V2.11 As of 16 Feb., 05 (5400 words, Sawyer)

From Response to Foresight: Managing Knowledge and Integrated Criminal Justice

Steve Sawyer[a]

Sara Reagor[a]

Michael Tyworth[a]

James B. Thomas[a]

[a] School of Information Sciences and Technology

The Pennsylvania State University, USA

(sawyer, jthomas, mtyworth, sreagor)@ist.psu.edu

Abstract

In this paper we report on our ongoing study of integrated criminal justice systems. Our focus here is on theorizing the nature of and arrangements among the policy issues, operational activities, and technical architectures to support knowledge sharing among personnel and across geographic and organizational boundaries. Here we draw on data from a comparative case study across three sites to report three findings. First, the aged computing infrastructures and dated technologies severely constrain the ability of criminal justice organizations to leverage information and communications technologies to support information sharing. Second, in contrast, criminal justice organizations have developed sophisticated work practices to support officer's data collection and information sharing. Third, we note the central role that dispatch plays in information sharing and knowledge transfer among criminal justice personnel.

Keywords: integrated criminal justice, knowledge sharing, knowledge-based work, sociotechnical theories, comparative case study.

Suggested Tracks:

Managing organizational knowledge and competence

The nature of knowledge work and knowledge workers

The role of information technology in knowledge management and collaboration

Public service sector approaches to Knowledge Management and Organizational Learning and comparisons with the private sector

From Response to Foresight:
Managing Knowledge and Integrated Criminal Justice

We are studying knowledge sharing and are doing so by studying the roles played by and the uses of integrated criminal justice systems. We are particularly interested in the relationships among information sharing, knowledge management and information system development and deployment. As outlined below, integrated criminal justice systems exist within an operational domain characterized by a high degree of institutional and technological complexity: one where information sharing and knowledge management is both important and difficult (Hansen, 1999).

Our intent is to theorize on the nature and arrangements among policy, operational actions, and technical architectures to support knowledge sharing. In this paper we report findings that help advance our understanding of the specific opportunities for integrated criminal justice systems in the United States. These findings also help us theorize on how polices, operations and technologies can be focused on gathering data, sharing information, and managing knowledge.

By ‘integrated criminal justice system’ we mean an information system that has four specific characteristics. First, they serve as vehicles to share (and sometimes gather) information and data among members of different criminal justice organizations. Second, in doing this these systems provide secure and authorized information access, and carefully monitor system uses and user identities. Third, integrated criminal justice systems span geographic and organizational boundaries. That is, they are neither a single institution’s resource nor do they operate solely in one jurisdiction. Finally, an integrated criminal justice system provides its subscribers or participants with communication capability (such as reporting and alerts, secure radio channels, common talk, and email). This, in turn, implies that integrated criminal justice systems provide mobile and fixed-location infrastructures and a set of services that both bridge and span legacy applications. An example of an operational integrated criminal justice system is Pennsylvania’s Justice Network (JNET)[1]

The pressures of the institutional and technological context of criminal justice in the US (and demands of operating in this environment) contributes to most integrated criminal justice systems developing as complex entities. Integrated criminal justice system development, governance and operation draw on concepts of *digital (and electronic) government* and improved *government practices* (and in particular the increasing importance of, and engagement with, information and communications technologies (ICT) and the state and local levels of government in the US). They are also increasingly a part of *homeland security* (particularly the Department of Homeland Security's emphasis on inter-operability, regional activity, and systems integration). There is a rich literature on *law enforcement and public safety* that is more recently engaging these systems and contemporary *enterprise systems,* and particularly the work of enterprise architectures and enterprise systems integration. Through this paper we make explicit several links between integrated criminal justice and the burgeoning literature on knowledge management.

The paper continues in four sections. In the next section we lay out our motivations for pursuing this research and summarize why criminal justice is an appropriate domain to pursue our work. In section two we develop our research approach, data collection and analysis effort. In section three we present and discuss current findings. In section four we reflect on the implications of these findings.

