The Sociotechnical Nature of Mobile Computing Work:

Evidence from a Study of Policing in the United States

Steve Sawyer, The Pennsylvania State University, USA
Andrea Tapia, The Pennsylvania State University, USA

ABSTRACT

*In this article we discuss the sociotechnical nature of mobile computing as used by three policing agencies within the United States. Mobile devices, access, and service was provided via a third-generation wireless network to a focal application, Pennsylvania's **J**ustice **NET**work (JNET), a secure Web-based portal connecting authorized users to a set of 23 federated criminal justice and law enforcement databases via a query-based interface. In this study we conceptualize mobility and policing as a sociotechnical ensemble that builds on the social-shaping of technology perspective and the tradition of sociotechnical theorizing, focusing on the co-design of work practices and technologies to support work. Drawing from the social informatics tradition, we turn a critical, empirical, and contextual lens on the practices of mobility and work. Our analysis of the data leads us to observing that the social and the technical are still considered separately in the context of mobile work. This simple view of social and technical as related, but distinct, often leads to problems with collecting and interpreting evidence of ICT-based systems' design and use. We further note that this over-simplification of sociotechnical action is likely to continue unless more viable analytic approaches are developed and the assumptions of the current techno-determinist approaches are challenged more explicitly.*

Keywords: field trial; mobility; policing; sociotechnical analysis

INTRODUCTION

One of the many alluring possibilities of mobile computing is that people will be able to access computing resources while on the move. In organizational contexts, mobile computing (or mobility as we refer to it here) engenders scenarios of increased productivity through instant access to computing resources at any time from anywhere. Here we explore the sociotechnical nature of this envisioned future for mobility. In the social informatics tradition, we turn a critical, empirical, and contextual lens on the practices of mobility (Kling, 1999, 2000; Sawyer & Eschenfelder, 2002).

We first explain why policing is an appropriate domain in which to explore mobility and work. We then conceptualize mobility as a sociotechnical ensemble. In subsequent sections we lay out the research, outline our data collection and analysis, and then present and discuss seven findings. We conclude by focusing on implications regarding sociotechnical analysis.

Why Focus on Policing?

There are at least three reasons why policing is an appropriate domain for studying mobility. First, police officers' work has always been highly mobile. It is also knowledge-intensive and pervasive (for more on this, see Manning, 2003). Second, there continues to be great interest in using ICT to better support police officers' information needs. For example Manning (1996), in his study of cellular phone take-up among police, reported on the long-standing disparity between police officers' information needs and the abilities of the ICT used to provide them that information.[1] Third, policing and criminal justice have long been a focus of academic study; that provides us with extensive literature on police work, the social norms, informal and formal organizational governance mechanisms, and an understanding of their technological basis (see Manning, 1977; Klockars & Mastrofski, 1991; Manning, 2003)[2].

Current research findings provide contrary views as to whether the take-up of ICTs is driving the organization and structure of police departments, or if it is the reverse (Manning, 2003; Lin, Hu, & Chen, 2004; NASCIO, 2003; Taylor, Epper, & Tolman, 1998). Evidence is clear that the uptake of new computer-based systems and uses of mobile technologies (beyond the nearly omnipresent radio communications suite in most cars and with most police officers in the U.S.) is accelerating in the U.S. (Nunn, 2001). Partly, this attention comes in response to the country's increased attention to Homeland Security (Rudman, Clarke, & Metzel, 2003), though efforts to improve policing through advanced computing pre-date current attention (Northrup, Kraemer, & King, 1995). The limited functionality and advanced age of many criminal justice and police systems further magnify this attention (Brown, 2001).

Contemporary research also suggests that police are open-minded about new technologies (wireless and otherwise) and generally view favorably the potential of new technologies to change policing (Nunn & Quinet, 2002; Lin et al., 2004). In fact, the evidence shows that most police departments across the United States have one- to three-year plans either to implement wireless technology or have already implemented some form of wireless technology (Dunworth, 2000). To support these efforts, both the United States departments of Homeland Security (DHS) and Justice (DoJ) provide a range of grants to support information technology innovations in police departments throughout the nation. In addition, there is funding by local jurisdictions and a variety of other sources, including internally generated revenue, such as fines, to support technological innovation.

