back-end systems. All work using JNET is done through the enterprise portal. For this reason, I will focus on the enterprise portal in this portion of the discussion.

**The JNET Enterprise Portal**

The enterprise portal application facilitates autonomous work and collaboration on a across referent by providing different content to different user groups based on access roles. As with the ARJIS mainframe, there are a variety of user communities that make use of the enterprise portal that resolve their individual goals and also collaborate using the enterprise portal.
All JNET users access the JNET system through the enterprise portal, but the content of the portal varies by user community. The content accessible through the portal is determined by the user’s occupation (e.g., law enforcement officer, medical examiner) and their JNET roles (categories of access assigned by the local JNET registrar). The result of this configuration is that the content can vary significantly both across and within occupations.

For example, in Table 15 are the systems a law enforcement officer and medical examiner can access through the portal:

<table>
<thead>
<tr>
<th>System</th>
<th>Law Enforcement Officer/Investigator</th>
<th>Medical Examiner</th>
</tr>
</thead>
</table>
| WebCPIN (photos) | - Booking photos  
- Offender demographics  
- Criminal charges  
- Missing & wanted person posters | - Booking photos  
- Missing & wanted posters |
| PennDOT | - Driver’s photo/history | - Driver’s photos/history |
| Records (Dept. of Transportation database) | - Certified driver records  
- Registrations  
- License orders  
- Driver’s License card design update |  
JNET CLEAN (PSP database) | - PA and out-of-state rap sheets  
- Wanted persons  
- Out-of-state vehicle/driver records  
- Stolen vehicles, guns, articles, boats, securities  
- Gang association  
- PennDOT records  
- Protection from abuse information | - PA and out-of-state rap sheets  
- Wanted persons  
- Out of state vehicle/driver records  
- Stolen vehicles, guns, articles, boats, securities  
- Gang association  
- PennDOT records  
- Protection from abuse information |  
Warrants | - Federated warrant search | - Federated warrant search |  
Juvenile Watchlist | - Juvenile court information | NO ACCESS |  
Notifications | - Real-time notification on arrests, wants/warrants, change of address (PennDOT), sentencing, case bind over, dispositions, parole violations, traffic and non-traffic citations | - Real-time notification on arrests, wants/warrants, change of address (PennDOT), sentencing, case bind over, dispositions, parole violations, traffic and non-traffic citations |  
Justice Data | - Constable/sheriff’s deputy query  
- DPW recipient address query  
- Electronic reporting  
- Flexible search  
- Master charge code  
- Protection from abuse  
- Search by state ID  
- State ID/Offense tracking number lookup | - Electronic reporting  
- Master charge code  
- Search by SID  
- SID/OTN lookup |  
Court Information | - Hearing schedules / case disposition lookup  
- Magistrate District Judge docket sheets  
- Pre-sentence investigation  
- Unified justice system portal | - Hearing schedules / case lookups  
- Pre-sentence investigations  
- Unified justice system portal |  

Table 10-3 Comparison of two JNET user roles.
Note the differences in available content for both the Medical Examiner and the Law Enforcement Officer. The officer has a much greater level of access to available content than the examiner. Some systems that the officer can access are simply not provided to the medical examiner. In almost all of the systems, the law enforcement officer has access to information that the medical examiner does not.

Even among law enforcement officers the content varies depending on the role. Consider the “Criminal History User” role for example. The Criminal History User role is the role from users from criminal justice agencies with one exception. A user assigned a “Criminal History User” role has full access to the content of JNET, while a “PA Criminal History User” only has access to information related to Pennsylvania. Users assigned the “Criminal Justice User” role have even more limited access until they are certified by the Pennsylvania State Police to access the CLEAN system.

Designed this way, the enterprise portal inherently provides different content to different user communities as defined by their user roles in JNET policy. The enterprise portal also allows different communities, defined organizationally, to work autonomously towards their separate goals. As the JNET website notes:

*Police use JNET to access criminal history records information and to assist in investigations. The Department of Corrections uses JNET to keep inmate records current. The PA Board of Probation and Parole accesses JNET to track offenders’ activity throughout the criminal justice system with real time JNET notification alerts. The FBI and other federal agencies access JNET for criminal history records information and to assist in investigations. Magisterial District Judges use JNET to access statewide Administrative Office of PA Courts' information.*

---

57 The one exception is that individuals from the PA Department of Public Works Bureau of State Children and Youth Programs can qualify for the Criminal History User role.
These criminal justice institutions are all using the enterprise portal for different, uniquely defined needs. However, because these communities are interconnected and interrelated, they are also able to collaborate using the enterprise portal when necessary. The previous quote shows us how this occurs. For example, the criminal history that the police officer accesses through the enterprise portal is a product of the work of the police who initially arrested the subject of the record, the court that convicted him, the information entered by the department of corrections during incarceration, and the status of the parolee or probationer upon release into society; all of which is accessed through the enterprise portal by the respective parties.

