

Organic Development: A Top-Down and Bottom-Up Approach to Design of Public Sector Information Systems

Michael Tyworth

The Pennsylvania State University
311B IST Building
University Park, PA 16802
01-814-571-0585

mtyworth@ist.psu.edu

Steve Sawyer

The Pennsylvania State University
301F IST Building
University Park, PA 16802
01-814-865-4450

sawyer@ist.psu.edu

ABSTRACT

In this paper we lay out interim findings and speculate on the implications for practice and theory of integrated criminal justice systems in law enforcement. In doing this we theorize on public sector information systems and their uses of information and communication technologies as engaging in what we call “organic development.” To develop our theorizing on organic development, we draw on a field study of the San Diego, California area’s Automated Regional Justice Information System (ARJIS). We develop organic development as drawing on both top-down and bottom up approaches to engaging the technologies, technological infrastructures, governance principles, and work practices that, together, are an integrated system.

Keywords

Institutional Theory, Integrated Criminal Justice Systems, Social Informatics, Emergent Design, Organic Design

1. INTRODUCTION

What technology architectures, governance structures and work practices are associated with successful integration of information and communications technologies (ICT) into law enforcement? In this paper we lay out interim findings and speculate on their implications relative to this question, pursuing more coherent theories, and greater insights into the practices, of integrating ICT into public safety, criminal justice and law enforcement. And, we theorize on public sector information systems as engaging in what we call “organic development.”

Law enforcement agencies have long recognized the need to integrate their ICT both within and across their individual organizational boundaries [12, 21]. Having recognized the need to integrate, law enforcement agencies and sponsors continue to struggle translate these needs into an operational reality [13-15, 25]. More recently, ICT integration became a top priority for homeland defense policymakers and renewed emphasis has been given to developing new technologies and forms of organizational collaboration [38]

The result has been a seeming explosion of design and development initiatives nationally, many with their own unique, and in some cases competing, approach to addressing the problem of organizational and system integration. These initiatives have been termed integrated criminal justice information systems

(ICJS). Examples of such initiatives include the Capital Integrated Wireless Network (CAPWIN) undertaken in the Washington D.C. metro area; Pennsylvania’s Justice Network system (JNET); Charlotte-Mecklenburg’s Knowledge-Based Cops (KBCOPS) system; and the Automated Regional Justice Information System (ARJIS) being developed for use in the San Diego, California region. There are many others.

The premise driving our work is that learning and sharing from these initiatives will lead to improved integrated criminal justice systems. To do this demands studying – to understand -- the proper governance structures, successful work practices and appropriate technological infrastructures. If the policy goal is indeed integration of law enforcement ICTs on a national scale, then it is critical to identify those designs that are successful and those that are not in order to avoid simply the development of new generation of systems that are as “siloed” as the systems they are intended to replace.

In this paper we present preliminary findings from our ongoing case study of the Automated Regional Justice Information System (ARJIS). We focus in particular on ARJIS’ “organic” or emergent method of system design and development as one that has led to successful system outcomes. This is in direct contrast to other ICJS design and development practices that emphasize a “grand” or enterprise approach to design where the system is designed in its entirety prior to development. The remainder of this paper consists of a review of the relevant literature, a description of our ongoing study of ARJIS and a discussion of this emergent design approach.

2. LITERATURE REVIEW

We begin by noting the entrenched but chaotic roles of ICT in policing; a historical practice of uncoordinated development efforts; and the need for integration of systems across organizational boundaries. We review our intellectual frame, Social Informatics: a perspective that focuses on our attention to the socio-technical and contextualized nature regarding the design, uses, and consequences of ICTs [32]. We then highlight our theoretical approach as grounded in institutional theory: a view that engages institutions as comprised of regulative, normative, and cognitive structures that provide and define social meaning [18].

2.1 Policing & Technology

For over 70 years, law enforcement agencies have engaged ICT for crime analysis, crime prevention, and agency administration. An early use of ICT in law enforcement was the combination of a simple map covered with push-pins to denote crime activity [29]. From maps and pins; the law enforcement community has gone on to adopt a variety of different ICT including radio, cellular phones, wireless computing, computer-aided dispatch (CAD), and electronic records management systems (RMS) [12]. Using ICT in law enforcement is approaching ubiquity and is now considered to be a fundamental component of policing [17].