MOBILE COMPUTING AS A SOCIOTECHNICAL ENSEMBLE

Sociotechnical perspectives focus both conceptual and analytical attention on three concepts: that which is social, that which is technical, and their interrelations. In our study of mobile access to computing resources for police work, the sociotechnical perspective helps us to highlight that mobility is a complex and interdependent set of relations among people (workers and managers), their organizational rules and roles, and various computing resources (such as the technical aspects of the mobile infrastructure, devices used, information sources, and applications accessed). Following Orlikowski and Iacono (2001), we conceptualize mobile access to computing resources as an *ensemble* comprising the wireless network, access devices, applications being used, information and data (both structures and content), procedures followed, norms of behavior (relative to events, systems, and others), governance structures, and both institutional and environmental constraints.

Conceptualizing mobility as a sociotechnical ensemble helps highlight the nuanced and multi-faceted interdependencies uniting people, what they do with computing resources, and how they are designed and used. We further argue that what is social and what is technical are engaged in certain times and places and in certain ways. Thus, we build on the work of policing by focusing on specific events and situate these events in specific times and places. This contextual frame provides us the means to ground the analysis of the sociotechnical interactions.

The particular interactions among these constructs will likely vary by situation. For example, in a routine[3] event such as a traffic stop, these constructs are tied together in a prescribed way. There are policies regarding the use of the car and personal (attached to the officer's uniform) radio, a standard set of practices that guide the set of interactions the officer has with both the police dispatcher and with the driver of the car being stopped, particular rules about the information needed from police resources (such as registration, license plate numbers, car details, and even data on the driver based on the driver's license proffered to the officer), and what data the officer can and should collect. Escalation procedures are proscribed, and these vary based on time of day, assessments of the local situation, and other operational considerations.

For instance, imagine that a sergeant[4] sees a pick-up truck speeding down a breakdown lane to avoid stopped traffic in the travel lanes and gives a chase. The drivers of the truck see the police car chasing them and, as is customary in the U.S., pulls over to the side of the road. The sergeant sees that the driver is agitated to the point where he is cursing out the vehicle's window; the truck is shaking from "omnidirectional fury," and the sergeant and calls for backup from his car radio. While waiting for backup, the officer puts on black leather gloves (in case they scuffle), unsnaps his weapon's securing strap (in case it goes beyond scuffling), calls in to police dispatch with vehicle information, and then switches to his body radio, talk activated. With the radio live (and all other officers on that frequency quiet, and the police dispatcher dispassionately updating time until backup arrives)[5], the sergeant approaches the upset driver and starts the (relatively prescribed) process of gathering particular information on the driver's identity as the first step in writing up a traffic citation. The backup officer arrives while the sergeant is confronting the driver, pulls up diagonally in front of the stopped pickup (to reduce the possibility of a "drive-off"), and stands in plain view and direct line of sight to the driver, weapon at the ready.

A more common traffic stop will have less drama for the driver (but perhaps some irritation), may not require backup or bring out the visible presence of force, and likely does not escalate until the driver receives multiple citations. But both traffic stops engage the same set of devices, applications, network, common information, and data flows; draw on the same governance structures; follow the same set of procedures (albeit down differing paths, but paths stemming from the same procedural guides); and reflect common and well-developed norms of policing behavior (norms both explicitly taught through extensive training, and also learned and reinforced by doing policing).

Conceptualizing mobility and policing as a sociotechnical ensemble builds on the social-shaping of technology perspectives developed by Bijker (1995), Law and Bijker (1992), and Bijker et al. (1987). In making this point, we acknowledge that there are several active streams of sociotechnical research/theorizing (see Horton, Davenport, & Wood-Harper, forthcoming). For example, the European tradition of sociotechnical theorizing, which we build on here, takes a social shaping of technology (SST) perspective. The SST perspective highlights that the material characteristics and actions of any technology are shaped by the social actions of the designers, the specific uses of that technology, and the evolving patterns of use over time. A second, work-studies tradition of sociotechnical theorizing focuses on the co-design of work practices and technologies to support work. This co-design perspective has been taken up in North America and evolved in two ways. The first is a benign neglect of the interaction between what is social and technical, leading to an evocation of the concepts without a concomitant analytical activity (see Scacchi, 2004, for a critical discussion). The second, an SST approach, is more recent and reflects social informatics in that the efforts are focused on developing specific analytic approaches that make explicit aspects of the social, the technical, and their interaction (**see Kling, McKim, & King, 2001**).

