

A revised version of this is published as: Tapia, A. and Sawyer, S. (2006) "The Sociotechnical Nature of Mobile Computing Work: Evidence from a Study of Policing in the United States," in Stahl, B. (Ed.) *Issues and Trends in Technology and Human Interaction*, Idea Group Publishing, Hershey, PA., 152-171.

THE SOCIOTECHNICAL NATURE OF MOBILE COMPUTING WORK: EVIDENCE FROM A STUDY OF POLICING IN THE UNITED STATES

Steve Sawyer
School of Information Sciences and Technology
301F IST Building
The Pennsylvania State University
University Park, PA 16802
Email: sawyer@ist.psu.edu
Phone: 814-865-4450

Andrea Tapia
School of Information Sciences and Technology
329G IST Building
The Pennsylvania State University
University Park, PA 16802
Email: atapia@ist.psu.edu
Phone: 814-865-1524

ABSTRACT:

In this paper 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 Justice **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 find that the social and the technical are still separate in this mobile work context. This simple view of social and technical as related, but distinct, often leads to problems with collecting and interpreting evidence of ICT-based system's design and use. We further note 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 challenged more explicitly.

Keywords: Mobility, Policing, Field Trial, Sociotechnical

THE SOCIOTECHNICAL NATURE OF MOBILE COMPUTING AND WORK: EVIDENCE FROM A STUDY OF POLICING IN THE UNITED STATES

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 and Eschenfelder, 2002, Kling, Rosenbaum and Sawyer, 2005, Sawyer, Wigand, and Crowston, 2005).

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, 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 officer's 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 officer's information needs. For example Manning (1996), in his study of cellular phone take-up among police, reported on the long-standing disparity between police officer's information needs and the abilities of the ICT used to provide them that information¹. Third, policing and criminal justice have long been a focus of academic study and that provides us with extensive literatures on police work, the social norms, informal and formal organizational governance mechanisms, and an understanding of their technological basis (see Manning, 1977, Klockars and Mastroski, 1991, Manning, 2003)²

Current research findings provide contrary views as to whether the take up of ICT are driving the organization and structure of police departments, or if it is the reverse (Manning, 2003, Lin, Hu and Chen, 2004; NASCIO, 2003; Taylor, Eppler and Tolman, 1998). Evidence is clear that the uptake of new computer-based systems and uses of mobile technologies (beyond the nearly omni-present radio communications suite in most cars and with most police officers in the US) is accelerating in the US (Nunn, 2001). Partly, this attention comes in response to the country's increased attention to Homeland Security (Rudman, Clarke and Metzel, 2003), though efforts to improve policing through advanced computing pre-date current attention (Northrup, Kraemer and King, 1995). The limited functionality and advanced age of many criminal justice and police systems further magnifies 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 and 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 inter-relations. 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 inter-dependencies uniting people and what they do with computing resources and how they are designed and used. We further 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 routine³ 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 sergeant⁴ sees a pick-up truck speeding down a breakdown lane to avoid stopped traffic in the travel lanes and gives chase. The drivers of the truck sees the police car giving chase and, as is customary in the US, 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 'omni-directional fury,' 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 back-up 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 back up 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, 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).

We acknowledge that there are several active streams of sociotechnical research/theorizing (see Horton, et al, 2005). 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. Conceptualizing mobility and policing as a sociotechnical ensemble builds on the social-shaping of technology perspective (SST) (MacKenzie and Wajcman, 1985; Mackay and Gillespie, 1992; Bijker, 1995, Law and Bijker, 1992; Williams and Edge, 1996).

In doing this we reject both technological determinism and social constructivist approaches in favor of the mutually-constituted view of material technologies as shaping and being shaped by evolving social processes. Both polarized frameworks have problems with agency, in that constructivists give none to technology and the technological determinists attribute none to society. Both are linear, one-dimensional, blackbox the artifact, and only address the outcomes of technological change (Feenberg, 1991; Thomas, 1994).

