



Information Technology, Privacy, and Power within Organizations: a view from Boundary Theory and Social Exchange perspectives.

Jeffrey M. Stanton and Kathryn R. Stam¹

Abstract

Over recent years, information technology has played an increasingly important role in the monitoring and surveillance of worker behavior in organizations. In this article, we take the position that managers, workers, and information technology professionals alike see worker-related information as a valuable organizational resource and that processes of social exchange influence how this information resource is controlled. These suppositions are woven together by joining two theories, information boundary theory, a motivational framework for examining privacy at work, and social exchange theory, which provides a perspective on social networks and social power. After discussing these two frameworks and how they might be interlaced, we analyze a corpus of semi-structured interviews with 119 managers, employees, and IT professionals that explored questions of privacy, motivation, and power in six not-for-profit organizations that were undergoing technology-driven change with potential for increased monitoring and surveillance.

Introduction

Overwhelming evidence from a series of U.S. industry surveys and research studies has converged on the ubiquity of employee monitoring and surveillance technologies in U.S. work organizations (e.g.: 9 to 5, 1990; Orthmann, 1998; SHRM, 1991; 1999; see Appendix A for more information). Although legal controls on worker rights are stricter in other locales such as Canada, Western Europe, Japan, and Australia, the use of electronic monitoring and surveillance of workers and workgroups occurs in those regions as well (Mayer-Schönberger, 1999; International Labour Office, 1993). In the U.S. it appears to now be routine for organizations to monitor telephone records, web usage, email recipient addresses and email message contents. Enterprise computing systems have centralized work records and other information about job-related activities in enormous linked databases. Camera surveillance has also become increasingly

¹ Authors' note: Jeffrey M. Stanton and Kathryn R. Stam, School of Information Studies, Syracuse University. This work was supported in part by award SES9984111 from the National Science Foundation. The National Science Foundation does not necessarily endorse the positions or conclusions expressed in this work. Address all correspondence to the first author at 4125 Center for Science and Technology, Syracuse University, 13244-4100, <mailto:jmstanto@syr.edu>

common particularly in public spaces (e.g., lobbies, parking lots, customer areas of retail stores), but additionally in non-public spaces such as employee locker rooms (also see Appendix A). The popular press often portrays these uses of technology in terms of the potential for “violation of privacy,” but this phrasing hides the underlying complexity of the issues involved by using the emotionally loaded word “violation” to cloud the subtle dynamics involved in the control over valuable information in organizations.

Leaders and managers of organizations frequently seek strategies for controlling their organizational environments. Uncontrolled or chaotic environments are problematic for organizations on a number of counts, not least of which is the difficulty predicting what will happen to or within the organization in the near or more distant future. Organizations have consistently sought methods to bring their environments under control; technology has often played a role in this effort (e.g., Simon, 1965: 73). Haggerty and Ericson (2000) refer to these concerns as based on management’s, “desires for control, governance, security, [and] profit...” (609). Technology can stabilize and routinize business processes, but more pointedly in the present era, *information* technology can streamline and amplify the collection and analysis of data as well as its use in decision-making. One source of uncertainty and unpredictability in any organization’s environment is the behavior of employees: productive, unproductive, and otherwise. Information technology can provide organizational stakeholders with data collection and analysis tools to increase the visibility of employee behavior, uncover patterns of behavior, relate patterns of behavior to individual and aggregate performance outcomes, and reduce or eliminate the lag between the discovery of behavioral patterns and subsequent managerial action or decision making. On the surface, then, information technology appears to provide a panacea of observation, analysis, prediction, and control for those who wish to reduce the uncertainty and unpredictability of employee behavior.

From this point, popular accounts of organizational monitoring and surveillance usually make a leap into discussion of how such technology violates regulations, cultural norms, and/or personal rights (also see: [Appendix B](#)). Although each of these concerns is valid in different contexts, this leap passes over considerable interesting territory, by tacitly assuming that employees simply accept these technologies as deployed, that relationships among employees and their managers or firms are irrelevant, and that organizations simply dominate employees with the unilateral imposition of technology. One might characterize this as the “done deal” conjecture of employee monitoring and surveillance. In contrast, any reader of the literature on technology acceptance in organizations will testify that integrating any new technology into a firm requires a set of highly interactive processes involving a network of relationships among stakeholders such as managers, employees, IT professionals, and others (e.g.: Davis, 1989). This observation suggests the possibility that employees do not simply accept technologies that capture potentially valuable information about their whereabouts, activities, or knowledge. Rather, one might suggest that a considered process may take place in which employees, IT professionals, and managers weigh what valuable information can and should be captured, what the benefits might be for each and all parties involved, and what alternative options are available for avoiding, thwarting, distorting, or resisting information gathering.