Rather than focusing on a specific theoretical approach to examining the sociotechnical action of policing and mobility, we use Bijker's (1995) principles of sociotechnical change theory to illustrate the generic goals of this approach, and to discuss the theoretical tensions that exist in sociotechnical IT research. These tensions provide a range of possibilities for specific sociotechnical research efforts. Here we use them as orienting principles for our conceptualization of mobility and the consequent design of our research, data collection, and analysis.

Bijker's (1995) four principles of sociotechnical change theory are derived from work in the sociology of technology. These four principles provide a set of goals for any theory that strives to take a sociotechnical perspective: the *seamless Web* principle, the principle of *change and continuity*, the *symmetry* principle, and the principle of *action and structure*. The seamless Web principle states that any sociotechnical analysis should not *a priori* privilege technological or material explanations ahead of social explanations, and vice versa. The principle of change of continuity argues that sociotechnical analyses must account for both change and continuity, not just one or the other. The symmetry principle states that the successful working of a technology must be explained as a process, rather than assumed to be the outcome of "superior technology." The actor and structure principle states that sociotechnical analyses should address both the actor-oriented side of social behavior, with its actor strategies and micro interactions, and structure-oriented side of social behavior, with its larger collective and institutionalized social processes.

While Bijker's principles provide a set of ideals for sociotechnical research to strive for, in practice they illustrate tensions to be managed in the research process. Given the space limitations, in the analysis to follow we focus on highlighting findings relative to our concepts and not specifically examining how the four principles guide this work.

EVIDENCE FROM A FIELD TRIAL OF POLICING, COMPUTING, AND MOBILITY

To explore the sociotechnical perspective on productivity and the effects on work due in part to pervasive access to computing resources, we report on a field study[6] of police officers' uses of an integrated criminal justice system accessed via the public wireless data network from laptops and personal digital assistants (PDAs) provided to the participants. Each element of our field trial is discussed below.

Mobile access for this trial was done via a third-generation (3G) data network. In the U.S., 3G networks are rolling out (typically based on population density) and mirror the cellular phone network in terms of coverage. However, 3G networks use Internet protocols, packet switching (and, thus, digital packets), spread-spectrum transmission (which is inherently more secure than cellular and 2G standards), and can sustain throughput speeds of up to 150 kilobits per second. The 3G data networks in the U.S. are private, and multiple providers compete directly in each market. While wireless coverage is extensive, no one carrier provides complete coverage of the geography of the U.S., and there may be gaps in service within covered areas. Moreover, collectively, all providers' coverage does not cover the geography of the U.S., and a service gap in one provider's coverage is not alleviated by the coverage of a second. The major carriers in the U.S. have deployed their 3G networks in different ways and at different rates[7]. Generally, though, they have focused on deploying in areas where that are most populated (cities and suburbs) and most traveled (along major highways). Costs, reliability, and coverage vary greatly in all other areas (Federal Communications Commission, 2002).

The focal application was Pennsylvania's *J*ustice *NET*work (JNET)[8], a secure Web-based portal connecting authorized users to a set of 23 federated criminal justice and law enforcement databases via a query-based interface. The JNET architecture is characterized by four elements. First, and as noted, for the user it acts as a portal to the criminal-justice-related databases of the Commonwealth of PA (and the U.S. Federal government). The data are owned by the relevant state or Federal agency (e.g., Pennsylvania's Department of Transportation, or PennDOT, maintains driver's license records and a picture database), and JNET provides query-based access to the driver's license photos. Second, JNET is a secure system. Users are carefully vetted before they get access, their use is tied to specific roles, and these roles grant them varying levels of access to the range of data available. Further, use is tied to secure connectivity (enabled through encryption and virtual private networks); this requires several forms of identification to be used[9]. Users must also re-authenticate periodically during their sessions in order to assure security during use. Furthermore, re-authentication is required when accessing certain specific databases through JNET. Until the field trial we report on here, there was no mobile access: thus, security was done via fixed lines and desktop computers. Third, JNET also provides electronic messaging, e-mail, and reporting functions for users. These functions serve as both a common message board across all criminal justice personnel in PA. The e-mail alerts provide a means for people to keep track of activities where they have some interests. For example, it is possible for a parole officer to set up a query on a particular name, social security number, or case number(s). If that name or those numbers come across the message board, she will be alerted and can more easily follow up on the parolee. Fourth, JNET has been operational since early 2000, and it supports thousands of queries each month (and use has grown by nearly 10% per month since inception) (JNET, 2004)[10].

