

Institutional and Organizational Influences on the Design of Integrated Criminal Justice Information Systems

Michael Tyworth
The Pennsylvania State University
329B IST Building
mtyworth@ist.psu.edu

ABSTRACT

In this paper I present preliminary findings from research on the design and use of interorganizational information systems being developed to facilitate information sharing among criminal justice agencies, called IJIS. One, institutionalized practices, values, and norms remain a barrier to effective integration, collaboration and information sharing. Two, individual IJIS have unique identities that are reflected in both their organizational and technological arrangements.

Categories and Subject Descriptors

K.43 [Computers and Society]: Organizational Impacts – automation, computer-supported collaborative work, employment, reengineering.

General Terms

Management, Design

Keywords

Organizational identity, integrated criminal justice information systems, design practices

1. INTRODUCTION

Through this paper I present findings on the design of integrated criminal justice information systems (IJIS). Complex technological and organizational ensembles, IJIS are being developed at all levels of government in an attempt to provide greater integration, collaboration, and sharing of information among criminal justice agencies. A comparative case study of two preeminent IJIS leads to two findings. One, institutionalized practices, values, and regulations remain a major barrier to effective integration, collaboration and sharing of information among criminal justice agencies. Two, individual IJIS have distinct identities that are reflected in both their organizational practices and arrangements of their ICT artifacts. Combined, these findings present a picture where comprehensive integration at a national level – providing a national criminal justice information infrastructure – is unlikely to be achievable in the foreseeable future.

2. INFORMATION INFRASTRUCTURE: INTEGRATED CRIMINAL JUSTICE INFORMATION SYSTEMS (IJIS)

In 1991 Congress set a goal of a National Information Infrastructure comprised of seamless public and private communication networks, interactive services, and interoperable hardware, software, databases, and ICT devices [7]. Though they predate the establishment of the NII, IJIS are an excellent example of the attempts to put the concept of an NII into practice. IJIS are complex organizational and technological ensembles created to integrated heterogeneous information systems in law enforcement [6]. The development of an IJIS includes integration of organizational processes, information stores, and technical infrastructures to some degree. IJIS initiatives occur at all levels of government but the most prominent reside at the local/regional level and the state level of government [4].

2.1 ARJIS& JNET

Two exemplar IJIS currently in operation are the Automated Regional Justice Information System¹ (ARJIS) serving San Diego County in California, and the Pennsylvania Justice Network² (JNET) which serves the entire Commonwealth of Pennsylvania. ARJIS is an IJIS created around a legacy mainframe database of the same name. Organizationally, ARJIS is governed by ten member agencies and the ARJIS management organization. Technologically, ARJIS has integrated ten separate local and state criminal justice information systems along with the federal systems such as the National Crime Information Center (NCIC). Over 11,000 users access ARJIS regular using mobile data terminals, desktop workstations, and handheld devices.

JNET was established as an organization within Pennsylvania's Office of Administration by executive order in 1995. JNET resides within the Executive Branch of the commonwealth government and its strategic-level governance is provided by a steering committee comprised of state level agencies. Operation and design of JNET is managed by the JNET organization itself headed by an executive director. JNET provides access to over twenty individual state and federal systems. The majority of these systems are criminal justice information systems; however JNET also provides access to transportation, transportation, public welfare, and other tangentially related systems. Currently, JNET

¹ See <http://www.arjis.org/>

²See

<http://www.portal.state.pa.us/portal/server.pt?open=512&objID=1189&mode=2>

provides access to over 30,000 users in all 67 counties in Pennsylvania.

3. INSTITUTIONAL BARRIERS INHIBIT INTEGRATION

Law enforcement in the United States is institutionally disintegrated and entrenched institutional practices remain a major barrier to comprehensive integration at a national level. There are over 19,000 police agencies in the United States [3]. Each of these agencies has its own leadership, management structure, norms, rules and regulations, missions, and ICT infrastructures. Myopia regarding information assets is highly prevalent among law enforcement agencies in terms of design, ownership, and access to information resources [5]. As a result, even successful IJIS efforts like ARJIS and JNET have to work around these institutional barriers in order to gain access.