These ICTs are used in many, legitimate, ways. For example, an officer patrolling a beat may have the dispatcher run a license plate through the RMS to check if a vehicle is stolen. A detective may run a license plate number through an RMS to see if the vehicle has been used in other crimes; and a crime analyst may mine the data in an RMS looking for patterns of criminal activity [27].

The increased reliance on ICTs in law enforcement raises a number of issues. Perhaps the most pressing issue resulting from the incorporation of ICTs into policing is that system design and development has for the most part been done in an ad hoc and incompatible manner [12, 26]. This piecemeal approach to system design and development has resulted in law enforcement agencies being burdened with inflexible-but-entrenched systems that are generally incompatible with other law enforcement systems outside of the organizational boundaries, and occasionally even incompatible with other systems within the organization itself! Incompatibility among ICTs in law enforcement not only impacts tactical operations by hampering the sharing of mission critical information; but it also hampers information-sharing initiatives such as the National Crime Information Center (NCIC).

Another factor contributing to the lack of systems integration across agencies is the nature of policing in the United States. Law enforcement in the U.S. is structured around a federalist model both in terms of the relationship between the federal government and the states, and within the states themselves. In a federalist model each level of government has its own jurisdiction. At the federal level there is the Federal Bureau of Investigation (FBI), the Border Patrol, U.S. Attorney Office, U.S. Marshals, U.S. Secret Service, and the police agencies of the various military services. The jurisdictions of these agencies are interstate and international and the focus is on the prevention and prosecution of federal and federal-level (interstate/ international) crimes. At the

state level there is the state police, and the occasional state marshal service (e.g., the Texas Rangers). The predominant role of state police is traffic law enforcement on the state highways; however state police also enforce other state level laws such as customs and organized crime [30]. At the local level there can be county, city, township, and even institutional (e.g., university) law enforcement agencies all within a limited geographical region. These agencies are engaged in the enforcement of local laws (including traffic), as well as prevention and solving of local crimes. What this means is that in the United States, the primary for delineating governmental and organizational boundaries is geographical location.

Take for example, the relatively small town of State College, Pennsylvania. State College is a university town with a population ranging from about 40,000 during the summer to 80,000 during the academic year [2, 3]. Agencies that have jurisdiction in the State College area five 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 Sheriffs department [1]. This totals to 12 different police agencies in a relatively small geographical area, each with its own jurisdiction, management structure, funding structure, organizational goals, and ICT infrastructures. Moreover, the police forces of the four adjoining townships are cross-sworn with State College Police (as are the State College Police with these townships). Designing any ICT-based system to be compatible with all these disparate agencies is a remarkably complex task; one that grows more even complex when the trying to incorporate federal agencies into the mix.

Even though these and other issues have resulted in ICT implementations that often fail to completely realize the promised gains, and often lead to new challenges, individuals in law enforcement continue to perceive ICTs as capable of benefiting law enforcement activities [7, 8, 17, 33]. So, law enforcement agencies and policymakers continue to look for opportunities to exploit ICTs to improve services. The impetus to develop integrated criminal justice information systems is rooted both in the failure to effectively share information within and across organizational boundaries and in the continued perception of ICTs ability to improve policing..

2.2 Integrated Criminal Justice Systems

Integrated criminal justice information systems (ICJS) encompass technological infrastructures, governance policies, and work practices and procedures intended to facilitate effective communication and sharing of information both within and across organizational and jurisdictional boundaries. Projected benefits of using ICJS include improved data quality, time and money savings, timely access to information, improved safety, greater efficiency and information sharing [12, 16]. Some have posited second-order benefits to ICJS use such as deterrence as a result of a perception that law enforcement is more knowledgeable of who commits crimes [4].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Conference '04, Month 1–2, 2004, City, State, Country.
Copyright 2004 ACM 1-58113-000-0/00/0004...\$5.00.

Claims that the benefits of ICJSs are now well-established [11, 12] are contested by empirical studies that make clear many of the benefits of ICJS initiatives are still unrealized [13, 15]. For example, the National Conference of State Legislatures (NCSL), a major advocate of the deployment of ICJSs, states explicitly that agencies should not expect to realize a financial savings as a result of their ICJS initiatives [24]. This echoes findings from studies of ICJS initiatives in law enforcement that note efficiency gains are often offset by the costs of the increased resources required to support the ICT [28].