We draw from the SST perspective because it facilitates the examination of the larger context of technological change, the processes of technological change and most specifically the content of the technological change itself (Williams and Edge, 1996). Central to the SST framework is the concept of choice, in that technological innovation and development can be represented by a series of choices of one technological path over another through a process of negotiation and sometimes leading to irreversibility and lock-in of certain technologies (Collinridge, 1992; Callon, 1993; Rosenberg, 1994; Arthur, 1989; Cowan, 1992). And finally the SST perspective is particularly adept at exposing the governance, control and political motivations behind technological choice and development, critically exposing privilege and power (Bijker, 1993; Winner, 1977; Winner, 1980, Hard, 1993, Latour, 1988)

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 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, and 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 socio-technical change theory to illustrate the generic goals of this approach, and to discuss the theoretical tensions that exist in socio-technical IT research. These tensions provide a range of possibilities for specific socio-technical 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 socio-technical 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 socio-technical 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 socio-technical analysis should not *a priori* privilege technological or material explanations ahead of social explanations, and vice versa. The principle of change and continuity argues that socio-technical 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'. Success and/or failure of a particular technology is explained as a result of socio-technological developments, not as a cause of those developments. Success is in the eye of beholder. The actor and structure principle states that socio-technical 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 socio-technical 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 study⁶ of police officer's uses of an integrated criminal justice system accessed via the public wireless data network from laptops and personal digital assistants (PDA) provided to the participants (see Sawyer and Tapia, 2003; Sawyer and Tapia, 2004; Tapia and Sawyer, 2005a, 2005b) Each element of our field trial is discussed below.

Mobile Access to Pennsylvania's Justice Network

Mobile access for this trial was done via a third generation (3G) data network. In the US, 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 US 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 US and there may be gaps in service within covered areas. Moreover, collectively, all providers' coverage does not cover the geography of the US and a service gap in one providers' coverage is not alleviated by the coverage of a second. The major carriers in the US have deployed their 3G networks in different ways and at different rates⁷. 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 Justice **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 that the Commonwealth of PA (and the U.S. Federal government). The data are owned by the relevant state or Federal agency (for example, PA's Department of Transportation, or PennDOT, maintains driver's license records and a picture database) and JNET provides a query-based access to the driver 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) and this requires several forms of identification to be used⁹. Users must also re-authenticate periodically during their sessions in order to assure security during use. And, 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, email and reporting functions for users. These functions serve as both a common message board across all criminal justice personnel in PA. The email 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 comes across the message board, she will be alerted and can more easily follow-up on their 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 non-trivial 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 cruiser's 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 paper.

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 *application's* uses, *information and data sharing*, and changes or alterations to police officer's *work practices* (particularly changes to in-field 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 paper'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 were provided with either a laptop or a personal digital assistant (PDA) 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, 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 user's 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-call 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, email 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 and 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 reports and such, not connected to 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 officer's 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 log on procedures and caused connection drops. The two factor log on 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 driver's 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 cruiser's onboard laptop).

We saw little changes to police officer's *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 officer's 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 reflect on these seven findings, general SST principles and return to Bijker's (1995) four principles of socio-technical change theory.

First, the social shaping of technology perspective (SST) lends itself to this analysis in three ways, through a focus on interpretive implementation, socio-technical ensembles, and the concept of the boundary object.

While many sociotechnical theorists have focused on the innovation stage of technological development, SST allows for a central place for the stage of implementation and stresses the non-linear, transformative, interpretive, and iterative nature of this stage (Williams and Edge, 1996). Fleck (1988) describes this process as "innofusion," a struggle between design, trial, exploration and use, as spiral, interactive and complex. Using this lens we can examine the struggle between the relevant social groups including the designers of the PDA and laptop devices, the designers of the 3G wireless cards, the developers of the JNET software, the providers of the 3G wireless broadband service, the policing administration of various departments and the officer-users, as entering, perhaps unwittingly, into a collaborative design process for mobile JNET. The struggle that we witnessed between each of these groups trying to make the devices work can be seen as such a process.