In sum, the JNET enterprise portal presents varies communities – whether defined institutionally, or in terms of user rights, or work responsibilities – different content that can be used by those communities to work autonomously to resolve different goals and to collaborate on common goals. Because JNET is more centralized and less collaborative, its organizational features do not exhibit the same boundary-spanning properties as ARJIS’ organizational features. Nonetheless, JNET retains the properties of a terrain with coincident boundaries type of boundary objects.

Conclusion
In this chapter I described two IJIS, ARJIS and JNET, and how they function as boundary objects among multiple stakeholder communities. The different communities engage the central IJIS in ways unique to their needs while at the same time recognizing the common IJIS. Because of the complexity of IJIS, many different types of collaborations can occur through them. Some of the types I have presented here include sharing and storing of information, providing and obtaining funding for criminal justice application, and communication about policy among policymakers, practitioners, and the general public. These
findings indicate that systems as complex as IJIS are likely to be ensembles of boundary objects. The particular properties the IJIS takes on as a boundary object reflect the nature of the interaction with any particular community. The example of how the ARJIS mainframe is different for the general public and for law enforcement officials makes this clear. What the data presented here cannot tell us is how the IJIS is understood from the individual communities’ perspectives or whether particular types of boundary objects may be more or less ideally suited for particular types of interactions. I discuss this limitation in greater detail in the next chapter.

Repositories, ideal, and forms and labels are subtypes of the terrain with coincident boundaries object

The terrain with coincident boundaries type of boundary object describes ARJIS and JNET most completely. This finding echoes that of Fleischmann and his study of dissection simulators (Fleischmann, 2006a, 2006b). Both ARJIS and JNET incorporate forms and labels, repositories, and platonic type boundary objects within their ensembles. But none of those types of boundary objects describe ARJIS and JNET, and IJIS in general, in their totality. Only the terrain type of object does.

In conducting this analysis I have come to the conclusion that when describing complex systems, the terrain with coincident boundaries type of boundary object encompasses the other identified types of boundary objects. Standards and labels, repositories, and platonic objects are a subset of objects of the terrain with coincident boundaries object. In complex systems like IJIS, the different internal content of such complex systems is the different repositories, standards and labels, and platonic objects arranged within the ensemble.

I argue that the other types of boundary objects are a subset of the terrain type of object for two reasons. One, the terrain object is abstracted to a level beyond the other types of
boundary objects. To define the *terrain* object as a commonly bounded object with variable content is, in my view, to make it all-encompassing, to an extent that it could possibly be argued that the terms boundary objects and terrain with coincident boundaries are redundant.

Two, it seems difficult to see how, for example, a *platonic* object that removes local idiosyncrasies could simultaneously contain locally idiosyncratic content. Similarly a standard with variable content would clearly seem to be an oxymoron. One could see how a *repository* could also exist as a *terrain* object – libraries contain different content for children than they do for adults for example. Given that the other *platonic* and *standards* objects cannot logically be terrain type objects, it seems clear then, that the terrain type of object supersede the other three types.
Chapter 11 Implications and Future Directions

Introduction

I conclude this dissertation with a three-part discussion. In the first part I summarize the contributions this research makes to both scholarship and professional practice with special attention paid to the implications for criminal justice. In the second part I discuss the theoretical and practical implications of this research. Finally, in the third part I detail the need for future research to address the inherent limitations of this research.

Contributions to scholarship

Through this research I make three scholarly contributions. One, I contribute to organizational identity scholarship by providing empirical evidence of the influencing role of organizational identity on the design and arrangement of organizational ICT. Two, through this research I contribute to social informatics research by contributing further evidence of ICT as complex socio-technical systems and by demonstrating the utility of organizational identity as a tool for helping to “unpack” the socio in socio-technical. Three, this research makes a limited contribution to boundary objects research by showing that IJIS act as boundary objects among multiple constituent communities.

Extension of organizational identity to the design and arrangement of ICT

This research contributes to organizational identity scholarship through its application of organizational identity theory to the study of the design and arrangement of IJIS. Until very recently (c.f., Tripsas, 2009) the influence of organizational identity on organizational technologies has been largely overlooked. I have shown that while sharing, at a broad level, very similar organizational imperative (facilitating the sharing of criminal justice information), differences in the identities of ARJIS and JNET have shaped their organizational practices and technological configurations resulting in significant differences in overall design. In doing so
this research provides further insight into “how organizations in various situations, choose what they want to be similar and what they want to be different (Ravasi & van Rekom, 2003).” To this end, this research realizes Brown’s (2001) anticipation that core identity attributes are linked to the strategies deployed by organizations.

**Contribution to social informatics**

Through this research I make a second scholarly contribution, a contribution to the social informatics perspective, in using organizational identity theory as a tool for unpacking the social context surrounding the design and use of information and communications technologies. This contribution continues the long established, yet still useful, practice of drawing on theory from other domains in order to achieve greater insight into the design and use of ICT (Orlikowski & Barley, 2001). Social informatics scholars now have a new theoretical lens with which to use in trying to unpack the complex nature of socio-technical systems. Social informatics scholars are likely to find utility in the recursive relationship among organizational identity and organizational attributes; and, in the concept of ICT as expressions of the identity of organizations. Also, organizational identity theory’s close ties to institutional and structurational theory are likely to appeal to socio-technical scholars currently engaged in those theoretical spaces.