The third part of the mobile access to JNET is the device being used to provide mobile access to JNET (and to the Internet more broadly). This device must have a special 3G modem card and needs to be mobile. Most police cruisers have an integrated laptop, making this seemingly a trivial effort (put in the wireless modem card, load on the security software, and use a browser). However, there were a number of operational and legal issues that made this a nontrivial effort. For example, many of the laptops are not equipped with space to load the modem card. Battery draw on police cruisers is substantial, and this further limits laptop use (and the 3G modem cards draw substantial power to run the antenna and maintain connectivity). Moreover, some cruisers' laptops have other software whose security and operational/ licensing requirements precluded additional applications from being added.

For officers not in a cruiser, the mobile device must be carried on their person. Again, this is not a trivial effort, considering that almost every square inch of the average police person's body is covered by some piece of gear. Moreover, the combination of current equipment (including communications, weapons, body armor, etc.) is nearly 25 pounds. This means that the mobile device must often displace something the officer already carries. We return to this discussion later in the article.

FIELD TRIAL DESIGN, DATA COLLECTION, AND ANALYSIS

The field trial's design focused attention to collecting data on the *wireless network's* use, *device* uses, *JNET* and other *applications'* uses, *information and data sharing*, changes or alterations to police officers' *work practices* (particularly changes to infield operations), *social norms* on computing/uses (particularly regarding the value and importance of both mobile access and JNET), and the officer's operational *governance* (particularly the role of dispatch). As we noted at the article's outset, in focusing on criminal justice, we leverage the extensive knowledge of policing and also partially control for industrial (extra-organizational) factors by staying within one work domain.

The field trial also served as an intervention: mobile workers[11] were provided with either a laptop or a personal digital assistant (PDA)[12] and secure access to the public 3G network. This was done in two phases for pragmatic reasons. The first phase lasted three months, included five participants, and focused on laptop usage. The small number allowed us to refine data collection protocols, and ensure that we could meet the technological demands of supporting the access, security, and application use demands of a demanding operational environment. The second phase began directly after the first phase's completion, involved 13 participants, lasted three months, and focused on PDA usage. All five of the participants in the first trial were part of the second trial. This provided us with a subset of users who were engaged in mobile access to JNET for six months. The two-phase trial's six-month duration was guided by practical constraints of users' ability to participate in a trial while doing their normal policing and official duties. The number included in the trial was constrained by the costs of providing devices, connectivity, and support to the officers.

Participants in both trials were police and other criminal justice officers from three organizations (one county level and two local level) located within one Pennsylvania county. Two incentives were used to motivate participants. First, we promised that all participants could keep the mobile device(s) they were given to use (late-model laptops and high-end PDAs, both equipped with 3G modem cards; and in the case of the PDA, an external sleeve and battery pack to support the modem card). Second, we made it clear that the participants' input would be used to drive the design of JNET for criminal justice uses, particularly for mobile access. Participants mentioned that both were important to their deciding to engage. In addition, we worked with the department heads and unit police chiefs to ensure that officers were given official recognition for engaging in the field trial. Participating department heads and unit police chiefs were both enthusiastic and supportive.

We used seven forms of data collection. First, we did pre- and post-interviews (at the beginning and end of each trial periods) of all users. In phase one these were face-to-face, open-ended, and semi-structured interviews that lasted from 60 to 90 minutes. In phase two, we used a more structured, self-administered survey in place of some of the open-ended user interviews and followed up with a phone discussion. Second, we led focus groups of users following the trials. These were voluntary, and only two participants did not participate (for schedule reasons). Third, all users completed a one-week time diary of work behavior during the field trial. Fourth, members of the research team did ride-alongs with users. We chose to ride-along with both police and court officers, and with both supervisors and patrol officers. Fifth, we gathered documents during all interviews, observations, and visits (and did extensive Web and library research to support the field work). Sixth, we engaged in informal weekly interactions (via phone, e-mail, and in person) with users. Finally, we gathered data about laptop uses, wireless data transmission, and JNET usage via unobtrusive means (such browser logs, server logs, and telecom activity logs). Data from the first six sources were either transcribed into digital format or collected at source in digital format. Data from the usage logs came in digital format.