In the present research, we take the view that each stakeholder in an organization knows that information is a valuable commodity: Managers, IT professionals, and employees all function as “intuitive information managers.” Relatedly, we suggest that controlling flows of information about oneself or others is a motivation-driven process. Further, we suggest that these motivations occur within a context of social relationships and social exchange that guides who can learn what, when, and at what cost. This orientation accords with Ball’s (2003 forthcoming) conception of the “contested and politicized” nature of surveillance in organizations. Finally, we expand upon the standard dichotomy of employees versus managers by focusing on the triadic relationship dynamics among employees, IT professionals, and managers. Lyon’s (2001) recent work on the subtle “social ordering” effects of surveillance suggests the possibility that the relations among these three groups may have changed because of the new technology.

We weave these suppositions together by joining two theories. The first, information boundary theory, arose from efforts at understanding personal privacy at work. This theory provides the motivational elements that illuminate when and why individuals withhold or release valuable information. The second, social exchange theory, provides an analysis of resource exchange and social power that situates personal motivation in a network of social relationships. After discussing a synthesis of these two theories, we analyze a corpus of interviews with managers, employees, and IT professionals that explored questions of privacy, motivation, and power in a set of organizations that were undergoing technology-driven change.

Overview of Information Boundary Theory

Information boundary theory (IBT) developed from a program of research that investigated the impacts of monitoring and surveillance technologies on worker privacy. Analysis of multiple waves of interview and survey data (Stanton, 2002; Stanton and Weiss, 2000, Stanton and Weiss, in press) suggested a synthesis of communications boundary management theory (Petronio, 1991), a group-value approach to organizational justice (Alder, 1998; Alder and Tompkins, 1997), and a general expectancy-valence framework for privacy protection (Stone and Stone, 1990). Earlier formulations of IBT appear in Stanton (2002) and Zakaria, Stanton, and Sarkar-Barney (in press).

IBT predicts that motivation to reveal or withhold valued information via a given medium follows rules for “boundary opening” and “boundary closure” (Petronio, 1991). Petronio’s work derived from Altman’s (1975; 1976) analysis of privacy, social behavior, and social environments. According to both Altman and Petronio, boundary opening and closure are dynamic, psychological processes of regulation by which people attempt to control flows of valued information to other people in their social environments. Boundary regulation applies to communicative and observational forms of information technology. Email serves as a prototypical example. Imagine that a worker learns that she must take a leave of absence to receive treatment for an illness. She must carefully consider what to reveal, when, and to whom. If she chooses email to communicate her message, someone might monitor the message, an initial recipient might forward the

message to someone outside her intended audience, and the possibility exists that a semi-permanent record of her message will be stored for later retrieval, either intentionally or inadvertently. The domain of IBT is thus to predict individual preferences and motivations regarding the amount and type of valuable information that the individual would be willing to reveal in this medium. Other organizational applications of information technology such as performance monitoring systems, knowledge management systems, list servers, bulletin boards, newsgroups, chat, blogging, and instant messaging also exemplify media for which individuals must regulate the disclosure of valuable information. Such information can relate to any of a variety of domains including work-related (e.g.: job performance), personal (e.g.: information about family members), etc. depending upon the communicative situation.

IBT predicts preferences and behavior based on individuals' beliefs about the nature of their relationship with the message audience (institutional, aggregate, or individual), the expected uses of revealed information, and the expected benefits of revealing information. As Stanton and Weiss (in press) suggested, individuals frame their uses of information technology to transmit information in similar terms to those used within human relationships (e.g., "telling about me," "becoming known," or "becoming visible to others"). Individuals can articulate a personal "calculus" of boundary negotiation, i.e., the conditions under which permitting information flow is acceptable or unacceptable. The negotiation of boundaries depends in part upon the status of the relationship between the sender and the audience (individual or institutional) receiving it.