Echoing these findings the recent research provides inconclusive evidence as to the impact on efficiency from using ICJSs. As noted, efficiency in one area of law enforcement has in some cases been offset by the decrease in efficiency in others. 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 [39]. CMPD effectively transferred the burden of data entry from record-management staffers to field officers. 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 et al. [33] reports similar findings. They found that connectivity drops, dual-layer authentication, and battery drain all added significantly to the cost to the officer trying to use the system. These issues were exacerbated by the limited IT support available within the agencies studied. Additionally, they report that the implementation of wireless access did not alter existing organizational structures. Officers using the technology still relied on existing communications structures (dispatch).

The issues that helped spur the movement to integrate ICTs 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 [26]. Similarly, the General Accountability Office 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 [15]. Battles over organizational turf continue to be a major obstacle resulting in a "lack of resource pooling, lack of information sharing, poor procedure development, and a lack of adaptation [10, 16]". Implementing the needed institutional reforms has often been relegated a low priority or resisted altogether [10].

In spite of the documented difficulties and ambiguous results, agencies continue to press on with their ICJS initiatives, and new initiatives continue to proliferate both in the United States and globally [27]. Each of these initiatives has its own design

methodology, governance structures, and system components [24]. The move is to integrate disparate information systems: but, the level of integration has been in many ways limited to the scope of the project. It would be too easy, and sad, if this were allowed to negate the overall goal of nationally integrated systems.

Integrating criminal justice systems has become one of the more visible aspects of digital governance. It seems wise, if not imperative, that the "best" design, development, and deployment practices are identified early in the process so that designers, managers, and policymakers can make informed decisions regarding their initiatives. This is why we focus our research on empirical and conceptual insights on the design of ICJS.

3. ARJIS STUDY BACKGROUND

Two practical motivations motivate our research on ARJIS. One is the increased public interest in the development of systems that allow disparate law enforcement agencies to communicate and coordinate across jurisdictional and organizational lines. Individual law enforcement agencies are complex and sophisticated organizations and as a result, any effort to integrate multiple law enforcement agencies must necessarily be complex and sophisticated as well. Our research seeks to understand how this organizational complexity and sophistication impacts system development and use.

A second motivation is that system development efforts at a macro level have, to date, been largely ad hoc. Funding and direction has come both from the top in the form of grants and directives from federal agencies such as the Department of Homeland Security and the Department of Justice (National Institutes of Justice and Office of Justice Programs), as well as from the bottom through the efforts of individual officers and units. System design choices have varied across initiatives in terms of technologies, policies, and governance structures. We seek to identify the successful design choices and practices with the goal of contributing to a more "standardized" approach to ICJS development.

We are also motivated to inform theory by drawing from our results on the nature and structure of the interdependencies among technical architectures and public-sector organizational governance. Specifically, we seek to understand how institutional influences impact the development, operation, and governance of integrated criminal justice systems. By doing so we intend to engage and extend a body of knowledge that is vibrant, discordant, and often not well-developed theoretically [34].

3.1 Social Informatics

We take a Social Informatics perspective grounded in Institutional Theory to this research. Social Informatics focuses on "the design, uses, and consequences of ICTs (information and communications technologies) that takes into account their interaction with institutional and cultural contexts [19, 32]." Our view of ICTs is that they are embedded with social context, shape human social context, and are shaped by human social context.

From this perspective, neither the technology nor the user is without agency. Nor is the user an abstraction that engages the ICT in a social vacuum. Rather, both the technology and the user are embedded in a highly complex and evolving context that is constituted and shaped by both.

Social Informatics research engages a range of social theories, drawing from a range of viable theoretical positions that engage human activity as bound by social norms and organizational constraints. Social informatics begins with the premise the people are social actors. That is, people's individual agency (their ability to act) is constrained by a number of social forces.

For this research we draw on Institutional Theory as our theoretical framework. Institutional Theory posits that social organizations are comprised of rules, sanctions and physical structures embedded in social and cultural contexts [5]. Social institutions constrain and define social life either through coercion (regulative), through the definition of appropriateness (normative), or by example (cognitive) [6, 18]. These social institutions can and often do transcend organizational boundaries. Examples of institutions include professional associations, corporations, political parties, bodies of professional knowledge, governments, cultural practices, and even technologies. These institutions constrain and shape the way organizations behave.