Our analysis focused on identifying issues with the 3G network's connectivity/reliability, speed and access, uses of JNET (and other sources/applications), information and data access, and the roles of the mobile devices. This was done through analysis of data drawn from the trouble-ticketing log, analysis of time use (drawn from the logs) regarding connection via 3G networks, volume of data transfer and time/usage of JNET, and through a series of topical analyses of the texts created from the six forms of intensive data collection.

Analysis of data regarding information and data sharing, work practices, social norms, and operational governance followed traditional qualitative data analysis approaches (see Miles & Huberman, 1994). In particular, we used three techniques: interim analysis of the data to guide both future data collection and its interpretation, explanatory even matrices, and content analysis of the transcripts, logs, and field notes.

FINDINGS

We present and discuss seven findings. We find that police officer's uses of 3G *wireless networks* is dependent more on coverage and reliability of access than on speed (bandwidth). Certainly, higher throughput speeds are better than lower speeds (particularly when transferring driver's license photos, as we discuss below). However, if coverage is not certain, then officers either forget to access the network, or become frustrated and actively choose to NOT access the network. Moreover, if an officer takes the time, cognitive energy, and effort to connect, and the access attempt fails (for any number of reasons), it appears they quickly cease trying.

We find that the police officers in our study do not value laptops as access *devices*. They do, however, appreciate these devices for other activities (such as writing up their incident reports and other tasks that did not require them to have wireless access). Police officers valued PDAs to an even greater degree. Again, these *devices* are valued for personal information management and not as connective devices to the 3G network. We did not attempt to trial pen-based or tablet computers: we suspect that these may combine the portability of a PDA with the power and screen size (an important issue for officers) of a laptop.

The mobile access to and uses of *JNET* and other *applications* was difficult to assess for two reasons. First, the low reliability of the network coverage made it difficult for officers to access these applications. The officer had to become very familiar with coverage patterns (that is, where they could and could not gain access) and then be able to adjust their work patterns to accommodate this coverage. Second, authentication and security overhead in access complicated the logon procedures and caused connection drops. The two factor logon procedures made it difficult for officers in the field to manage both connection and conduct their work. The design of JNET (which asks for updates on passwords and re-authentication as different databases are searched) meant that it was easy for JNET to shut down the session unless the officer devoted considerable attention to managing the interaction. This considerable attention to JNET had to come at the expense of attention to other aspects of the officer's work. In any operational event (such as a traffic stop) the officer would not make this commitment.

Despite this difficulty, officers value JNET for its ability to provide them *information* about drivers, particularly the driver's license photos and drivers' records. On this (and limited evidence of this) alone, officers prized mobile access to JNET and found value in mobility. We did not see any changes in *information and data sharing* for at least two reasons. First, the design of JNET for mobile access is to provide it to officers, and not through police dispatch. Most all other information and data sharing, however, goes through police dispatch (both in a controlled voice-based interaction and via current text-based systems that come to the police vehicle's onboard laptop).

We saw little changes to police officers' *work practices*. Perhaps this is not surprising — the operational environment of policing is harsh, and sometimes fatal. Police train extensively, continually, and with great care to develop procedures to take an ambiguous situation and make it less so. Changes in operational procedures are, thus, slow to come, painstakingly thought out, and must be demonstrable improvements. If not, police are unlikely to risk their lives.

The great enthusiasm and interest on the uses of computing to improve policing seems to be one of the strong *social norms* that police carry forward (Manning, 2003). However, when confronted with changes to operational procedures and concerns with the computing system's reliability, the social norms of policing operations such as safety, professionalism, and force projection overwhelm the potential value of mobile access to computing resources that cannot be consistently demonstrated.

The trial of mobile access to JNET and other computing resources amplified the institutional embeddedness of the command and control structures in policing. In particular, the critical social, organizational, and technical roles that the police dispatcher plays came clear during this trial. The design of JNET for individual access does not work well within police officers' operational *governance*. Were JNET to be a dispatch-based access model, however, governance and information sharing would likely change more quickly.