Knowledge Sharing and Integrated Criminal Justice

The United States' criminal justice system is in the midst of wholesale changes relative to the gathering, the sharing and the management of both data and information. These changes arise in large part from long-simmering issues with inter-agency territorialism regarding information sharing and cooperation (9-11 Commission Report, 2004). Second, many of these changes come in direct response to terrorist activities (real and anticipated) against the U.S. homeland over the past few years. This is due to most experts expecting that the criminal justice system (which includes police, the courts and correctional/ probations agencies) will be the primary vehicle through which to improve homeland security.

Given this context, there are at least four reasons why the criminal justice domain, is an excellent domain to study knowledge management because. First, there is demonstrated need (and interest) to share data, information and knowledge across departmental, organizational, geographic and institutional boundaries (Rudman, et. al, 2004). Second, the institutional structures are complex, often problematic, and must be accounted for in any organizational change or information systems development effort. These institutional structures lead to a current operational environment characterized in part by a confusing tradition of formal pressures to both share and not share data, information, and knowledge and a visible legacy of 'silo-oriented' computing systems (Manning, 2003). Third, there is a history of increased computerization, including recent efforts to both specifically focus on, and encourage, knowledge management and knowledge sharing (Nunn, 2001; Northrop, Kraemer, and King, 1995). Fourth, there is extensive contemporary attention to the importance of this computerization (e.g., Sawyer, Tapia, Pesheck and Davenport, 2004; Oppenheim, Stenson, and Wilson, 2004; Lin, Hu, and Chen, 2004; Dunworth, 2000).

Criminal justice in the US is a complex and overlapping tangle of federal, state and local units each charged with various aspects of prevention, detection, response, prosecution, incarceration, and education relative to criminal (and thus, terrorist) actions. The federal system of the US is very much the institutional landscape. While the central agencies such as DHS, the DoJ, and the U.S. congress draw public attention, much of the U.S. criminal justice activity is done at the local and state levels. This helps underscore the simple observation that cross-institutional activities have always been a central aspect (and concern) of any effort to do work or build systems. And, currently, there are literally hundred (if not thousands) of efforts to develop integrated criminal justice systems (Bureau of Justice Statistics, 2003; NASCIO, 2003; Taylor, Epper, and Tolman, 1998). This innovation soup is driven by funding from several federal (and state) sources, local taxes and a concern for the country's homeland security.

The contemporary U.S. efforts to improve criminal justice and homeland security mirror in many ways similar efforts in the United Kingdom (UK). The U.K. efforts to integrating criminal justice were one response to terrorist acts (by the Irish Republican Army) in the late 1980s. These efforts evolved, in the early 1990s, into a series of efforts to both integrate and provide more computing support for the national police force (I'm guessing this is what you meant). The culmination of these efforts was manifested in the creation of the U.K. Police Information Technology Organization (PITO) and its multi-pronged effort to modernize, to extend, and to integrate the systems collectively known as the Police National Computer (PNC). PNC improvements in the past three years,and the deployment of a nationwide mobile radio system (known as Airwave) provide evidence of the U.K.'s leadership in this area (PITO, 2004; Pica, 2004).

Direct comparisons between current U.S. efforts and the U.K. experience are difficult since the U.K. criminal justice system is nationalized, administered by the home office, and centrally administered (albeit with extensive local control). The institutional complexity of the U.K. criminal justice system is more driven by long histories and legal traditions than by the decentralized approaches to policing and justice as practiced in the US.

Two passing comparisons between U.K. and U.S. efforts are warranted. First, it has taken the UK nearly 15 years to achieve their current level of criminal justice systems integration. Given the substantial population and geographic size disparities, the differential approaches to criminal justice, and the similar motivations, the U.K. efforts to date are useful data points. Second, in their efforts to integrate criminal justice, the U.K.'s focus has shifted from improving response to more intelligence-based and proactive policing (e.g., National Intelligence Model, 2000). That is, their ongoing efforts to support integrated criminal justice and improved homeland security have led them to focus on ways to increase the sharing of information among personnel and to be more proactive in using information to both guide efforts and improve reaction and response (Pica, 2004).

The 15 year history of the U.K.'s work to improve criminal justice suggests that it is useful to contrast U.S. efforts with U.K. efforts to both learn from the U.K.'s work-to-date and possibly accelerate U.S. activities. The U.K.'s focus on intelligence-led policing suggests that is appropriate to focus on information sharing and knowledge management.