This need to work around barriers to integration is especially prevalent at JNET where designers and managers are attempting to integrate not only law enforcement systems but systems from other governmental domains. Partly as a response to these institutionalized barriers to integration, JNET designers act as a central hub to the individual systems rather than as an integrator of them. JNET users access each system individually, one-at-a-time. If a user wishes follow-up a query of the Pennsylvania State Police’s (PSP) CLEAN system with a query of the Department of Transportation’s (DOT) license photo database, they have to run two separate queries. This is because early in JNET’s development JNET had to approach these agencies individually and sequentially in order to get them to participate. JNET had to establish trust with each by allowing each to retain maximum control over their assets.

Table 1. Institutional Barriers to Integration

Institutional Barrier	ARJIS	JNET
Data myopia – highly institutionalized norm among participating agencies of “protecting” individual data assets	Individual agencies retain ownership of data, but must conform to IJIS standards to attach to system.	Brokerage architecture where JNET acts as a connectivity bridge among disparate information sources
Regulatory barriers inhibit information sharing across regional / state borders	ARJIS development efforts hampered by requirement of state approval for all new systems attaching to state connected databases	JNET has had difficulty expanding connectivity to regional systems because of state information sharing prohibitions.

Though ARJIS managers and designers faced lower institutional barriers to sharing they still were forced to allow member agencies to retain a large amount of autonomy in regards to their

ICT. Individual member agencies are free to develop their own ICT infrastructures independent of ARJIS or any other ARJIS member agency. Individual agencies still retain control over their data and public use of agency data must be approved by the agency that owns it. As with JNET ARJIS takes this approach in order to maintain participation. Though interested in sharing information, agencies want to be able to pursue their own ICT agendas.

Institutional barriers exist outside the IJIS as well. For example, because ARJIS connects to a state law enforcement database, all new connections to the system – either new connection points or new systems – must be approved by the state. This burden adds to the difficulty of integrating new systems into ARJIS.

JNET has experienced obstacles to integrating with systems in bordering states due to legal restrictions on the use of criminal justice data in Pennsylvania. As a result, JNET’s ability to integrate across state borders has been greatly hampered. Institutional barriers are one reason why national-scale integration remains supremely difficult; how the IJIS organizations perceive themselves is another.

4. ORGANIZATIONAL IDENTITY SHAPES IJIS ORGANIZATIONAL AND TECHNOLOGICAL DESIGN OF IJIS

Organizational identity is a concept with roots in the scholarship and literature on management and organizations. An organization’s identity is what is collectively perceived by its members as the organization’s central, enduring, and unique features [8]. Just as with individual identity, organizational identity serves to not only define for the organization who the organization is, but who it is not; or, in other words, how the organization is different from other organizations [1, 2]. An organization’s identity serves as a guide to organizational action, and through shaping the organization’s culture, shapes its artifacts.

The organizational identities of ARJIS and JNET differ, and these differences are reflected in the designs of their organizational ICT. ARJIS’ organizational identity is that of a regional center for collaboration and technology for the purposes of serving law enforcement. This identity is reflected in the ARJIS system in three important ways. One all additions or modifications to the features and functionality of the ARJIS system are collectively negotiated by the ARJIS member agencies. Two, every design decision is guided by an overarching criterion: will the change be beneficial to law enforcement? Three, member agencies contribute their data to the ARJIS mainframe in exchange for access to the ARJIS system and data definitions, standards, and integrity are collaboratively negotiated and maintained.

JNET’s identity is that of a broker of criminal justice information in the Commonwealth of Pennsylvania. Like ARJIS JNET’s identity is reflected in its organizational ICT. Instead of collaborating among member agencies to design the overall system, JNET partners with specific agencies to provide the connectivity they need. JNET as an organization is not interested in retaining data, but rather JNET is interested in acting as a

mediating access point between different agencies – as reflected in its hub-and-spoke architecture³ discussed previously.