Prior formulations of IBT elaborated several distinctive sources of motivation (trust, fairness, value-expressive, and instrumental) but here we attempt to amalgamate these components by situating each of them within a regulatory focus perspective (Higgins, 1997, 1998). In brief, Higgins work suggests that people use overt behavior (and particularly social behavior) as one method of self-regulating emotional states. Higgins describes two basic self regulatory foci: "promotion focus," concentrates on the motivating power of achieving gains and striving toward ideals; "prevention focus," emphasizes the motivating power of avoiding or mitigating losses by attending to "oughts," duties, or felt responsibilities. In a workplace environment, typical gains might include career advancement, bonuses, or earned perquisites. Typical losses might include job loss, punitive sanctions, or removal of discretionary resources. Higgins' research program has repeatedly affirmed that the antecedents and consequences surrounding gain and loss fundamentally differ from one another in character and process. Recently, Brockner and Higgins (2001) directly applied Regulatory Focus Theory to work motivation by integrating goal setting theory, expectancy-valence theory, and behavioral decision theory under the regulatory focus umbrella. In [Table 1](#) (overleaf) we have crossed these two basic regulatory foci with the two boundary regulation processes of IBT to describe four different motivational situations for IBT.

Table 1:

Motivational Variants in Information Boundary Theory using a Regulatory Focus Perspective

	Promotion (Gain) Focused	Prevention (Loss) Focused
Boundary Opening	<i>Exoteric:</i> Revealing information in an effort to achieve or solidify gains.	<i>Redemptive:</i> Revealing information in an effort to prevent or mitigate losses.
Boundary Closure	<i>Political:</i> Withholding information in an effort to achieve or solidify gains.	<i>Protective:</i> Withholding information in an effort to prevent or mitigate losses.

Our distinct motivational categories – trust, group-value, and instrumental – map onto this arrangement in a logical way. In previous work (e.g., Stanton, 2002), we asserted that trust was a necessity for boundary opening, and we further refine this assertion by suggesting that trust is a necessity in the redemptive category. Trust must exist to facilitate the voluntary revelation of information that casts the message sender in a negative light. In contrast, the exoteric motivational situation allows for the revelation of *positive* information regardless of the trust status of the relationship. In the absence of a trust relationship, either political or protective motivations may also lead to the withholding of valuable information.

In parallel, the group-value perspective (Alder, 1998; Alder and Tompkins, 1997; Lind and Tyler, 1988, pp. 230-240), suggests that the revelation of information can affect one's status in a valued social group. In groups that value intimacy and/or secrets (e.g.: Vangelisti, 1994), the redemptive motivational situation facilitates voluntary revelation of information that casts the message sender in a negative light. In groups that value status and achievements, the exoteric motivational situation can facilitate the revelation of information that casts the message sender in a positive light.

With regard to instrumental motivations, we built onto Stone and Stone's (1990) expectancy-valence privacy framework, in which message senders control personal information to achieve desired end states. With respect to Table 1, we further suggest that individuals both strategically reveal *and* withhold information in expectation of reaching desired end states. In accord with Higgins (1997; 1998), we have divided such end states into two fundamentally different types, promotion-focused and prevention focused. Thus, in an effort to avoid financial loss, *revealing* one's health problems to an insurance company might reflect a redemptive motivation, while *withholding* the date of onset of those health problems might reflect a protective motivation. An important subsidiary point demonstrated by this particular example is that the pursuit of gains and avoidance of loss through control over information places this theory at a more general level than impression management and self-presentation (e.g.: Arkin and Shepperd, 1989; i.e.: we are not as concerned with the tactical use of information in the form of persuasive speech as we are in information as a strategic resource).

Power in Social Exchange Theory

Theory and research on social exchange has flourished since its introduction near the middle of the last century. Early formulations included works by Homans (1958), Thibaut and Kelly (1959), and Adams (1965). For example, Homans' reductionist theory of elementary social behavior posited that the occurrence of social behaviors is mediated by the probability that such behaviors will result in valued reward outcomes. Although these theories provided a somewhat mechanistic view of exchange in human relationships, others built on them to develop more nuanced perspectives. Blau (1964), for example, described his research as an attempt, "to derive the social processes that govern the complex structures of communities and societies from the simpler processes that pervade the daily intercourse among individuals and their interpersonal relations" (2). Blau provided an analysis of several domains of social interaction, and it is his analyses of social power that we use as a starting point for our synthesis.