Research Approach and Methods

To explore issues of information sharing, knowledge management, and information system development and deployment, we pursue a multi-method research approach in which we combine secondary data and comparative case studies. In this paper we use secondary data primarily as a means of providing background, focusing instead on reporting interim findings drawn from comparing three case studies. The first two case studies are of regional U.S. efforts (in PA and CA) and the third case study is drawn from the United Kingdom (UK) activities.

In reviewing ongoing efforts we further identify two dominant approaches to developing integrated criminal justice systems: an open-standards[1] approach and a commercial-off-the-shelf (COTS) approach (Lin, et. al, 2004; NASCIO, 2003; Sawyer, et. al, 2004; Oppenheim, et. al., 2004). In Table 1 we highlight some examples of these two approaches. Our intent with this research and in this paper is to focus on the open standards efforts as the open standards model seems to be more long-term viable as a platform for the public sector's integrated criminal justice systems (e.g., NASCIO, 2003). Future efforts may be useful in comparing open standards systems to COTS.

Type of system	**COTS**	**Open Standards**
Examples	*COPLINK systems in: Tuscon, AZ, Polk County, TN….. * Motorola systems in: LA County, CA, Austin, TX …. * Oracle system (CLEAR) in Chicago, IL.	* CapWIN -- Metro DC, VA & MD * JNET -- Commonwealth of PA * Airwave/PITO -- United Kingdom * ARJIS -- San Diego, CA, area

Figure 1: Types of Operational Integrated Criminal Justice Systems

We draw on two broad forms of data collection. Secondary data is drawn from a range of sources including popular press, professional press focused on the public sector, criminal justice, and homeland security, and specific data sets available from U.S. federal sources such as the Bureau of Justice Statistics (BJS) and the National Institutes of Justice (NIJ), The National Association of State Chief Information Officers (NASCIO) and the International Chiefs of Police Association (ICPA). In this paper, secondary data serves only to help us frame the comparative case study. Case study data is collected via a combination of reports, interviews, visits, focus groups/seminars and interactions.

All of the ongoing case studies are guided by a common research framework, which we will use to study ARJIS. The common framework builds on that reported on in Sawyer,

[1] By open standards we mean the use of publicly available technologies or their underlying policies/protocols. This includes things such as XML, browsers (http, html, etc.), and published APIs.

Tapia, Pesheck, and Davenport (2004) and focuses research (and thus data collection) attention on six inter-related elements (see Table 2).

Element	*Description*
Computing infrastructure	Nature and structure of wired and wireless connection, throughput, coverage, reliability and costs.
Computing devices used	Their types, uses and characteristics.
Applications and systems software used	Their functionality, feature sets, design principles and development efforts. This includes attending to issues with security and authentication.
Information sharing	This includes the uptake, uses of, distribution and sharing patterns, needs, sources, volume, and both form and type.
Work activities	This includes both task analysis and work structuring perspectives and spans both a range of stakeholders (such as mobile and fixed-location users, dispatch, developer, administrators, …) and a range of work environments.
Governance	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).

Table 2: Research Framework

This common research framework serves as a guide for our data collection. We draw on specific conceptual frames and theories to help us organize and report on the data. For example, to describe technical architecture issues (such as network, device, application, and operations) relative to criminal justice, we draw on the work of Oppenheim, Stenson, and Wilson, (2004) to situate our analysis. Here we draw on Sawyer, et. al, (2004) to structure our exploratory analysis across these six dimensions.

To do the analysis summarized in this paper we have used traditional qualitative/case study data analysis approaches (see Miles and Huberman, 1994). In particular, we draw on two techniques: interim analysis of the data to guide both future data collection and its interpretation and explanatory event matrices. Space limitations drive us to report briefly on the case studies, deferring detailed description to other venues. In the remainder of this paper we report on several common findings and discuss their implications. All three case studies are ongoing, so this report must be seen as interim (as we noted in our short discussion of data analysis, this is a central feature of our research approach).