A SOCIOTECHNICAL ACTION PERSPECTIVE

In this section we draw on Bijker's (1995) four principles of sociotechnical change theory to help us reflect on and interpret these seven findings (see Table 1). Building on this reflection and interpretation, we raise three points: that the sociotechnical principles were supported by these findings; that simplistic approaches to engaging the sociotechnical nature of mobility may make it hard to interpret the results; and that there is a dire need for more substantive sociotechnical analysis techniques.

Table 1. Sociotechnical analysis

Findings	Principles	Comments
Coverage and reliability of access more important than speed/bandwidth	Seamless Web	Technological features (bandwidth) were seen as more central than operational needs of officers (operational reliability).
PDA valued for personal use, not for mobile access	Symmetry	Take up of the device is a social decision, shaped by technical characteristics, and often made for personal needs.
JNET and other *applications* are used when mobile	Change and continuity	The expectation that JNET would be valuable for mobile officers (as it has been for officers via fixed access) was borne out in the study.
Officers value *information* drawn from *JNET*	Change and continuity	The expectation that information received while mobile would be valued was borne out in the study.
No changes in *information and data sharing*	Actor and structure	Social and operational structures seemed to be resilient to new technologies of access and use.
No changes to police officer's *work practices* and *social norms*	Actor and structure	Work practices seemed to be resilient to new technologies of access and use.
No changes to work *governance*	Actor and structure	Governance structures seemed to be resilient to new technologies of access and use.

The premise of this field trial was that technological factors, such as mobile connectivity and higher bandwidth, would be central to taking up mobility. This violates the seamless Web principle. The findings suggest that the institutional structures which help to govern the work of policing serve as powerful moderators to both taking up and taking advantage of mobility. It appears, however, that the technological belief of connection and bandwidth were privileged, relative to these institutional structures. It appears from these findings that moving out access to high-value resources (from fixed to mobile connection) is valued, supporting the principle of change and continuity. However, the structural and institutional forces severely constrain action, and the promised performance of the devices, mobile access, and information sharing require more agentic effort than police officers have.

Second, we observe that the current professional practice of evaluating new ICT does not seem to engage sociotechnical principles. For example, the failure to fully engage sociotechnical principles when designing and trialing mobile access to JNET reflects a naïve view of sociotechnical action: that social and technical are distinct of one another (and that change in one leads to change in the other). The findings we note above are not surprising; current institutional structures in policing were not considered (or, worse, ignored — as was the case with dispatch) when designing new work technologies. And, the technological elements must be considered on par with social elements — had this been more carefully considered, bandwidth would not have been the focus; it would have been reliability.

The field trial design reflects the collaboration between wireless service providers, device manufacturers, local and state police and information technology leaders, and faculty. That the resulting trial underplayed the sociotechnical issues leads us to theorize that organizational decision makers, users, and technology evaluators' orientation towards problem solving will make it attractive to focus on matching technical features with work and organizational needs. In doing this they are not likely to address the systemic interactions or to consider extended interdependencies. In essence, this simplification in analysis comes at the cost of accuracy in implementation.

Sociotechnical approaches, such as Bijker's (1995) four principles, appear more likely to be applied in *post-hoc* analysis. They become a comfortable frame for scholars to use. However, they are at best a weak analytic structure to base proactive action. That is, the principles are useful to frame and interpret evidence, but are difficult to use in guiding specific designs. What is missing are the intermediate-level guidance linked to specific technologies or specific social actions. In the absence of this intermediate-level guidance, the principles are difficult to apply proactively.

Building on this, it seems important, if not imperative, that sociotechnical models provide more intermediate guidance. By this we mean support for constraints and enablers tied to particular social actions or that highlight elements of particular technologies. This intermediate level of sociotechnical knowledge is likely to be represented as contingent or localized models. In doing this, such localized models will help academics and practicing professionals more directly to dominant patterns of interactions and consequences, and make these findings available in ways that more directly influence ICT/systems design and organizational decision making.