**Extension of boundary objects theory to organizational level of analysis**

I make a third, limited, scholarly contribution through this dissertation via my application of boundary objects theory to the organizational level analysis. Prior boundary objects research has focused on the creation of artifacts – drawings, presentations, memorandums – to facilitate collaboration among different groups. But there are organizational-technological ensembles that emerge (ARJIS) or are created (JNET) to facilitate collaboration among groups; and I have
shown that IJIS are boundary-spanning objects through which collaboration and communication occur.

**Empirical contributions**

Through this dissertation I make two empirical contributions. One, I add to our knowledge and understanding of integrated criminal justice information systems. Two, I add to the, to date, limited body of empirical research on organizational identity. I will now discuss each contribution in greater detail.

*Expanded our knowledge of integrated criminal justice information systems*

The body of empirical research on IJIS is relatively small and much of what is available is prescriptive in nature. This research extends our knowledge of IJIS in two ways. First, this thesis provides a detailed empirical accounting of two of the exemplar IJIS currently in operation. The ARJIS and JNET case studies presented in this thesis provide a detailed picture of the origins, presents, and futures of both IJIS.

Second, the findings from this research increase our understanding of these systems by comparing and contrasting the organizational and technological characteristics of ARJIS and JNET. IJIS are being developed all over the United States, yet we a minimal understanding of the similarities and differences among the various initiatives. In order to achieve anything close to large-scale integration (e.g., super-regional or national), it is critical that we identify the ways successful systems like ARJIS and JNET are alike and are different so that we may develop strategies to capitalize on common ground and overcome the barriers resulting from design differences. This research contributes to that goal.
Added to the body of empirical research on organizational identity

As noted previously in the review of the literature on organizational identity, most of the work on organizational identity has been theoretical, and the lack of empirical research on organizational identity is considered to be a key issue for organizational identity scholars (Ravasi & van Rekom, 2003). This research makes an empirical contribution to organizational identity research through the two case studies, and thereby makes a contribution to redressing the theoretical/empirical imbalance in organizational identity research. In particular, the linking of organizational identity to the design and arrangement of organizational ICT provides further evidence of the importance of accounting for organizational identity in trying to understand organizational action. Also, by empirically linking organizational practice to organizational ICT, this research lays the foundation for future empirical and theoretical research on organizational identity which I discuss in greater detail below.

Implications

Implications for theory

Two implications for theory emerge from this dissertation. One, the relationship between organizational identity and organizational ICT is likely to be structurational in nature. Two, complex systems that function as boundary objects are best described by the terrain with coincident boundaries type of boundary object.

The relationship between organizational identity and organizational ICT is likely to be structurational in nature

One implication of this research is that the relationship between organizational identity and organizational ICT is structurational in nature, a possibility discussed in Ravasi et al. (2003). Whetten (2006) states that organizational attributes that reflect an organization’s identity represent “irreversible” commitments. While the evidence described in this dissertation does not

187
indicate that the ICT being created by organizations is irreversible, it does indicate that organizations are highly invested in their ICT as a manifestation of their identities. This high level investment indicates that it would be very difficult for organizations to discard prior ICT commitments in favor of new ones that are inconsistent with their espoused identity. In other words, while organizational ICT reflect organizational identity only as long as organizations continue to enact them, breaking that commitment will be very difficult because the ICT are tied-up in who the organizations are. This implication would appear to be supported by recent research that found that organizational identity not only binds organizations to technological commitments, but filters the organization’s very perception of what technologies might be appropriate (Tripsas, 2009).

**Complex systems are best describes as terrain with coincident boundaries objects**

An implication of this research is that of the four types of boundary objects only the *terrain with coincident boundaries* type is conceptually capable of describes complex systems such as organizations. Organizations, and in particular integrated criminal justice organizations with their inherently boundary-spanning nature do serve in a boundary object capacity and contain different types of boundary objects within them. That content can include the other types of boundary objects – symbols, standards, and repositories. This suggests, perhaps, that we should treat the *terrain with coincident boundaries* type of object as meta-boundary object that can include the other previously identified types.

Additionally, the fact that complex systems can be or contain any and all of the types of boundary objects implies that the actual type of the boundary object may be less relevant than the uses and negotiations that occur around the boundary object. It may be enough to simply identify something as a boundary object because it is not clear the additional insight that is
gained from labeling the object as a standard rather than a symbol when conceptually the two do not appear to be substantially different. This implication is consistent with recent work on boundary objects by scholars such as Lee and Lutters & Ackerman (2007; 2007) who have emphasized the role of boundary objects in the forming of and negotiation of boundaries.