Table 2. Influences of Identity on IJIS Design

IJIS	Identity Attributes	Impact on Design
ARJIS	Identity of regional center for technology and collaboration serving law enforcement	System design is collectively negotiated All design decisions are evaluated against benefit to law enforcement Data definitions and standards are collaboratively determined and maintained Data is stored centrally in mainframe database
JNET	Broker of criminal justice information for the Commonwealth of Pennsylvania	Input on design of new system features and forms of access limited to individual agencies providing connectivity. JNET does not own or store data but provides access Needs of Commonwealth agency (or government) take precedence in design decision hierarchy

Similarly, JNET’s identity as a state government agency results in a design prioritization of Commonwealth needs. When selecting which features to add, what hardware and software to employ, what vendors to contract with, JNET’s identity as a state agency plays a decisive role. Priority is given to system features identified by commonwealth partnering agencies, the legislature, or the governor’s office as being critical. Local agency needs, from whom the majority of JNET’s user base is derived, are relegated to bug fixes and minor updates requested through the help desk.

³ In many ways the JNET portal acts like the roundhouse found in rail yards of history. Just as a locomotive would enter the roundhouse and be routed out in the direction it needed to go; a user virtually enters the JNET portal and is routed to the desired back-end system.

5. CONCLUSION

So, given that institutional barriers and organizational identities shape individual IJIS efforts, what does this mean for national efforts to integrated law enforcement ICT as part of a broader information infrastructure policy? Most importantly it means that total national integration is unlikely given the varying needs at different levels of government. Instead, collectives, brokers, and mediated access will likely be the basis for sharing. Two, it means that short of a significant institutional overhaul – such as nationalizing police – national integration is likely to remain at best, a goal just out of reach for the foreseeable future. Local identities, institutional structures, norms and the reality that crime is primarily a local problem to be solved, are likely to prevent systematic integration are likely to limit the ability to integrate to regional levels. Policymakers should continue to push integration and standardization however, with time enough homogeneity in systems development will make a greater level of integration much easier to achieve.

6. ACKNOWLEDGEMENTS

I would like to thank my adviser, Dr. Steve Sawyer, for his guidance and assistance in conducting this research. Also thank you to the members of the ARJIS and JNET management teams who provided their time and access. This research was funded in part by National Science Foundation grants IIS-05-0742687 and IIS-05-34889.

7. REFERENCES

- [1] Albert, S., Ashforth, B.E. and Dutton, J.E. Organizational identity and identification: Charting new waters and building new bridges. *Academy of Management. The Academy of Management Review*, 25 (1). 13-17.
- [2] Ashforth, B.E. and Mael, F. Social Identity Theory And The Organization. *The Academy of Management Review*, 14 (1). 20-39.
- [3] Bureau of Justice Statistics. *Census of State and Local Law Enforcement Agencies (CSLLEA)*, 2000. U.S. Department of Justice Office of Justice Programs ed., 2000.
- [4] Gil-Garcia, J.R., Schneider, C.A. and Pardo, T.A. *Effective Strategies in Justice Information Integration: A Brief Current Practices Review* Center for Technology in Government, Albany, NY, 2004.
- [5] Manning, P.K. *Policing contingencies*. University of Chicago Press, Chicago, 2003.
- [6] Morton, H. *Integrated Criminal Justice Information Systems*. National Conference of State Legislatures ed., 2004.
- [7] Shin, D.-S. Next Generation of Information Infrastructure: A Comprehensive Case Study of Korea Versus the United States of America. *Journal of the American Society for Information Science for Information Science and Technology*, 50 (11). 1785-1800.
- [8] Whetten, D.A. Albert and Whetten Revisited: Strengthening the Concept of Organizational Identity. *Journal of Management Inquiry*, 15 (3). 219-234.