Blau (1964) adopted an inclusive definition of social power – "all kinds of influence between persons and groups, including those exercised in exchange transactions" (p. 115) – although he acknowledged that this definition might capture some social dynamics not typically construed as based in power. Importantly, however, this definition allowed the inclusion of both rewards and sanctions as mechanisms that enforce power in social exchange. This consideration facilitates an elegant mapping of power mechanisms onto Higgins (1997; 1998) two regulatory foci. Specifically, we echo Blau's belief that individuals exert power over others in organizations partly through mechanisms of reward and partly through sanctions. This duality also fits closely with French and Raven's (1959; French, 1956) notions of reward power and coercive power. Using Regulatory Focus Theory as a guide, however, we further suggest that there is an important asymmetry in the exercise of power through these mechanisms. Specifically, the promise of reward pushes individuals toward a promotion-focused self-regulatory mindset, whereas the threat of punishment pushes individuals toward a prevention-focused orientation. We expand on the significance of this distinction in the next section.

Blau also added three definitional restrictions. First, he suggested that the recurrent ability of the more powerful party to influence the behavior of the less powerful was an important factor distinguishing power from other situations in which the latter agent could easily "leave the field." This restriction maps suitably onto workplace power relationships because the workplace is prototypically a set of linked situations in which employees and managers enact social exchange over the course of many interactions. Second, Blau describes an element of voluntarism in response to power that distinguishes it from the extreme boundary case of coercion (particularly physical coercion). Workers often have at least a limited set of choices among a range of compliance and resistance behaviors, even though they are sometimes severely constrained in behavioral options due to financial dependency on the organization. Finally, Blau described social power resulting from an inherent asymmetry in social influence: Relationships characterized by co-equal influence do not qualify as power relationships. In the workplace, such asymmetry appears most often between those lower in the formal administrative hierarchy and those higher, but it seems reasonable to also assume that some peer

relations are also asymmetric, for example between a more experienced manager and a less experienced one.