Our final observation from this analysis is that the over-simplification of sociotechnical action is likely to continue unless more viable analytic approaches are developed and the assumptions of the current techno-determinist approaches are challenged more explicitly. Given this view, it seems likely that organizational decision makers, users, and ICT designers will have trouble making sense of evidence drawn from failed attempts to implement and use ICT based on their simple views of ICT use, cause and effect. We believe the inability to understand this data is driven by the unsound approach of invoking direct effects of ICT use, not by the measurements taken or instruments used to gather evidence (e.g., Sawyer, Allen, & Lee, 2003).

While the research literature focused on the effects of ICT highlights on the indirect and often nuanced relationships among use of ICT and performance, professional practice continues to press for the direct effects model of ICT value. This suggests that more robust system or contingency models of ICT effects are needed (e.g., Avgerou, 2002). This is one of the most active areas of scholarship in IT, and this activity needs to enter the texts, teaching cases, and classrooms of the next generation's IT leaders, organizational managers, and technology developers. For example, those who have focused specifically on the roles of mobile and fixed location uses of ICT in policing all note that the operational value derived from using new ICT-centric information systems is minimal, if discernible (Ackroyd, Harper, Hughes, Shapiro, & Soothill, 1996; Dunworth, 2000; Meehan, 2000).

What seems important to us is a more focused effort to engage the principles of sociotechnical action in direct comparison to the bases of direct effects models (e.g., Kling & Lamb, 2000). They develop a comparative analysis of tool and Web models of computing relative to organizational activity. In doing this, they highlight both the seamless Web principle (privileging neither the social nor the technical) and the principle of action and structure by highlighting the concept of a social actor — one that has agency, but constrained by institutional structures (Lamb & Kling, 2003). Building on these two principles, in the work reported here we provide a means of representing the principle of change and continuity by explicitly linking elements of the technical structure of JNET, the institutional structures of police work, and the actions of police.

REFERENCES

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

Avgerou, C. (2002). *Information systems and global diversity*. Oxford: Oxford University Press.

Bijker, W. (1995). *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change*. Cambridge, MA: The MIT Press.

Bijker, W., Hughes, T., & Pinch, T. (1987). *The social construction of technological systems*. Cambridge, MA: The MIT Press.

Brown, M.M. (2001). The benefits and costs of information technology innovations: An empirical assessment of a local government agency. *Public Performance & Management Review, 24*(4), 351-366.

Dunworth, T. (2000) Criminal justice and the information technology revolution. In Horney (Ed.), *Policies, processes and decisions of the justice system* (volume 3, pp. 372-426). Washington, DC: National Institute of Justice/Office of

Justice Programs.

Horton, K., Davenport, E., & Wood-Harper, T. (2005). Exploring sociotechnical interaction with Rob Kling: Five 'big' ideas. *Information, Technology and People,* (in press).

JNET. (2004). Usage statistics. Retrieved from: *http://www.pajnet.state.pa.us/pajnet/site/default.asp*

Kling, R. (1999). What is social informatics, and why does it matter? *D-Lib Magazine, 5*(1). Retrieved from: *http://www.dlib.org:80/dlib/january99/kling/01kling.html*

Kling, R. (2000). Learning about information technologies and social change: The contribution of social informatics. *The Information Society, 16*(3), 217-232.

Kling, R. & Lamb, R. (2000). IT and organizational change in digital economies: A sociotechnical approach. In B. Kahin & E. Brynjolfsson (Ed.), *Understanding the digital economy: Data, tools and research*: Cambridge, MA: The MIT Press.

Klockers, C. & Mastrofski, S. (Eds.). (1991). *Thinking about police: Contemporary readings*. New York: McGraw-Hill.

Lamb, R. & Kling, R. (2003). Reconceptualizing users as social actors in information systems research. *MIS Quarterly, 27*(2), 197-235.

Law, J. & Bijker, W. (1992). Technology, stability and social theory. In W. Bijker (Ed.), *Shaping technology/building society* (pp. 32-50). Cambridge, MA: The MIT Press.

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

Manning, P. (1977). *Police work: The social organization of policing*. Prospect Heights, IL: Waveland Publishing.

Manning, P. (1996). Information technology in the police context: The 'sailor' phone. *Information Systems Research, 7*(1), 275-289.

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

Meehan, A. (2000). The transformation of the oral tradition of policing through the introduction of information technology. *Sociology of Crime, Law and Deviance, 2,* 107-132.