We draw data from case studies of two of the most ambitious U.S. efforts to support integrated criminal – Pennsylvania's Justice NETwork (JNET)[2] and the San Diego, CA Automated Regional Justice Information System (ARJIS)[3]. We consider these before all other efforts in the US to pursue integrate criminal justice systems for five reasons: both are operational (many of these systems are still in development[4]), have a large geographic scope, provide a wide breadth of jurisdictional coverage, span multiple organizational and institutional boundaries, and have common information systems architectures and designs. Together these two systems cover nearly 18 million people (about 7% of the U.S. population), bring together several thousand distinct criminal justice organizations, and have remarkably similar technical architectures. We began our case study of JNET in Spring, 2004, and ARJIS in Summer, 2004.

Our third case study is of the U.K.'s PITO. The PITO systems encompass 97% of the U.K. geography and some 60 million inhabitants. The PITO systems share the characteristics of JNET and ARJIS in that they are operational, span jurisdiction and geographical boundaries, and their technical architecture is similar to the U.S. systems. We began our case study of PITO in Summer, 2004.

Findings and Discussion

We report on and discuss here three interim findings from our comparative analysis of the JNET, ARJIS and PITO case studies:

1. The limitations, issues and pressures of infrastructure,
2. Sophisticated work practices supporting officer's data collection, and
3. The role of dispatch in information sharing.

Limitations, issues and pressures of computing and mobile infrastructures.

[2] See www.pajnet.state.pa.us for more information on JNET.
[3] See www.arjis.org for more information in ARJIS.
[4] A third system, the Capital Area Wireless Integrated Network or CAPWIN went operational in Summer, 2004. For more information on CAPWIN, see www.capwin.org.

Data are drawn from sources within each of our case studies. We observe across all three case study sites that the base technologies that support computing and operations are often antiquated, and that many of the legacy systems are difficult to maintain or upgrade. We further observe that efforts to expand these systems to support mobile access often over-extend existing (or built) wireless networks.

The base technologies on which JNET, ARJIS and PITO systems are built are each different, but all have three common characteristics. First, they are all mainframe-driven efforts. In each, the number of applications, data owners, and the ages of these assets vary. However, all grapple with the legacy that most public-sector systems face: poor funding, antiquated operational platforms, and limited internal support resulting in a reliance on a revolving series of contractors to do the support and maintenance. This legacy results in an almost unsupportable collection of computing assets. In essence, the architecture reflects a computing slum, not a planned development.

Each of the three case study sites is taking a different approach to their outmoded computing infrastructure. The JNET leadership has a federated design, focusing on data sharing among agencies who participate with no effort to engage those host systems. This data sharing uses publicly available extensible markup language (XML), internetworking protocols, active security, and a browser-based interface to users. In addition, JNET provides a more modern n-tier server architecture to support its operational activities (authentication of users, query support and reporting, and messaging).

The ARJIS system is centered on a still-evolving but 30-year old set of COBOL programs hosted on an IBM mainframe. They are now engaging in what will be a redevelopment effort to move away from the mainframe towards some form of n-tier server architecture, expand and modularize their system(s) functionality, and move more towards open standards, internetworking, and browser-based access.

The suite of systems that PITO supports (and are collectively known as the PNC) are in practice a combination of antiquated mainframe and more modern server-based applications. However, current applications development takes advantage of more modern languages and platforms. PITO continues to support the mainframe applications, though this is an increasingly problematic constraint, particularly so as they must tailor new development to interact with this legacy.

All three case study sites have or are extending their infrastructure to support mobile data and voice communications. In this area, PITO has taken a lead in that they have deployed a nationwide common wireless infrastructure. Airwave, as it is known, is an innovative public/private partnership with a U.K.-based mobile services provider (O2). In exchange for operational contracts and $5 million to support build out, 02 deployed a wireless network across the UK that meets certain quality of service requirements set in place by PITO. Police forces in the UK have access to a base set of services and each can subscribe to a suite of other services (though these cost additional money).

Both ARJIS and JNET leadership continue to explore alternatives for supporting wireless and mobile access. There are essentially three choices. The first is to use the 800 Mhz public safety frequency spectrum that is set aside in the US for such uses. The drawbacks with this approach include the limited deployment of operational 800 Mhz systems in the US and the limited bandwidth supported. A second option is to contract for mobile provisioning with private carriers such as Sprint and Verizon. The drawbacks with this option are cost and coverage. Reliability may also be an issue, as some studies of NYC mobile phone usage suggest. The third option is to develop and deploy networks based on other standards (such as mesh or broadband wi/fi). The drawbacks here include all the issues of the first two with the additional issue that these technical resolutions have not been widely deployed or evaluated. All three options have additional security and identity issues. While each option has different flavors, all are seen as suspect.