Seen as a means to explain how longstanding sets of formal, informal and overlapping social forces and organizations interact, Institutional Theory is most appropriate to the law enforcement domain. Law enforcement agencies are highly social and cultural agencies, with strong professional associations and well-defined bodies of knowledge. They are embedded in a complex system of institutions that includes government and community as well as the historical, the political, and the technological. We seek to understand to understand how these institutions drive and constrain the design, development, and use of ICJSs.

3.2 Research Approach

The practical value of studying ICJS makes these worthy objects of study. Conceptually, these systems are an ideal example to study inter-organizational systems. Such systems are complex due to the relationships among technical elements (their computing architecture) and the institutional structures in and across which they exist and influence (the broad range of agencies, levels of government and stakeholders in and out of the public sector) [27]. The nature and effects of the relations among technical architectures and institutional structures links various social science and computing research areas, and the theorizing in this area, while nascent, is quite active [20, 22, 27, 31].

Since this research is part of a larger, comparative, study a common framework is critical. The common framework we used builds on that reported on in Sawyer, et al. [33] and focuses attention to:

- Computing infrastructure elements to include nature and structure of wired and wireless connection, throughput, coverage, reliability, and costs.
- The types, uses and characteristics of the devices being used.
- The functionality, feature sets, design principles, and development efforts regarding applications and systems software. This includes attending to issues with security and authentication.
- Information sharing, uptake, distribution, and needs. This includes sources of information, cross-system and cross-boundary information sharing, and the volume, types, and uses of information
- Work activities of stakeholders from both task analysis and work structuring perspectives. This includes a range of stakeholders (such as mobile and fixed-location users, dispatch, developer, administrators, etc.) and a range of work environments.
- Governance structures and processes. This includes both operational governance (of the work being done and of the systems development efforts) and inter-organizational governance (problem-resolution, policy-setting and decision-making).

This research framework also guides the cross-time (temporal) nature of our data collection. We used five forms of data collection. Three focus on gathering primary data: interviews (face-to-face, by phone, and via email, depending on the point of the interaction), ride-alongs with – and other direct observation of – users. We also gathered secondary documents such as reports, memos and locally-relevant material (we, of course, have done and continue to do extensive web and library research to support the field work) as well as data about device uses, data transmission, and ARJIS usage via unobtrusive means (such browser logs, server logs, and telecom activity logs).

Data from the sources are transcribed into digital format or collected at source in digital format. Data from the usage logs came in digital format. This supported our analysis across different data sets and data collection approaches. To do this analysis we are using traditional qualitative/case study data analysis approaches (see [23]). In particular, we are focusing on three techniques: interim analysis of the data to guide data collection and interpretation in the future, explanatory event matrices, and content analysis of the interview/focus group transcripts and field notes.

We are currently completing the case study of ARJIS. When the study is complete we expect to have fifteen (30 hours) interviews, six officer ride-alongs, and analysis of over 650 pages of documents. At the end of this research we expect to have a comprehensive and in-depth understanding of the ARJIS system both technologically and institutionally.

3.3 Automated Regional Justice Information System (ARJIS)

The Automated Regional Justice Information System (ARJIS) of San Diego, California is one of the preeminent criminal justice information systems initiatives in the United States. Initially a mainframe records management system accessible by multiple jurisdictions in the San Diego area, ARJIS has evolved over the past 20 years both organizationally and technologically. Organizationally ARJIS has become its own organization embedded in the county government structure. Technologically ARJIS is in the process of developing wireless communications systems, global query application, and public safety cable television channel.

Beyond its established record of success, ARJIS is an ideal system and organization to study is that is both horizontally and vertically multi-jurisdictional. ARJIS is horizontally jurisdiction-spanning because it (the organization and the system) spans numerous local jurisdictions such as the San Diego and Carlsbad Police Departments among many others. Vertical jurisdiction spanning results from ARJIS' spanning of multiple of government including the San Diego Sheriff's Office (county), the California Highway Patrol (state), and the U.S. Border Patrol (federal) [35]. Over ten law enforcement agencies with over 10,000 law enforcement officers policing a population of over 38 million citizens are participants in the ARJIS system [9].