Merging Boundary Theory and Social Exchange Perspectives

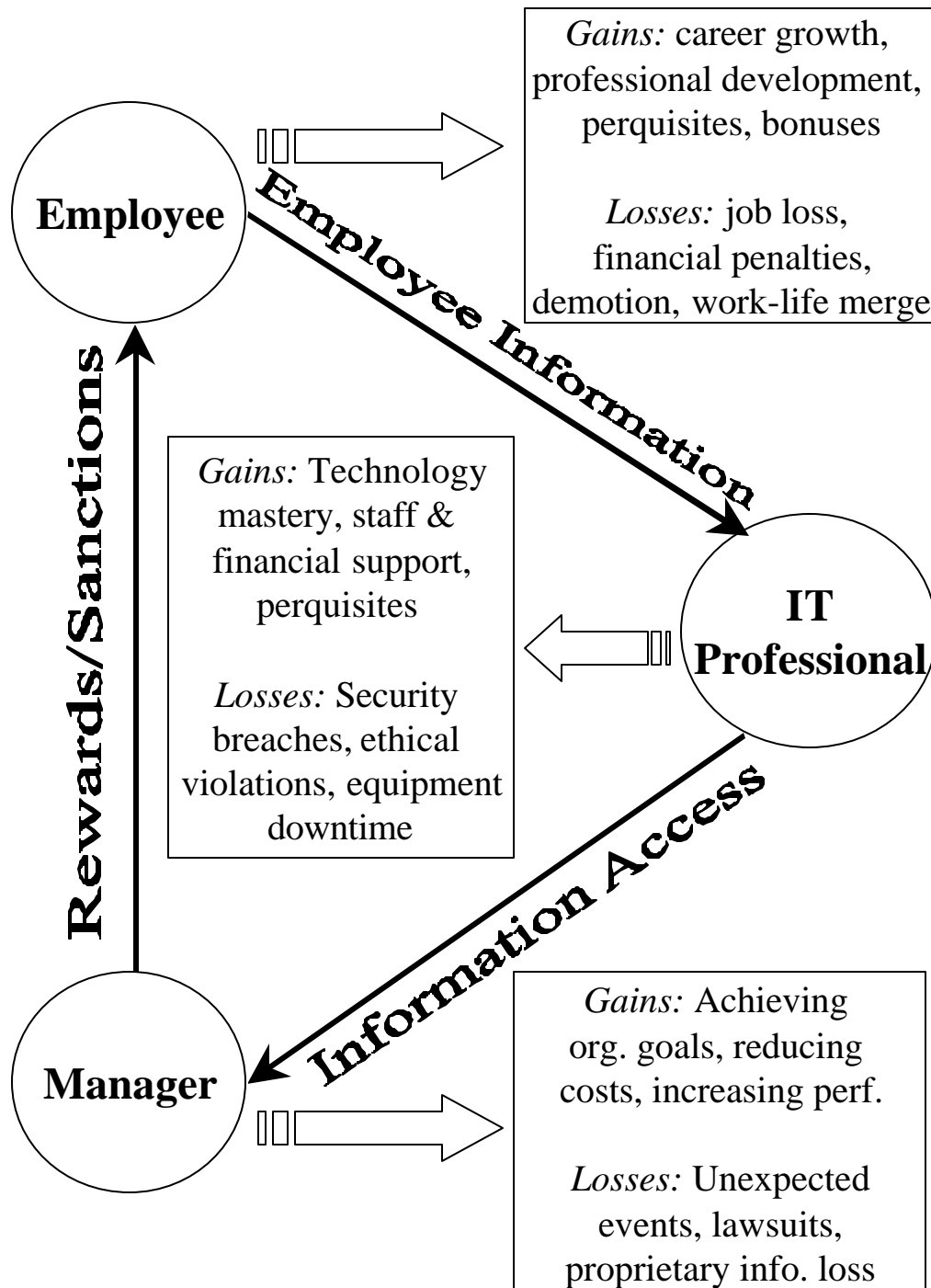
In the decades since Blau's (1964) book on social exchange and power, a plethora of studies and theory developments have appeared on these topics. One important development was the shift by Emerson (1972) to a focus on the structural aspects of social networks among individuals in interacting groups. In turn, Cook, Molm, and others (e.g., Cook, Molm, and Yamagishi, 1993) subsequently reintegrated the affective reactions of actors into the structural versions of exchange theory, a key emphasis for us because of our use of the regulatory focus perspective. The heart of Cook and Molm's integrated theory lies in the balance between dependency and power. To the extent that one actor is independent of a second actor, but the latter is dependent on the former, a state of imbalance exists: This imbalance gives the more independent actor power over the less independent actor. In workplace relationships, these balances are rarely absolute. A supervisor may have a higher degree of independence than her employee, thanks to her ability to allocate valued resources and influence personnel decisions, but a degree of dependency also exists to the extent that the supervisor relies on the employee's expertise and productive abilities to accomplish the work of the unit.

Molm (1991) further suggested that, "dependence increases with the value of outcomes that the other controls and decreases with the availability of alternative sources of those outcomes" (476). This point serves as our primary linking pin with information boundary theory. With our focus on monitoring and surveillance practices, one of the fundamental "valued outcomes" in the present day organization is inexpensive, timely, and accurate information about employees and their activities: what employees are doing now, what they have done recently, what they might do in the future, their capabilities, preferences, tendencies, and inclinations. Enterprise computing systems, performance monitoring systems, network activity monitoring systems, and surveillance devices each facilitate a diminution of employees' control over valued information about themselves and their activities. As a result, those who have access to the information provided by these systems may "gain independence" if they control this valued resource. In accord with our integrated perspective, such gains must come attached to reciprocal exchanges with the less powerful party in the form of promised rewards or potential sanctions.

In contrast with a simple dyadic social exchange between employees and management, however, we believe that IT professionals serve a crucial intermediary role here. Because of the complexity of many monitoring and surveillance technologies, the typical manager cannot directly access the information derived from monitoring and surveillance, but rather depends on the IT professional to grant such access. This may represent in some cases a net transfer of independence from managers to IT professionals. The end result may be that the IT professional serves a "power broker" role in which management cannot gain the control over employees' valuable information without the participation of IT professionals in the transfer of this control. In Molm's (1994) terminology, this

represents a situation of “indirect-generalized exchange,” in which no one of the actors in the social network gains the benefits of exchange without cooperation of the other actors.