In the face of this option soup, JNET has conducted studies of public access and other uses, but has no clear forward path. In contrast, ARJIS has deferred this effort to local jurisdictions. The ARJIS system does, however, provide some functionality to mobile data terminals such as personal digital assistants and mobile data terminals (essentially ruggedized laptop computers) in police cruisers via public safety radio channels. Currently both systems (and many other like-interested units across the US) are looking to the DHS' SAFECOM department to help establish regional and national infrastructures to support secure communications infrastructures.

Sophisticated work practices supporting officer's data collection

Here we focus in particular on the work of police officers, noting in passing that the case work of probation and correctional workers is more structured. The work of police officers is (and has been) highly mobile, knowledge intensive, and pervasive. Simply, their work has always been mobile. And, until recently, limitations of most available ICT made it difficult to adequately support these workers' information needs. For example Manning (1996) reported on the large disparity between police officer's information needs and the abilities of the ICT they use to provide them that information.

In addition, policing has always been atypically adept at contingency planning, emergency handling, and articulation management. That is, one of the central tasks in policing (and other first responders) is to deal with messy, ongoing, knowledge-intensive situations. Much of the day-to-day activity of the average police officer is articulation management. We further note that criminal justice organizations traditionally place an atypically strong emphasis on training and support. Officers are trained in the use of weapons, negotiating skills, and both data collection and reporting procedures for several regularly-scheduled hours each month.

We find through our interviews, observations, and discussions that this attention to training-up and becoming expert in problem-solving and data gathering around messy incidents is common across all three case study sites. While the procedures for gathering, sharing and recording information on incidents, people, and situations varies, all three systems focused on supporting this work. We further note that far from becoming workflow applications, JNET, ARJIS and PITO applications were made as flexible as possible, with very simple interfaces and limited additional functionality. This reflects the rigors of the operational environment and the limited cognitive attention that officers can give to systems. We also learned that current efforts to develop and deploy systems often focus on extensive additional functionality that both degrades performance and distracts the user's attention.

Finally, we note that there are strong social norms that govern policing work. In the U.S. criminal justice system the orientation is towards individual autonomy. Most U.S. officers operate alone, from a police cruiser, and develop their own habits of note taking and information sharing. Since these officers tend to work with a small set of other officers and leaders, the operational network of interactions becomes an unwritten code of conduct. This localized social norms of behavior leads to subtle but very important operational differences across relatively close geographic jurisdictions. This, in turn impedes information sharing.

In the UK, police officers tend to work in pairs, with officers tending to take on more specialized roles. This leads to more standardized means for gathering and sharing information. The centralized nature of the PNC and the common use of these systems across the UK provides additional support for information sharing due to common training protocols and explicit work breakdown structures.

Role of dispatch in information sharing

The uses of JNET, ARJIS, and the PITO-provided computing resources makes clear the institutional embedding of the command and control structures in criminal justice. In particular, the critical social, organizational, and technical roles that the police dispatchers play transcends all three sites. By dispatch, we mean the use of a central office that provides communication support, information, and situational awareness to both the deployed assets in the field and senior tactical and strategic leadership.

Dispatch centers vary in size and sophistication across (and within) the three case study areas. The San Diego area centers are large and modern. The Pennsylvania dispatch centers vary from small and austere regional (multi-county) units in low-population density areas to sophisticated places that support large metropolitan areas. There is little standardization of systems across the U.S. sites, or even within the PA centers. Much of the software to support operations is home-grown or vender-supplied and varies. A *de facto* standard is the use of Motorola-made radio systems. However, radio systems made by the same vendor may not be interoperable (as is the case of the PA State Police and PA local police systems). This means that there may be two, parallel, radio systems in a police cruiser and in the dispatch center. In contrast, the U.K. dispatch centers are large, very well-quipped, places. They have a relatively standard set of systems, and even a relatively standard layout.