The concept of socio-technical ensembles is also highly useful in this setting. SST stresses that technology and organizations cannot be treated as separate entities. There exists a complex web of mutual dependency between all relevant social groups, devices, expertise and information. Bijker uses the term sociotechnical ensemble to denote this network of objects, infrastructures, and humans and the roles they play (Bijker, 1995). These elements of the ensemble, whether human or technical, must work together to produce a functioning whole. We can clearly see the relationships of dependency within a socio-technical ensemble in the mobile JNet trial, even more explicitly when the ensemble failed to perform up to expectations. In order for this trial to have been labeled a success by all relevant social groups the devices, service and software would have needed to perform as promised. However, the wireless coverage was inconsistent and unreliable, the batteries were not sufficiently powerful to sustain required usage, the security protocols were tedious, the officers' tasks and information needs did not match what was offered, and the officers need for administrative and IT training and support was unmet. At each of these points the ensemble failed to perform in conjunction and never approached harmony.

It is obvious that mobile JNet was defined differently to different relevant social groups. For the officers JNet mobile JNet was defined as a novelty, a potentially interesting tool to gain information in the field but not reliable, simple, or hands-free enough to use in critical life-or-death moments. For the developers of JNet, mobile JNet was an extension of an already proven killer desktop application that just needed a few logistical bugs worked out to be a killer application mobilely. For the device providers Mobile JNet was an open door into local government market development. For the 3G wireless providers mobile JNet was a group of unanticipated users who taxed and challenged a system that was not designed for their use. These relevant social group can also be seen as communities of practice who share a technological device in common, yet who interpret that device very differently. A boundary object is defined as an object that is located in the middle' of a group of actors with divergent viewpoints (Star,

1989; Bowker and Star, 1999). The concept of the boundary object implies negotiation of definitions between different communities of practice of a common artifact. This negotiation is also a process infused with elements of competition, protection of one's assets and territory and ownership of the final definition and control of the object (Fox, 2000)

The principle of the seamless web is that analysis should not *a priori* privilege the technological explanations ahead of social explanations, and vice versa. The principle of change and continuity means that analysis must account for both change and continuity. The symmetry principle focuses analysis on the temporal processes by which social and technical interact. The actor and structure principle makes clear that analysis must account for both action and structure. In Table 1 we summarize these principles relative to the seven findings we noted in the previous section and in the remainder of this section we discuss this summary.

<insert Table 1 near here>

Building on this, we make three observations. First, the institutional structures that help to govern the work of policing serve as powerful moderators to both taking up and taking advantage of new practices such as having mobile access to computing resources and information. Even when the principles of change and continuity are instantiated with evidence that moving out access to high-value resources (from fixed to mobile connection) is welcomed, the structural pressures constrain action. And, the findings from this study provide more support for the principles of seamless web and symmetry. That is, there are no direct effects of new ICT on outcomes (as seen in the ways that PDAs were taken up and used in this trial). Nor is it possible to make predictions of change based on solely technological properties (as evidenced by the unfounded belief in bandwidth here).

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 un-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 evaluator's 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 point 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.

In the United States such a localized model might be found in the example of a single police officer in a vehicle. This officer has expectations of reliability in terms of his or her equipment including the vehicle itself, communication equipment, and weapons; connectivity via radio to a central dispatch office and other officers, and fast-arriving backup sent by dispatch in times of need. This model would fail if the situation changed to a single officer on foot or on a bicycle, or to multiple officers in a vehicle, or to officer-non-officer combinations. This intermediate model demands being situated if the sociotechnical ensembles of policing organizations, device designers and software developers are going to proactively develop technologies for criminal justice institutions that are not destined for some form of failure.

Our final observation from this analysis is 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 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 and Lee, 2003).