**Implications for practice**

*Organizational identity both enables and constrains the design and arrangement of organizational technologies and processes*

One implication of this research for IJIS those engaged in professional practice is that the identity of the organization of the IJIS will serve to both enable and constrain their design decisions. For those managers and policymakers just embarking on the creation of a new information system for their organization, it is important that they try to align the systems they would like to have with the type of organization they would like to be. Is the organization to be a collaboratory or a broker? Are the systems to be distributed or federated? The answers to these questions will shape the design of both the organizational and technological components of the IJIS.

For IJIS practitioners already engaged in managing and growing an established IJIS, they must attend to “who they are” as an organization when deciding on what new systems or technologies they are going to incorporate into the existing infrastructure. IJIS professionals are likely to find that systems that align with the identity of the organization are more easily adopted and ultimately more successful; while those that do not align are likely to be ill-fitting and little used.

*IJIS design requires attention to the boundaries that will be spanned*

As shown earlier, IJIS act as boundary objects among multiple communities. The very purpose of IJIS is to transcend organizational, institutional, and technological boundaries to
facilitate information sharing. Therefore, designers and administrators of IJIS would be well served to identify and understand the communities they seek to integrate and the nature of the boundaries that separate them. Attention to these details will allow system designers and managers to implement the appropriate systems, architectures, policies and processes for spanning the types of boundaries the IJIS is intended to transcend.

**Implications specific to Criminal Justice & Policing**

The main implication of this research for criminal justice and policing is that large-scale integration of criminal justice information systems is likely to provide a difficult, if not impossible policy-goal to achieve. As discussed in Chapter 2, criminal justice agencies have a highly provincial outlook towards their ICT and data. “Turf” issues pertaining to control of data and access to data have and continue to act as impediments to integration efforts. And, as demonstrated in the case of JNET, these issues can play a major role in the ultimate identity the integration effort assumes. Criminal justice policymakers should expect that IJIS initiatives will assume identities that resemble many aspects of the institutional environments they serve. As these IJIS become established and more entrenched in their identities, it seems clear that attempting to integrate the integrators and realize a fully integrated criminal justice information system covering all levels of government may simply be an unreachable goal.

**Organizational traits such as identity will inhibit large-scale integration of organizational ICT**

The impact of organizational identity on the design of IJIS in conjunction with broader institutional issues such as local norms, regulations, and values will continue to make large-scale integration very difficult. Policymakers, instead of devoting resources to a top-down integration strategy, should instead focus resources on integrating at the local and state levels and building upon those successes. As part of this strategy, when looking for systems to integrate at higher
levels – such as among states – should look for IJIS that align in terms of their identity. For example, policymakers should look for other IJIS who identify themselves as state-level brokers to integrate with JNET; and when looking for IJIS to integrate with ARJIS, they should look for IJIS with a local, collaborative, and law enforcement identity. Conversely, an attempt to integrate ARJIS and JNET with their different identities will likely prove very difficult.

Limitations and need for future research

There are at least three limitations to this research that can be addressed with follow-on work. One, my decision to focus on the identities of the IJIS organizations exclusively precluded me from gaining insight into identity-related interactions among the IJIS and their various stakeholder groups. These stakeholder groups play important roles in, and exhibit considerable influence on both ARJIS and JNET (and I suspect this to be true for many IJIS). Therefore, in order to gain a more complete understanding of the IJIS’ identities, future research should look closely at the perceptions of, and interactions with, the stakeholder organizations.

Two, this research is limited to an understanding of ARJIS and JNET during the time it took to complete this research. For various reasons, I did not attempt to document historically the identities of ARJIS and JNET, and so this dissertation has little to say about how these identities were formed, or what changes, if any, the identities have gone through over time. Since I am arguing that there is a structurational relationship among organizational identity and technology, understanding the origins of the organization’s identity is of obvious importance. Rather than try and reconstruct the historical identity, the opportunity for the future is to begin studying and tracking the identity and technology of an IJIS over time, beginning in its infancy.

58 Two reasons are that many of the actors involved in the early formation of these organizations are no longer in the organizations, and there are epistemological issues involving the reliance on recalled perceptions.
Three, because I focused on the IJIS organizations themselves and their technological architectures, this research is limited to describing the IJIS as boundary objects and does not shed insight into the collaborations that go on around or through the IJIS. There is an opportunity for future research to explore how negotiation and collaboration occur “around the edges” of an IJIS which may also provide some insight into the organizational identity/image dynamic. To this end, Lee’s (2007) theory of boundary negotiating artifacts may indeed prove more insightful.

This research going forward

Building on this research and its contributions, I identify three streams of future research to emerge out of this dissertation. One stream is to further unpack the process by which organizational identity shapes organizational technology. In this research I have shown, at a relatively abstract level, how organizational identity shapes design practices resulting in particular ICT designs and configurations. I plan to continue to explore this process and try to identify the specific processes by which organizational identity is inscribed in technology. For example, I can foresee future research following the design of a new technological component of an IJIS from its inception to implementation; observing and tracking expressions of organizational identity commitments and their translation into design requirements (see Appendix G for a related discussion on lessons learned from this research).