Technologically, ARJIS is equally robust. The ARJIS system includes over 2,500 workstations and printers, and 10,000 registered users. Over 35,000 transactions accessing 2.9 million recorded incidents, 5 million digital photos, and 4.4 million map and crime statistics occur daily. With its sheer scope, ARJIS provides a unique opportunity to study an ICJS initiative in an institutionally complex environment.

The ARJIS organization is currently engaged in a variety of different development initiatives. These initiatives include both the development of hardware and software. The ARJIS system is being developed along two separate but parallel paths. One path is the development of a web-based interface to a SQL database designed to first interact with, and then later replace the legacy systems that comprise ARJIS today. This system, called Global Query, makes use of both proprietary and commercial-off-the-shelf (COTS) applications. One benefit of these applications is that it provides a vehicle for the development of other projects such as wireless PDA access to the system for the BorderSafe project.

The other development path is more ad hoc and is driven by customer (agency) demand. These initiatives consist primarily of adding functionality or access to the existing ARJIS infrastructure. For example, the addition of "Wants and Warrants" information to the system, mapping or geographical information systems applications, and access to the databases tracking pawn shop transactions. These applications are incorporated ARJIS in a manner that is consistent with their

overall design approach ensuring that everything done is towards the larger goal of integration.

4. EMERGENT DESIGN APPROACH

We observe that the ARJIS approach to designing both their information system and their organization differ from other ICJS design approaches, and most of the recommendations to be found in the literature. Gil-Garcia et al. [16] identify three types of ICJS development approaches: selective, comprehensive and incremental. A selective approach is organizational or functional-area specific, such as a computer-aided-dispatch (CAD) system. A comprehensive approach is multi-organizational, multi-level, and is completed in a short time frame such as the implementation of a juvenile records system accessible by law enforcement, the court system, and social services. This is often driven by a comprehensive master (or enterprise) plan. Like the comprehensive, the incremental approach is multi-level and multi-organizational. However functionality is added incrementally relative to a comprehensive enterprise plan.

These three approaches adhere to the literature on ICJS development that recommends two fundamental components of the ICJS process. The first is an extensive, detailed project plan / design document itemizing not only the technical specifications, but the organizational design and the information sharing procedures and policies [16]. The second views significant government support and leadership and infrastructure upgrading as critical to ICJS development efforts [24]. These two views are consistent with what Truex et al. [36] identify as assumptions and ideas that have been privileged in systems development discourse in general.

Based on our examination of ARJIS, we suggest a fourth approach that we call "organic." The organic approach appears similar to the incremental approach, but is also "bottom-up," or a combination of both bottom-up and top-down. Instead of being driven by an advocate in a position of high authority and guided by a structured and enterprise-level project plan, the "organic" approach is emergent [22]. This approach to development is closer to approaches Truex et al. [36] identify as marginalized in the literature, yet as they also point out, it is also likely to be closer to how system development actually occurs.

By emergent we mean that the organic approach reflects what Truex and colleagues argue is a more realistic (and thus viable) basis for designing, developing and delivering information systems [36, 37]. Truex et al. [37] identify principles that define both emergent systems and the organizations that develop them (see Table 1).

Table 1 Emergent Systems Principles

Emergent Systems Principles	Meaning
Always analysis	Organizations, and thus, their systems, are dynamic. This demands that analysis must continually engage these

	changes.
Incomplete and usefully ambiguous specifications	Specifications can never be complete, but can serve as guiding principles and to establish parameters
Continuous redevelopment	The system is ever evolving, never complete and uses are always changing.
Adaptability orientation	Developers, leaderships and users engage these changes as matters of course, not as exceptions or problems.
Back-channel communications	Interactions among key stakeholders must include many informal and formal mechanisms, and be seen as a discourse, not as a set of contracts.
Emergent IT organization	The symbioses among the system and the systems development organization suggests that both must be flexible, changing dynamically and often in relations to one-another
Proper reward systems	Developers, users and leadership must be incentivized to engage in this dynamic approach to systems.