While the research literature focused on the effects of ICT highlights 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 discernable (Ackroyd, Harper, Hughes, Shapiro and 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 and 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 and 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.

Arthur, W.B., (1989), Competing technologies, increasing returns and lock-in by historical events, *The Economics Journal* 99,116-131.

Avgerou, C. (2002). *Information Systems and Global Diversity*. Oxford: Oxford University Press.

Bijker, W., (1993), Do not despair: there is life after constructivism, *Science, Technology and Human Values* 18(4), 113-138.

Bijker, W., (1995), Sociohistorical technology studies, in: Jasanoff et al. (Editors), *Handbook of Science and Technology Studies*, Sage Publications, London, pp. 229-256.

Bijker, W. and J. Law (Editors), (1992), *Shaping Technology/Building Society: Studies in Socio-technical Change*, MIT Press, Cambridge, MA.

Bijker, W., T. Hughes and T. Pinch (Editors), (1987), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (MIT Press, Cambridge, MA).

G. C. Bowker and S. L. Star. (1999) *Sorting things out: classification and its consequences*. 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.

Callon, M., (1993), Variety and irreversibility in networks of technique conception and adoption, in: D. Foray and C. Freeman (Editors), *Technology and the Wealth of Nations: The Dynamics of Constructed Advantage* (Pinter, London) pp. 232-268.

Collingridge, D., 1992, *The Management of Scale: Big Organizations, Big Decisions, Big Mistakes* (Routledge, London).

Cowan, R., 1992, High technology and the economics of standardization, in: M. Dierkes and U. Hoffmann, *New Technology and the Outset: Social Forces in the Shaping of Technological Innovations* (Campus/Westview, Frankfurt/New York) pp. 279-300.

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,

Feenberg, Andrew. (1991). *Critical Theory of Technology*. New York: Oxford University Press.
Fox, S. (2000). Communities of practice, Foucault and actor-network theory. *Journal of Management Studies*, 37(6), 853-867.

Hard, M., (1993), Beyond harmony and consensus: a social conflict approach to technology, *Science, Technology & Human Values* 18(4), 408-432.

Horton, K., Davenport, E., and Wood-Harper, T. (2005). Exploring Sociotechnical Interaction with Rob Kling: Five 'Big' Ideas, *Information, Technology and People*.

JNET. (2004). Usage Statistics, available online at URL:
<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) Available online at URL: <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 Socio-Technical Approach. In B. Kahin and E. Brynjolfsson (Ed.), *Understanding the Digital Economy: Data, Tools and Research*: Cambridge, MA : MIT Press.

Kling, R., Rosenbaum, H. and Sawyer, S. (2005), *Understanding and Communicating Social Informatics: A Framework for Studying and Teaching the Human Contexts of Information and Communication Technologies*. Medford, NJ: Information Today.

Klockers, C., & Mastrofski, S. (Eds.). (1991). *Thinking About Police: Contemporary Readings*. New York: McGraw-Hill.

Lamb, R., and Kling, R. (2003). "Reconceptualizing Users as Social Actors in Information Systems Research." *MIS Quarterly*, 27(2), 197-235.

Latour, B., 1988, How to write "The Prince" for machines as well as machinations, in: B. Elliott (Editor), *Technology and Social Process* (Edinburgh University Press, Edinburgh) pp. 20-43.

- Law, J. & Bijker, W. (1992). Technology, Stability and Social Theory. In W. Bijker (Ed.) *Shaping Technology/Building Society*. Cambridge, MA: MIT Press: 32-50.
- Lin, C., Hu, P., & Chen, H. (2004). Technology implementation management in law enforcement. *Social Science Computer Review*, 22(1), 24.
- Mackay, H., Gillespie, G. (1992). "Extending the social shaping of technology approach: Ideology and appropriation." *Social Studies of Science*, 22(4), pp. 685—716.
- MacKenzie, D. and J. Wajcman (Editors), 1985, *The Social Shaping of Technology: How the Refrigerator Got Its Hum* (Open University Press, Milton Keynes).
- 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, 2003, *Concept for Operations for Integrated Justice Information Sharing Version 1.0*, The National Association of State Chief Information Officers, Available online at URL: <https://www.nascio.org/publications/index.cfm>.
- Northrop, 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.
- Rosenberg, N., 1994, *Exploring the Black Box: Technology, Economics and History* (Cambridge University Press, Cambridge).