The second stream is to explore the structurational relationship between organizational identity and organizational technology. This dissertation has shown how organizational identity shapes technology. Future research will explore how organizational identity is shaped by an organization’s technologies. For example, I suspect that radical technological change requires a parallel radical change to an organization’s identity, and a main research goal is to find empirical
evidence that this is the case. To do so would represent an important theoretical and empirical contribution.

A third stream of research that emerges out of this research is to study what happens to organizational technologies when organizations experience profoundly difficult situations. Having invested their identity in their technologies, do organizations, as Whetten (2006) argues, fall back on back on those technological commitments at times of crises or “fork-in-the-road moments?” ARJIS, for example, is undergoing just such a crisis as one of their primary members has stated it will not be honoring its financial commitment to ARJIS. I would like to follow ARJIS through this crisis and see how their organizational identity and technological commitments shape how they respond.
Appendix A – Initial Interview Guides

1) Initial Interview
   a) Background Information
      i) What is your position within (ARJIS/JNET)?
      ii) How long have you been in this role?
      iii) Were you with (ARJIS/JNET) prior to taking on this organizational role?
         (1) If so, what role were you in then?
            (a) What were your responsibilities?
      iv) What has been going on recently at (ARJIS/JNET)?
   b) Organizational
      i) Describe for me the organizational structure of (ARJIS/JNET).
      ii) How are the organizational and technological decisions made at (ARJIS/JNET)?
      iii) Who do you report to?
      iv) Tell me about the governance structure of (ARJIS/JNET).
         (1) Are there any legal documents that provide the basis for this structure?
         (2) What are the responsibilities of the governing bodies?
   c) Technology
      i) Tell me about the (ARJIS/JNET) infrastructure.
      ii) Describe (ARJIS/JNET)’s design process.
      iii) Does (ARJIS/JNET) develop technology in house or rely on COTS products?
      iv) Does (ARJIS/JNET) employ staff or contracted programmers?
      v) What communications infrastructures can users access (ARJIS/JNET) over?
      vi) What systems do you have in place for security?
   d) Organizational Identity
      i) If we were to meet randomly, and you wanted to tell me about the place you worked, how would you describe (ARJIS/JNET) to me?
      ii) List for me some adjectives that you would use to describe (ARJIS/JNET)?
      iii) What do you think is central to who JNET is as an organization?
      iv) Complete this sentence: (ARJIS/JNET) is _____________.
      v) How is (ARJIS/JNET) different from other IJIS?
      vi) What characteristics would a technology have to have in order to be consistent with who (ARJIS/JNET) is?
      vii) If you had to deal with an ambiguous situation, what guidelines would you use in order to make a decision about how to proceed?
      viii) Can you think of an example where (ARJIS/JNET) adopted/developed a system that didn’t seem to ‘fit’ with the organization?
   e) Boundary Objects
      i) Can you list for me ways in which different groups use (ARJIS/JNET) to communicate or collaborate?
Appendix B – Follow-up Interview Guides

I. ARJIS

a. Organizational Identity
   i. Based on my initial interviews I’ve derived some terms that were commonly used to describe ARJIS. I’d like you to rate them using the following scale: (1) Strongly Disagree; (2) Disagree; (3) Neither agree nor disagree; (4) Agree; (5) Strongly agree
      1. ARJIS is a center for regional collaboration.
      2. ARJIS is a service and technology provider for law enforcement.
      3. ARJIS is highly democratic.
      4. ARJIS centralizes information.
   ii. Elaborate on responses to identity components
      1. Examples of system design reflecting these identity commitments
      2. Examples of conflicts with identity commitments

b. Organizational
   i. Do you have any perception of how the agencies funding participation affects their overall participation? Do you see they behave in certain ways based on how they fund?

c. Technology
   i. Can you think of a project at ARJIS that was directed from the top (Management Committee) down?
   ii. Can you think of a project that was the result of collaboration by the member agencies?
   iii. When an agency proposes an addition or change to the ARJIS system and one or more other agencies do not want to implement it, what happens?
   iv. Do you know why the decision was made to go with Global Query?
   v. The mainframe is collecting this data from all the member agencies; this is a central characteristic of the technology. Can you think of any others about the organization or the system that make it central for the San Diego region?
   vi. When new applications are added, who normally does the programming or configuration of those applications?

d. Boundary Objects
   i. So let's say we're in the Business Working Group. I'm saying I want to do this pawn system, and Carlsbad doesn't. There's that disagreement there. Does it get resolved in the working group or does it get forward it on to the chiefs for resolution?
   ii. The standardization occurs through a working group? That's negotiated by member agencies who say we want to add this code make this change?
iii. What was the motivation for providing the crime data on the public website?

iv. You mentioned that you're working on a new one for law enforcement only. The data for the public website had to be scrubbed make it consumable?

v. Can you think of ways ARJIS as an organization, or the ARJIS technologies, allow the agencies who participate or use ARJIS, to communicate amongst each other in ways they would otherwise not be able to?