5. CONCLUSIONS AND FUTURE DIRECTIONS

This section is incomplete and tentative, as befits the interim nature of what we are reporting. Having said this, we are beginning to see two second-order effects resulting from organic approach, as we discuss briefly. In the discussion in the previous section, we began developing the idea of organic development as a strategically sound, technologically wise, and operationally useful approach. Here we elaborate on that by invoking the architectural metaphor of the New England farmhouse.

The first second-order benefit we can highlight is that the bottom-up and top-down means of organic development are mutually reinforcing. For example, we find that when ARJIS' staff engages the individually requested components in the system, it provides them the opportunity to bring those systems into adherence with ARJIS data standards. ARJIS accomplishes this by requiring agencies to comply with ARJIS standards in order to have their data incorporated into the larger system.

We also find that this attention to engaging stakeholders at the work level creates a virtuous feedback loop to the leaders involved in governance. They are more willing to engage in long

term thinking and supporting larger-scale activities because they see these as helping achieve both strategic and tactical objectives.

The architectural metaphor represented by organic development is visible in the way New England's farmhouses have evolved. The strategic goals (house the family, access to livestock, to protection from the elements) guide the design (top-down). The evolving needs of the family (as children grew and married, as parents aged, and as the number and nature of the family changed) led to additions, expansions and new functionality. Likewise the changing nature of the farm (more livestock, more tools) and protection from elements (connecting house to barn) led to an evolving structure. The structure is architecturally distinct and functionally sound. Each farmhouse is different, but collectively they are identified because they emerged following the same top down, while responding to similar bottom-up pressures – that vary due to specific local forces.

6. ACKNOWLEDGMENTS

This work was supported in part by National Science Foundation grant IIS-051238.

Our appreciation to the officers and staff of ARJIS whose assisted us in studying and understanding their organization.

7. REFERENCES

- [1] 9/11 Emergency Communications. Centre County Government Office of Communications ed., 2005.
- [2] Fall Enrollment Summary. The Pennsylvania State University ed. University Fact Book, 2005.
- [3] State College (borough), Pennsylvania. U.S. Census Bureau ed. State & County Quick Facts, 2003.
- [4] Agrawal, M., Rao, H.R. and Sanders, G.L. Impact of Mobile Computing Terminals in Police Work Journal of Organizational Computing & Electronic Commerce, Lawrence Erlbaum Associates, 2003, 73.
- [5] Avgerou, C. Information systems and global diversity. Oxford University Press, Oxford ; New York, 2002.
- [6] Avgerou, C., Siemer, J. and Bjorn-Andersen, N. The academic field of information systems in Europe. European Journal of Information Systems, 8 (2). 136.
- [7] Brown, M.M. The benefits and costs of information technology innovations: An empirical assessment of a local government agency. Public Performance & Management Review, 24 (4). 351.
- [8] Brown, M.M. and Brudney, J.L. Learning organizations in the public sector? A study of police agencies employing information and technology to advance knowledge. Public Administration Review, 63 (1). 30.
- [9] Bureau of Justice Statistics. Local Police Departments 2000, 2000.
- [10] Clayton, R. and Haverty, D.M. Modernizing Homeland Defense and Security. Journal of Homeland Security and Emergency Management, 2 (1). Article 7.