Each of the case studies showcased different design approaches relative to the role of dispatch. The JNET system is designed to be used by officers and essentially bypasses dispatch. This makes it difficult for officers to share information drawn from JNET with each other and with dispatch. The ARJIS system provides information both directly to the officer or to dispatch, depending on what subsystems are used. However, there is no choice in how information is routed. The PITO systems are dispatch-centric.

Information shared with officers is also available in dispatch, and can also be shared with other officers in the field.

The U.K. approach suggests that they are leveraging dispatch as a means of providing information sharing support through a hub-and-spoke arrangement. They focus on training dispatch personnel and officers to use dispatch as a key means of managing situations, searching and sharing information, and maintaining tactical and operational control. The U.S. approach suggests that designers are not emphasizing the role of dispatch, pushing instead to provide more autonomy to officers. The more limited training (and higher turnover) of dispatch center personnel in the US also suggests that their role, while clearly central from an operational and tactical perspective, is not seen as strategically central in sharing information and managing knowledge.

Implications and Speculations

We discuss three implications of these findings and speculate on their effects to professional practice and future research needs. We note the need for a more common technological infrastructure, the need for improved means to collect and share data, and the importance of engaging dispatch more actively in the design and operations of U.S. integrated criminal justice systems.

The chaotic, under-supported, and often out-dated computing infrastructure that is the basis for supporting the development and operational uses of integrated criminal justice systems hobbles their current value and significantly reduces future potential. Too often the focus is on interesting applications and possibilities of new technologies. However, evidence from three case studies supports the secondary data: the operational computing environments supporting criminal justice can barely support current operations. Investments in infrastructure, particularly computing infrastructure, are expensive (as the PITO/UK Airwave project demonstrates) and often difficult to justify (which is part of the reason why they are so chaotic). Without significant investments in base systems, the foundation of application delivery, the sharing of information and uses of data will continue to be terribly constrained.

A second implication of these findings is the need for improving data collection and information sharing. Systems in each of the three case study sites focus on delivery of more information to officers in the field. A second set of systems provide the means for system users to communicate more directly and interactively. Both of these are important next steps to developing more integrated criminal justice systems and improving homeland security. As Rudman, et. al. (2003) noted, this functionality is sorely missing in the US. The PITO/Airwave project in the UK provides a clear view of the potential of such interoperable information sharing and communication. Beyond meeting these basic (though complex to support) needs, one high-value extension to integrated criminal justice systems functionality will be means to gather data and information at sites or incidents and share this with others.

Building on the need and opportunity that integrated criminal justice systems have to expand information sharing, there are at least three reasons for engaging dispatch more actively in the design and operations of these systems. First, the distributed nature of the officers and information requires some sort of support (e.g., Heath and Luff, 1991; Whalen, 1995). This is a role which the dispatcher plays in current systems, albeit in a limited capacity (in the US) due to decisions to reduce, not leverage, their value. Second, the ability of someone to be both actively engaged in the flow of information yet able to monitor and evaluate the situation is a potentially useful asset in the design of more flexible knowledge sharing efforts. Third, the dispatcher serves as a bridge into other information sharing and decision-making loops and may be a useful connective element across incidents and over time (e.g., Whalen, 1995).

More generally, the need for a resilient and modern computing infrastructure, improved information gathering and sharing, and leveraging the role of people in positions to enable increased information sharing transcend the specific needs of integrated criminal justice and seem like viable principles for systems to support knowledge sharing in most any context.

References

Ackroyd, S., Harper, R., Hughes, J., Shapiro, D., & Soothill, K. (1996). *New Technology and Police Work*. Buckingham: Open University Press.

Alavi, M. and Leidner, D. (2001) Knowledge management and knowledge management systems: conceptual foundations and research issues, *MIS Quarterly, 25*(1), 107-136.

Bureau of Justice Statistics (2003) *Local Police Departments 2000*, U.S. Department of Justice, Office of Justice Statistics, Law Enforcement Management and Statistics Series, Report NCJ 196002, Washington, DC.

9-11 Commission Report (2004), Report of the National Commission on Terrorist Attacks Upon the United States, Government Printing Office. Available online at: http://www.9-11commission.gov/.

Cross, R. and Baird, L. (2000) Technology Is Not Enough: Improving Performance by Building Organizational Memory*, Sloan Management Review, 41*(3), 13-25.