II. JNET
   a. Organizational Identity
      i. Based on my initial interviews I’ve derived some terms that were commonly used to describe ARJIS. I’d like you to rate them on a scale of 1 (low) to 7 (high) how much you think they describe JNET
         1. JNET is a developer of IT.
         2. JNET is an information broker.
         3. JNET is technologically progressive.
         4. JNET serves the Commonwealth.
         5. JNET is a state agency.
      ii. Elaborate on responses to identity components
          1. Examples of system design reflecting these identity commitments
          2. Examples of conflicts with identity commitments
   b. Organizational
      i. How do you think budget cuts are going to affect what JNET is doing going forward?
      ii. Would you say that JNET has changed from an organization in growth mode to an organization in stabilization mode?
          1. In what ways, if any, has this change affected JNET organizationally?
          2. Do you see a correlation between the degree to which JNET is embedded in the Commonwealth government structure and the stabilization of JNET as an organization?
   iii. Clarify some details on the Executive Order and Management Directive obtained in Interview 1
   c. Technology
      i. It seems there is a lot of customization going on with the COTS applications that JNET purchases, is this an accurate assessment?
      ii. How do you define scalable and agile when describing JNET’s technology?
iii. Has the stabilization of JNET as an organization affected JNET’s technologies in any way?

iv. Can you explain for me how the scoring matrix works?
   1. What distinguishes a critical project from a non-critical project?
   2. How do you measure alignment of a project with JNET’s plans?

d. Boundary Objects
   i. When I attended the User’s Meeting I noted a number of times that attendees used the forum to express their concern about policies and about features of the systems in place. How common is this?
   ii. Can you explain to me how the JNET user roles translate into different forms of system access?
      1. Who assigns these roles?
      2. What happens if I’m a user and I want to change my role designation?

iii. The Enterprise Portal provides different content to different users correct?

iv. Can you describe for me how users use the messaging system to collaborate?
Appendix C – ARJIS Applications

Master Operations Index (MOI11)

The MOI11 is the main query screen for the legacy mainframe.

Crime Analysis and Statistic Screen (CASS)

The CASS application is a statistic reporting tool used by crime analysts as well as other applications such as the crime mapping interface.

Global Query

Global Query is a federated query application that allows users to input a single query and sent it to multiple databases with results returned in a single, aggregated, format.

Crime Mapping

The crime mapping application is a web-based graphical information system for mapping criminal activity.

Domestic Violence Communication System (DVCS)

This application is a web application used for investigating domestic violence incidents.

COPLINK Detect

COPLINK Detect is a third-party application that allows users to conduct association queries – queries that attempt to find associations within the data (e.g., similar vehicles used in similar crimes).

Sex Offender Management System (SOMC)

This list was derived in part from information obtained in (Mitretek Systems, 2006)
This application is used to by agency workers to manage sex offender cases.

Cal-Gang

Cal-Gang is a separate repository of gang-related data used by investigators in investigations of gang-related activities.

Cal-Photo

Cal-Photo is a database containing statewide booking and driver’s license photos.

Crime Statistical Reports & Crime Mapping

These applications are the public crime statistic web interface.
Appendix D – JNET Applications

AOPC Portal

A service that provides access to docket sheets for Pennsylvania’s Appellate Courts, the Court of Common Pleas, and the Magisterial District Judges. Authorized users can access the Law Enforcement Portal, Local Rules, Court Calendars, and Warrant Search through the AOPC Portal.

CNET

CNET is a web-based police records management system (RMS).

Department of Health (DOH) Birth Record Inquiry

This application provides authorized JNET users with the ability to search for and retrieve birth certificate record information to verify citizenship.

Domestic Relations Office Warrants

This application permits authorized JNET users with the ability to query domestic relations warrants from all 67 counties in Pennsylvania using various search criteria.

Electronic Reporting Statistics

This application provides authorized JNET users with the ability to query pre-built reports based on the electronic reporting data provided by county probation officers and county prisons.

Justice Data Flexible Search (JDFS)

This application provides JNET users with access to data from justice agency sources (courts, corrections, probation and parole, state police) via a single entry point using a web interface.

JNET Facial Recognition Investigative Search (JFRS)
The Facial Recognition Investigative Search software allows JNET users to compare unknown suspects’ images with those archived in the Commonwealth of Pennsylvania’s Photo Imaging Network (CPIN).

**JNET CLEAN**

This application provides access to the Pennsylvania State Police’s Commonwealth Law Enforcement Assistance Network (CLEAN) and to the National Crime Information Center (NCIC).

**Webmail**

A closed, encrypted, web-enabled e-mail client limited to the secure JNET user community.

**Juvenile Inquiry Application**

This application provides justice workers with the ability to retrieve juvenile data provided by county juvenile probation officers via a single-point search application and user interface.

**Juvenile Watch List Inquiry**

This application allows law enforcement officers and other authorized users to access juvenile watch list records. These records contain information provided by those agencies that monitor juveniles required to be under supervision.