- [11] Dunworth, T. Criminal Justice and the IT Revolution. Policies, Processes, and Decisions of the Criminal Justice System, 3. 371-426.
- [12] Dunworth, T. Information Technology and the Criminal Justice System: A Historical Review. in Pattavina, A. ed. Information Technology and the Criminal Justice System, Sage Publications, Inc., Thousand Oaks, CA, 2005, 1-28.
- [13] General Accountability Office. Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security. Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, 2005, 198.
- [14] General Accountability Office. Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities, 2003, 30.
- [15] General Accountability Office. Project SAFECOM: Key Cross-Agency Emergency Communications Efforts Require Stronger Collaboration, 2004, 27.
- [16] 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.
- [17] Hoey, A. Techno-Cops: Information Technology and Law Enforcement. International Journal of Law and Information Technology, 6 (1). 69-90.
- [18] Hossam, A.-H. Institutional Theory. Applachian State University and York Universite eds. Theories used in IS Research, 2005.
- [19] Kling, R., Rosenbaum, H. and Sawyer, S. Understanding and Communicating Social Informatics: A Framework for Studying and Teaching the Human Contexts of Information and Communications Technologies. Information Today, Inc., Medford, New Jersey, 2005.
- [20] Law, J. and Bijker, W.E. Technology, Stability, and Social Theory. in Bijker, W.E. ed. Shaping technology/building society : studies in sociotechnical change, MIT Press, Cambridge, Mass., 1992, 32-50.
- [21] Manning, P.K. Policing contingencies. University of Chicago Press, Chicago, 2003.
- [22] Markus, M.L. and Robey, D. Information Technology and Organizational Change: Conceptions of Causality in Theory and Research. Management Science, 34 (5). 583.
- [23] Miles, M.B. and Huberman, A.M. Qualitative data analysis : a sourcebook of new methods. Sage Publications, Newbury Park, 1984.
- [24] Morton, H. Integrated Criminal Justice Information Systems. National Conference of State Legislatures. ed., 2004.
- [25] National Association of State Chief Information Officers (NASCIO). Concept for Operations for Integrated Justice Information Sharing Systems, 2003.
- [26] National Association of State Chief Information Officers (NASCIO). Concept for Operations for Integrated Justice Information Sharing Systems, 2003.
- [27] Northrop, A., Kraemer, K.L. and King, J.L. Police use of computers. Journal of Criminal Justice, 23 (3). 259.
- [28] Nunn, S. Police information technology: Assessing the effects of computerization on urban police functions. Public Administration Review, 61 (2). 221.
- [29] Ratcliffe, J.H. Crime Mapping and the Training Needs of Law Enforcement. European Journal on Criminal Policy and Research, 10 (1). 65.
- [30] Rendell, E.G. and Miller, C.J.B. Pennsylvania State Police 2003 Annual Report. Pennsylvania State Police ed., 2003, 48.
- [31] Rudman, W., Clarke, R. and Metzel, J. Emergency Responders: Drastically Underfunded, Dangerously Unprepared Report of an Independent Task Force Sponsored by the Council on Foreign Relations, 2003.
- [32] Sawyer, S. Social Informatics: Overview, Principles and Opportunities. Bulletin of the American Society for Information Science and Technology, 31 (5). 9.
- [33] Sawyer, S., Tapia, A., Pesheck, L. and Davenport, J. Mobility and the First Responder. Communications of the ACM, 47 (3). 62.
- [34] Sawyer, S. and Tyworth, M., Integrated Criminal Justice Systems: Designing Effective Systems for Inter-Organizational Action. in Sixth Annual National Conference on Digital Government Research: Emerging Trends, (Atlanta, GA, 2005).
- [35] Scanlon, P. ARJIS: Automated Regional Justice Information System, ARJIS, 2004, 30.
- [36] Truex, D., Baskerville, R. and Travis, J. Amethodical systems development: the deferred meaning of systems development methods. Accounting, Management and Information Technologies, 10 (1). 53-79.
- [37] Truex, D.P., Baskerville, R. and Klein, H. Growing systems in emergent organizations. Communications of the ACM, 42 (8). 117.
- [38] Walker, L. Integrated Criminal Information System Trends in 2002: Communication, Collaboration, Cooperation. Courts, N.C.F.S. ed., 2002.
- [39] Williams, S.R. and Aasheim, C. Information Technology in the Practice of Law Enforcement. Journal of Cases on Information Technology, 7 (1). 71.

8. ENDNOTES

1. We use the term 'public safety' to refer to ambulance and fire services; 'criminal justice' to refer to the courts, prison, and parole systems; and 'law enforcement' to refer to police agencies. First responders are found in both law enforcement and public safety organizations.
2. See <http://www.arjis.org/>
3. For a comprehensive history of the use of ICTs in law enforcement see Dunworth, T. Information Technology and the Criminal Justice System: A Historical Review. in Pattavina, A. ed. (2005) Information Technology and the Criminal Justice

System, Sage Publications, Inc., Thousand Oaks, CA, 1-28.

4. See <http://www.usdoj.gov/jmd/mps/manual/crm.htm#content>
5. There are 2,565 individual municipalities in Pennsylvania. Additionally, Pennsylvania is a commonwealth with strong townships and relatively weak county governments. These two factors may

make Pennsylvania one of the more institutionally complex states in the Union.

6. As we complete the study, we anticipate directly mapping ARJIS activity to these principles (and in doing this engage and contributes to institutional theory).