Figure 1:
Prototypical Triadic Exchange Relationship



At this point, we need to delve into information boundary regulation for the members of this triad in order to predict how these power transfers might unfold. [Figure 1](#) (above) displays each of the three roles, the fundamental resource that each exchanges with regard to employee monitoring and surveillance, a list of prototypical gains representing promotion-focused ideals for achievement, and a list of losses representing prototypical prevention-focused “oughts” for avoidance. The overall structure of the figure suggests an indirect-generalized exchange (Molm, 1994) in which valuable information about employees (including both performance information such as task completion and non-performance information such as personal communications) is a resource created by employees and made available, by means of technology, to IT professionals. In turn, IT professionals can and may be influenced to provide management with access to valuable information about employees. Finally, management provides rewards and/or threats of sanctions to employees. At this point it is important to note that we are intentionally isolating the prototypical resources associated with surveillance and monitoring: A holistic view of the organization and these stakeholders would undoubtedly reveal many more resource transactions than those depicted here as relevant to monitoring.

For each role, [Figure 1](#) samples some of the basic gains and losses relevant in a monitoring and surveillance context. Employees might reveal valuable information (exoteric boundary opening) in order to gain feedback useful for career growth and professional development, to gain discretionary privileges (perquisites), or to obtain some financial award (e.g., performance bonuses). Alternatively, employees might reveal valuable information (redemptive boundary opening) in order to avoid job loss, financial penalties, demotion, or loss of other work-related resources. In some cases, employees might prefer to withhold certain valuable information (protective boundary closure; e.g., about the health of family members), for example, to maintain a desired separation between work and non-work life.

IT professionals might choose to enable monitoring and surveillance and provide management access to the resultant information in order to demonstrate technological mastery, support the need for staff and financial support for IT operations, and to obtain discretionary resources (exoteric boundary opening). On the contrary, handling and granting access to valuable information also opens up the possibility of security breaches and accompanying downtime, both of which most IT professionals wish to avoid (protective boundary closure). Additionally, any misuse of valuable information that results from IT-granted access also has the potential to be construed as an ethical breach to the extent that the IT professional facilitated it. Note that these points deliberately simplify the IT professional role: IT professionals are employees too, and the typical gains and losses listed for employees apply equally to them.

Managers obtain valuable employee information, and in particular information about worker performance outcomes, to achieve organizational goals by reducing costs or increasing productivity (exoteric boundary opening). In contrast, managers might obtain non-performance information to avoid or anticipate unexpected events (e.g.: a key employee taking family leave), to avoid lawsuits (e.g., those that occur because of harassing communications among employees), or to avoid the loss of proprietary

information to outsiders (e.g., by monitoring and filtering outbound email that contains valuable information (redemptive boundary opening)).

This discussion of gains and losses raises several interesting subsidiary points. First, the figure affirms that managers can obtain the access to performance information that they desire through applying rewards rather than sanctions. Relatedly, employee gains seem to associate with the revelation (i.e.: exoteric boundary opening) of performance-related information (e.g., task progress), whereas the avoidance of losses seems to associate with the withholding (protective boundary closure) of non-performance information (e.g.: about the contents of personal email messages). On the same tack, it is this same non-performance information that seems most closely bound to the loss potential of managers: The email that the employee wishes to hide may be the one that opens up the organization to the threat of a lawsuit. Lastly, the insider knowledge that the IT professional has by dint of full access and control over valuable employee information may be problematic because it heightens the possibility of security breaches and ethical violations. Thus, to gain access without heightening IT professionals' loss liability, management would seem to have to provide some assurance against such loss.

In summary, our analysis of the control over valuable information in terms of the power elements of social exchange suggests several general research propositions to explore.