**Master Charge Code (MCC)**

The MCC allows agency charge codes to be linked to master charge codes.

**Notifications**

The JNET Messaging Infrastructure allows users to subscribe to real-time event messages for comparison against offender watch lists.
PCCD Constable Query/Deputy Sheriff Query

The Pennsylvania Commission on Crime and Delinquency constable/deputy sheriff query application provides access to information about sheriffs and constables.

PennDOT License/Registration Pickup

This application provides JNET users with access to current lists of driver’s licenses and vehicle registrations currently expired or revoked by the Pennsylvania Department of Transportation (PennDOT).

PennDOT Photos/History

This application provides JNET users with current and historical driver’s license photos.

PennDOT Vehicle Registration

JNET user can access a vehicle’s registration information.

PFAD

The Protection from Abuse system contains information about restraining orders related to domestic violence.

Pre-Sentence Investigation Index (PSI)

This application allows JNET users to search for pre-sentence related court documents.

Sentencing Guidelines Software

This application provides court officials with sentencing guideline information.

SID/OTN Lookup

Users use this application to look up state ID numbers or offender tracking numbers.

Federated Warrant Search

This is a federated query application that allows users to query the CLEAN system, the NCIC< and the AOPC for outstanding warrants using a single query.
WebCPIN

This is a database with over five million photos from arrest/booking centers, state and county prisons, probation and parole and the NY/NJ High Intensity Drug Trafficking Area (HIDTA).
## Appendix E – JNET Project Prioritization Matrix

<table>
<thead>
<tr>
<th>Item #</th>
<th>Prioritization Criteria</th>
<th>Weight</th>
<th>Select</th>
<th>Decision Weight</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Alignment</strong> – How well does this initiative support JNET’s Mission and Goals?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Provide a platform for improved public safety</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Resolve integration issues</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Deploy emerging technologies</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Pursue more aggressive means to ensure protection of data</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Explore cost-effective solutions</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• <strong>Strategic Goal 1</strong> - Transition from collaboration to integration</td>
<td>5</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• <strong>Strategic Goal 2</strong> - Primary Public Safety information broker</td>
<td>5</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• <strong>Strategic Goal 3</strong> - Transition from a Technology Centric focus to Customer Centric focus</td>
<td>5</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• <strong>Strategic Goal 4</strong> - Highest quality of service (i.e., eliminate or reduce bugs)</td>
<td>5</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td><strong>Urgency</strong> – Is there a funding time limit, or regulatory compliance date that must be met?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• No</td>
<td>0</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td><strong>Does it require additional funding from the JNET Operating Budget?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
<td>0</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>4</td>
<td><strong>Cost Savings</strong> – Determine if this project will reduce the Commonwealth's cost to carry the existing process over the next 3 years?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reduces Costs</td>
<td>10</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• No Change</td>
<td>5</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Increases Costs</td>
<td>0</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Number of Users Impacted - How many users are affected?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All JNET Users</td>
<td>10</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5K to 28K</td>
<td>7</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>100 to 5K</td>
<td>5</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fewer than 100</td>
<td>2</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>None</td>
<td>0</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Agency Impact – How many agencies are impacted?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>More than Ten and/or PSP in mix</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Six to Ten and/or AOPC in mix</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Three to Five and/or DOC in mix</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>One or Two and/or OAG in mix</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>None</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Agency Readiness - Is Partner Agency willing to commit to JNET's Project Schedule?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes, or no partner agency involved</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Staff Resources Impact -Estimated Number of JNET Staff Needed to Work on the Project</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1-20</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>21-35</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>More than 35</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Will additional skills, training, or professional services be required?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Service Levels – How will this impact service levels, including SLAs?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dramatically increases</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Generally increases</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Has no effect</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Generally decreases/negative impact</td>
<td>-5</td>
</tr>
<tr>
<td></td>
<td>Dramatically decreases/negative impact</td>
<td>-10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>How many enhancement requests or bug fixes can be included in the project scope?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3 or more</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>0-2</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>TOTAL</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>100%</td>
</tr>
</tbody>
</table>
Appendix F – List of Acronyms