NASCIO (National Association of State Chief Information Officers). (2003). Concept for operations for integrated justice information sharing version 1.0. Retrieved from: *https://www.nascio.org/publications/index.cfm*

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

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

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.

Orlikowski, W. &. Iacono, S. (2001). Desperately seeking the "IT" in IT research — A call to theorizing the IT artifact. *Information Systems Research, 12*(2), 121-124.

Rosenbach, W. & Zawacki, R. (1989). Participative work redesign: A field study in the public sector. *Public Administration Quarterly, 43,* 111-127.

Rudman, W., Clarke, R., & Metzel, J. (2003, July 29). *Emergency responders: Drastically underfunded, dangerously unprepared.* Report of an independent task force sponsored by the

Council on Foreign Relations. Retrieved from: *http://www.cfr.org/pdf/Responders_TF.pdf*

Sawyer, S. & Eschenfelder, K. (2002). Social informatics: Perspectives, examples, and trends. In B. Cronin (Ed.), *Annual review of information science and technology* (volume 36, pp. 427-265). Medford, NJ: Information Today Inc./ASIST.

Sawyer, S., Allen, J., & Lee, H. (2003). Broadband and mobile opportunities: A sociotechnical perspective. *Journal of Information Technology, 18*(2), 11-35.

Sawyer, S., Tapia, A., Pesheck, L., & Davenport, J. (2004). Observations on mobility and the first responder. *Communications of the ACM, 47*(2), 62-65.

Taylor, M., Epper, R., & Tolman, T. (1998). *Wireless communications and interoperability among state and local law enforcement agencies*. Report 168945 of the National Criminal Justice Clearinghouse, Washington, D.C.

ENDNOTES

[1] Manning (1996) focused on the take up and uses of cellular phones by police. Personal cellular phone ownership and use is now common among criminal justice officers. While the take up and use of a cellular phone is beyond the scope of this article, two attributes are worth noting. First, the officers use their own (personal) cellular phones and do not consider them as part of their professional equipment. Second, personal use has made officers aware of issues with wireless coverage, reliability, and use.

[2] Given the extensive literature on policing, in this article we draw from but do not develop or discuss principle findings. Instead, we refer the interested reader to anthologies of such work (listed in our references and cited here). The interested reader can also find courses in crime, law, and justice offered in most sociology departments, and the extensive material on the Web in locations such as the U.S. Department of Justice, the UK Home Office, and the International Association of Chiefs of Police.

[3] Perhaps one of the more difficult parts of a police officer's job is to remember that even a seemingly common thing such as stopping a speeding car may lead to armed confrontation. Thus, training is focused on preventing common from becoming routine.

[4] Policing in the United States is organized along paramilitary lines. Thus, sergeants are senior/experienced officers, typically with both patrol and supervisory responsibilities.

[5] Most police in the United States work alone, which means: 1) they rely on the radio as a link to others and 2) the police dispatcher is a critical node in this linkage. The radio stays on, and no one else speaks so that all can listen for a gunshot or the words "officer down."

[6] Our research design here builds on previous public-sector field studies of work (Rosenbach & Zawacki, 1989).

[7] Details of the debate and key issues in wireless network deployment, coverage, access,and use are beyond the scope of this article.

[8] For more information about JNET, see www.pajnet.state.pa.us.

[9] Security in the trial was done via "two-factor" identification. This means having a physical key, called a dangle by the officers, that stores a digital record identifying the owner that is tied to a logical password that must be entered when the physical key is connected (via USB port) to the computer.

[10] JNET is one of the earliest and most visible examples of a small and growing

number of these integrated criminal justice information systems that are a focus of homeland security efforts in the United States. Others include the Capital Area Wireless Integrated Network (CAPWIN, see www.capwin.org), the automated regional justice administration system (ARJIS, see www.arjis.org),and a fast-growing number of municipal efforts such as systems in Chicago, IL;Montgomery County, MD; and Los Angeles County, CA.

[11] Participants included one sergeant (or shift supervisor), nine patrolmen, and three deputies (of the court). Participants were male from ages 28 to 45. The average work experience was 11 years; the most experienced officer had 18 years of work and the least experienced officer had seven years of work.

[12] Laptops and PDAs were provided to officers as an incentive to participate and were paid for by the research team.

Please provide current bios