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

Sawyer, S. & Eschenfelder, K. (2002). Social Informatics: Perspectives, Examples, and Trends. in Cronin, B. (Ed.) *Annual Review of Information Science and Technology*, 36, Medford, NJ: Information Today Inc./ASIST, 427-465.

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.

Sawyer, S., Wigand, R. and Crowston, K. (2005) "Redefining Access: Uses and Roles of Information and Communications Technologies in the Residential Real Estate Industry from 1995-2005," *Journal of Information Technology*, 20(4), 3-14.

Sawyer, S and Tapia, A. (forthcoming), "Always Articulating: Theorizing on Mobile and Wireless Technologies," *The Information Society*.

Star, S.L. (1989) The structure of ill-structured solutions: Boundary objects and heterogeneous distributed problem solving. In *Distributed artificial intelligence*, Vol 2. London: Pitman.

Tapia, A. and Sawyer, S. (2005a) "The Sociotechnical Nature of Mobile Computing Work: Evidence from a Study of Policing in the United States," *International Journal of Technology & Human Interaction*, 1(3), 1-14.

Tapia, A. and Sawyer, S. (2005b) "Beliefs about Computing: Contrary Evidence from a Study of Mobile Computing Use" in Lytinen, K., Yoo, Y. and DeGross, J. (Eds), *Designing Ubiquitous Information Environments Socio-technical Issues and Challenges*. London: Kluwer, 21-40.

Thomas, R. J. (1994). "Introduction." In *What machines can't do: politics and technology in the industrial enterprise*, Berkeley: University of California Press.

Taylor, M., Epper, R. & Tolman, T. (1998). *Wireless Communications and Interoperability among State and Local Law Enforcement Agencies*. National Criminal Justice Clearinghouse Report 168945, Washington, DC.

Williams, R., Edge, D. (1996). "The social shaping of technology." *Research Policy*, 25, pp. 865—899.

Winner, L., (1980), Do Artifacts have Politics? *Daedalus* 109, 121-136.

Winner, L., (1993), Upon opening the black box and finding it empty: social constructivism and the philosophy of technology, *Science, Technology & Human Values* 18(3), 362-378.

Table 1: Sociotechnical analysis

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

Author biographies:

Steve Sawyer is a founding member and associate professor at the Pennsylvania State University's School of Information Sciences and Technology. Steve holds affiliate appointments in Management and Organizations; Labor Studies and Industrial Relations; and the Science, Technology and Society. Steve does social and organizational informatics research with a particular focus on people working together using information and communication technologies. Steve can be reached at sawyer@ist.psu.edu.

Andrea Hoplight Tapia is an assistant professor of Information Sciences and Technology at the Pennsylvania State University. Prior to her arrival at Penn State, Andrea completed a National Science Foundation funded post-doctoral fellowship at the University of Arizona entitled "Universities in the Information Age." Her Ph.D. is in the area of Sociology and focuses on the study of technology, culture and workplace organizations. Her most recent work examines the nature of computer-centered, high-tech industry. She is particularly interested in the how the workplace and employer-employee relations change when in a high-tech environment. At the core of her research is her interest in the social values attributed to technology and the power structures that arise within organizations due to the manipulation and use of those techno-values, in other words, techno-social capital. Andrea can be reached by email at atapia@ist.psu.edu.

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 cellular phone is beyond the scope of this article, two attributes are worth noting. First, the officer's 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 paper 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 U.K. 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 hear listen for a gunshot or the words 'officer down.'

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

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

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 on 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.