- First, as an overarching assumption of this inquiry, we expect that employees will not passively accept the capture of valuable information from them, but rather that a resource exchange process will occur among employees, managers, and IT professionals. Specifically, we have suggested the existence of an indirect-generalized exchange triad, in which employees comply with (or resist) monitoring and surveillance technologies as implemented by IT professionals when requested by managers who provide rewards or sanctions.
- Next, we propose that IT professionals' roles in these exchange processes will lie at the intersection between employees and managers. Relatedly, the high degree of information access that IT professionals may have (i.e.: the technical capability to view all monitoring and surveillance data) may be construed as a liability because of the potential this access provides for security breaches and ethical violations.
- Finally, we expect to find some linkage between regulatory foci and exchange processes. Managers may promote organizational gains by obtaining performance information that employees may wish to disclose for their own gains. In contrast, however, managers may wish to mitigate the organization's potential for losses by obtaining access to the same types of non-performance information that employees may wish to withhold.

Method

The primary method used was qualitative semi-structured interviews with employees from six not-for-profit organizations in various stages of information technology (IT) change. The organizations represented in these data were a social service agency, suburban hospital, a psychological counseling center, a private university, and a public utility; these sites were selected from a larger pool of 12 non-profit organizations based on the readiness of their information technology change plans and the compatibility of their timetables with our research. Data from all six organizations that participated in our study were included in the analysis. The results are based on our analysis of interviews (30-40 minutes each) with N=119 different individuals conducted, audiotaped, and transcribed by a team of 10 trained research assistants from Sept 2001-Sept 2002 (see Appendix C for sample protocol). Within this sample, we interpreted the role of "IT professional" broadly by including in this designation 30 employees who had IT-related responsibilities ranging from maintenance of PC's and software training to budgetary and strategic/long term planning duties. Although the majority of the IT professionals we interviewed had front line roles, at least one interviewee from each organization was a director-level IT professional.

The monitoring and surveillance potential associated with each IT change varied substantially. At the social service agency, for example, the management deployed cellular telephones for caseworkers, whose time was primarily spent in the field. The management's aims included the improvement of communication, expediting data processing, and enhancement of workers' safety, although the employees focused on the monitoring aspects of carrying the phones. The psychological counseling center planned a move from a paper-based information system to a computerized system for centralized scheduling of counselors in order to simplify billing processing with insurance companies. For budgetary reasons, the new system would be only partially implemented, such that IT staff would temporarily intermediate the processing of necessary information from and subsequent feedback to counselors. At the hospital, new "enterprise" system was adopted to replace three overlapping legacy systems whose problems had plagued the hospital's processes of data management. The new system was intended to simplify data management, improve interdepartmental communications, and facilitate the work of IT service providers. Respondents at the university faced routine issues of IT management and pertinent innovations, rather than major overhauls of IT. Those issues involved security and privacy of information, new instructional technology, and hardware innovations such as wireless networking. The manufacturing plant and the public utility had planned but not yet begun substantial IT overhauls at their sites.

Results

As a strategy for organizing our presentation of the results we have developed four brief narratives – punctuated by respondent verbatims – illustrating the main themes we encountered in the interview data. The first two of these describe the employee perspective in two of our six organizations. The third describes the IT professional's

perspective with verbatims from several organizations. The fourth does likewise for the managerial role. Because the very large amount of available data prevents a succinct presentation of all respondents' perspectives, we close this section with an overall summary of responses for the three roles. Throughout the material below, "R" refers to the respondent, while "I" refers to the interviewer.

Illustration 1: Social Service Agency and Cellular Telephones

The overarching assumption of our inquiry was that employees would not passively accept the capture of valuable information from them, but rather that a resource exchange process would occur between employees, managers, and IT professionals for control over valuable information. Our interview data with employees from several organizations displayed reactions of anxiety, frustration, and rejection during the introduction of new means for collecting and processing of information. Data from the social service agency portrayed both the reactions and the resource exchange process. About six months before the interviews were conducted, a new policy had been introduced in which caseworkers were required to carry cellular telephones for their client visits. The management established some restrictions on the use of the cellular phones, such as prohibition of personal use, requirements for documentation of calls, and minimization of non-emergency use. Typically, caseworkers described the new telephones in this way:

R: We have cell phones but we aren't allowed to use them. They are used for emergencies or if they [management] want to call us. I wouldn't think about using that phone for calling anyone... We have to fill out a form and write down what we used it for.

It is apparent from this and other interviews that caseworkers reacted predominantly by rejecting use of the phones. The following excerpt illustrates a typical reaction:

I: Are the cell phones useful?