API – Application Programming Interface
ARJIS – Automated Regional Justice Information System
CAD – Computer Aided Dispatch
CLEAN – Commonwealth Law Enforcement Assistance Network
CLETS – California Law Enforcement Transaction System
CPO – Comprehensive Planning Organization
DDC – Data Distribution Center
DHS – Department of Homeland Security
DOJ – Department of Justice
HCI – Human-Computer Interaction
ICT – Information and Communication Technologies
IJI – Integrated Criminal Justice Information System
IMPACCT – Improve Management and Control Cost Task Force
IR – Information Retrieval
IT – Information Technology
JAAS – JNET Agency Advisory Subcommittee
JMS – JNET Messaging System
JNET – Pennsylvania Justice Network
JPA – Joint Powers Agreement
JTTF – Joint Technology Task Force
LAN – Local Area Network
LDAP – Lightweight Directory Access Protocol
MCT – Mobile Computer Terminal
MDT – Mobile Data Terminal
NASCIO – National Association of Chief Information Officers
NCIC – National Crime Information Center
NICBCS – National Instant Criminal Background Check System
ONS – Officer Notification System
PennDOT – Pennsylvania Department of Transportation
PKI – Public Key Interface
PSC – Public Safety Policy Advisory Committee
PSP – Pennsylvania State Police
SANDAG – San Diego Association of Governments
SCOT – Social Construction of Technology
SDDPC – San Diego Data Processing Corporation
SDPD – San Diego Police Department
SDSD – San Diego Sheriff’s Department
SNA – System Network Architecture
SOA – Service Oriented Architecture
SST – Social Shaping of Technology
STS – Science and Technology Studies
VPN – Virtual Private Network
WAN – Wide Area Network
Appendix G – Lessons Learned

Here I describe lessons I learned during the process of working on and completing this dissertation. Two of the most important – if seemingly paradoxical – purposes of dissertation research are to demonstrate research skills and to train in research skills (Isaac, Quinlan, & Walker, 1992). The demonstration of skills is implicitly evident in the completion and acceptance of the dissertation by my committee members. In order to assess the degree to which this dissertation served as tool for training in empirical research it is worth discussing the lessons I learned in the process of completing it. In conducting this research, I learned many lessons, three of which stand out. One, detailed planning is critical to quality research. Two, determining the proper scope for the research is fundamental to successful outcomes. Three, data collection is more effective when it is more structured.

Detailed Planning is Critical to Quality Research

The need for a detailed, highly structured research design was made plain in the comments from the committee on the dissertation proposal, and became immediately apparent when I thought I was ready to begin data collection. My initial research design was too vague, imprecise, and incomplete to be ultimately useful. Once I got into the collection of data I immediately realized I had not fully thought-out how I was going to approach the collection and analysis of data. As a result, much of the early stages of work on this dissertation were spent adding detail and giving more structure to the research design so that I could be more effective in the field. Had I spent more time at the beginning of this process constructing and articulating the research design, I would have been that much more effective and efficient in the collection and analysis of data.
**Research Must Be Properly Scoped**

A common piece of feedback from my committee to come out of the proposal defense was that I was attempting to do too much in this project. The too-large scope was one contributor to ambiguity in the research design. It was also a source of delay as I attempted to redefine the scope of the research to a manageable level.

Though I was able to significantly pare down the scope of this research, in the end, I still tried to accomplish too much in a single research project. In retrospect, attempting to combine empirical research with theory integration was beyond my means and the decision to do so was clearly based more in visions of grandeur rather than pragmatic reality. In paring down the project the way I did, I now realize the inclusion of boundary objects theory in this research was unnecessary, and perhaps ultimately counterproductive.

I also should have more carefully thought about the sites where I would conduct case studies. While ARJIS is an exemplar IJIS, its location 3,000 miles away greatly limited my ability to spend time in the field studying ARJIS given my other commitments and limited resources. I would have been better served to have selected a case study site geographically closer to home; thereby being able to spend more time at the site of the case study collecting field data. I also think a startup IJIS would have been a better selection for this study because a startup would have provided the opportunity observe the formation of an IJIS organizational identity at the same time the technological infrastructure was being built.

**Data Collection is More Effective When it is More Structured**

Once I began data collection I learned that the more structured my data collection instruments were the more effective they were at eliciting the data I was looking for. The second round of interviews I conducted at both ARJIS and JNET were much more efficient and
effective. The second round of interviews generated larger volume of more specific data than the first. This is not to say that I would abandon the use of semi-structured interviews. On the contrary, I still find efficacy in semi-structured interviews for exploring emergent data in greater detail. Rather, in future research I will continue to use semi-structured interviews but with more structure in the form of more closed and fewer open questions. This will allow me to continue to pursue interesting avenues of inquiry while simultaneously elicit detailed, specific data from the subjects.

The importance of a detailed research design, of limited scope, and of structured data collection were three lessons I take away from working on this dissertation. Having learned these lessons, I know that future research endeavors will be much more conceptually focused and operationally efficient.
References


Chan, J. B. L. (2001). The Technological Game:: How Information Technology is Transforming Police Practice. *JCriminology and Criminal Justice, 1*(2), 139-159.


http://www.budget.psu.edu/FactBook/StudentDynamic/EnrollmentSummary2Years.asp? SemesterCodes=200405FA200506FA


Vita – Michael Tyworth

Education
Ph.D., Information Sciences & Technology (2009)
The Pennsylvania State University

Indiana University Bloomington

Bachelor of Arts, Psychology (1992)
The Pennsylvania State University

Publications

Teaching
Visiting Assistant Professor of Information Technology Leadership, Washington & Jefferson College

Awards
Harold F. Martin Graduate Assistant Outstanding Teaching Award Nominee - 2009
International Conference of Information Systems Doctoral Consortium Participant - 2007