Dunworth, T. (2000) Criminal Justice and the Information Technology Revolution, in Horney (Ed.), *Policies, Processes and Decisions of the Justice System* (Vol. 3,). Washington, DC: National Institute of Justice/Office of Justice Programs, 372-426.

Hansen, M (1999) The search-transfer problem: the role of weak ties in sharing knowledge across organization subunits. *Administrative Science Quarterly, 44*: 82-112

Heath, C. and Luff, P. 1991. *Collaborative Activity and Technological Design: Task Coordination in London Underground Control Rooms*. in *Proceedings of ECSCW'91*. (Amsterdam, Netherlands) Kluwer, 65-80.

Lin, C., Hu, P. J-H., and Chen, H. (2004). Technology implementation management in law enforcement. *Social Science Computer Review, 22*(1), 24.

Law, J. and W. Bijker. 1992. "*Technology, Stability and Social Theory." in Shaping Technology/Building Society,* edited by W. Bijker. Cambridge, MA: MIT Press: 32-50.

Luff, P. and C. Heath (1998). *Mobility in Collaboration*. Proceedings of ACM 1998 Conference on Computer Supported Cooperative Work, ACM Press.

Manning, P. (2003). *Policing Contingencies*. Chicago: University of Chicago Press.

Markus, M. and D. Robey (1988). "Information Technology and Organizational Change: Conceptions of Causality in Theory and Research." M*anagement Science, 34*(5), 583-598.

Miles, M., & Huberman, A. (1994). *Qualitative Data Analysis: A Sourcebook of New Methods*. (2nd ed.). Thousand Oaks, CA: Sage.

NASCIO, 2003, Concept for Operations for Integrated Justice Information Sharing Version 1.0, National Association of State Chief Information Officers, July, 2003. Available online at: https://www.nascio.org/publications/index.cfm.

Northrop, A., Kraemer, K., & King, J. (1995). Police Use of Computers. *Journal of Criminal Justice, 23*(3), 259-275.

National Intelligence Model (2000). The National Intelligence Model – A New Approach to Policing. U.K. Association of Police Chief Officers. Available at: http://www.policereform.gov.uk/implementation/natintellmodeldocument.html.

Nunn, S. (2001). Police information technology: Assessing the Effects of Computerization on Urban Police Functions. *Public Administration Review, 61*(2), 221-234.

Nunn, S., & Quinet, K. (2002). Evaluating the effects of information technology on problem-oriented-policing: If it doesn't fit, must we quit? *Evaluation Review, 26*(1), 81-108.

Oppenheim, C., Stenson, J. and Wilson, R. (2004) Studies on Information as an Asset III: Views of Information Professionals, J*ournal of Information Science, 30*(2), 181-190.

Pica, D., Sorenson, C. and Allen, D. (2004) On Mobility and Context of Work: Exploring Mobile Police Work, Proceedings of the 37th Hawaii International Conference on Systems Science, ACM Press. Available online at: http://csdl.computer.org/comp/proceedings/hicss/2004/2056/03/205630081c.pdf

PITO, 2003, U.K. Police Information Technology Organization Annual Report, Available at: http://www.pito.org.uk/newsroom/annual_report/html/english2003/index.html

Rudman, W., Clarke, R. and Metzel, J. (2003) "*Emergency Responders: Drastically Underfunded, Dangerously Unprepared*," Report of an Independent Task Force Sponsored by the Council on Foreign Relations, 29 July, Washington, DC. Available online at http://www.cfr.org/pdf/Responders_TF.pdf.

Sawyer, S., Tapia, A. Pesheck, L. and J. Davenport, (2004) Observations on Mobility and the First Responder, *Communications of the ACM, 47*(2), 62-65.

Taylor, M., Epper, R. and Tolman, T. 1998. *Wireless Communications and Interoperability among State and Local Law Enforcement Agencies.* NCJ 168945.

Whalen, J. 1995. *A Technology of Order Production: Computer-Aided Dispatch in Public Safety Communications,* in *Situated Order: Studies in the Social Organisation of Talk and Embodied Activities,* P. ten Have and G. Psathas (eds.), University Press of America, Washington, 187-230.

[1] For more information on JNET, see www.pajnet.state.pa.us.