R: Not for me, because I am not comfortable with it... We are not allowed to use it, so I can't get comfortable with it...

I: Have they (the management) ever tried to contact you in the field?

R: ... People get you on the cell phone and say, 'While you're on your way back, do this.' Well, I have a real hard time with that. I have a real heavy schedule already, and to be bothered in the field...

In part, employees' hesitation to use the cellular phones reflected their unwillingness to give up their independence, one of the few aspects of their job that made up for the low pay and difficult working conditions of social service. Giving away information about their whereabouts might have implicated them in unauthorized behavior and could have inhibited their freedoms in the future. In addition, the way the telephones were presented by the management there was an implicit suggestion of distrust that interfered with caseworkers' sense of themselves as professionals (i.e.: trustworthy and responsible). Rather than contributing to their safety and convenience, caseworkers explained that the telephones were heavy, a safety risk, intrusive, and left them vulnerable to unexpected changes in their schedule or other negative consequences. From their perspective,

understanding that their use of the telephones would not contribute to the care they were providing for their clients, there was little reason to comply other than to prevent disciplinary action. Their dissatisfaction about the cellular telephones reflected frustration over their general treatment by the management. In the following excerpt, this caseworker described her coworkers' reactions to this aspect of their work environment:

R: Even now, they are having that when you go to a client's house, they want to make a way that you can have the client sign something that you were actually there for the time you said you were there...

I: Why would the management be concerned about that?

R: That they (caseworkers) are wasting time, that they (management) have no accounting for our time. That they will have closer tabs on us. But you hear in the back of the office sometimes, 'I don't want to be treated like a baby. I don't want a babysitter. I am here to do my job and however long it takes, it takes.' You know, you hear that all the time.

Explaining this in a slightly different way, this respondent does not want to take on the extra burden of carrying and using the cellular telephone because of close association between the telephone and the management's lack of trust in her professionalism:

R: I mean, I don't mind documenting it but I should be trusted. I have a real hard time with the cell phone... If you don't want me to use it, don't give it to me.

Another caseworker describes her concerns in terms of fear of loss:

R: We are accountable like practically every minute where you are going to be. They are saying that you have to get the client's signature. I mean, there are people who have skipped out, but, I mean, I think that eventually they get caught or they get fired. I mean, if you don't want to lose your job...not if you're smart.

The caseworkers' attitude of rejection and the absence of communication between them and the management reflect an underlying lack of trust, articulated by the respondents in the excerpts above. As mentioned in the theoretical development, trust can facilitate the voluntary revelation of information. Using the cellular phones, management could retrieve information about caseworkers' whereabouts and activities in the field. In contrast, from the caseworkers' perspective, revelation of information about activities not in compliance with management's expectations and demands, such as provision of transportation services to clients, over expenditure of appointment time, or even attention to occasional personal errands, would cast them in a negative light. This case exemplifies the requirement of trust for boundary opening in the redemptive category mentioned above.

Unfortunately for the organization in this case, trust was never consolidated and the successful implementation of the cellular telephones and potential information exchange

were compromised. The absence of trust inhibited boundary opening, and facilitated a situation where voluntary revelation of information about activities and whereabouts became increasingly unlikely as a result of subtle forms of resistance. Aside from leaving the telephones in the trunk of the car or not learning how to use them, some caseworkers chose to ignore telephone maintenance requirements or deliberately allow batteries to run out.

Even more unfortunate was the precedent for the introduction of other new information technology. Like many other social service agencies, this organization faced increasing pressure to comply with federal reporting procedures that require secure electronic transmission of data. Since there was no change in the prevailing organizational culture, subsequent plans requiring caseworkers to participate in electronic reporting by bringing laptop computers to their field visits were met with even more skepticism. This suggests that the organization could have avoided later resistance to new technologies by anticipating how the cellular phones affected the nature of social exchanges between the management and the caseworkers.

The conceptualization of power that we have adopted here has interesting implications in this illustration: The voluntary characteristic of power implies the possibility of bargaining by the less powerful. Additionally, the vertical asymmetry of power may generate horizontal interdependence among the less powerful in the form of collective action. The response above, along with the two previous responses, appeared to support the development of a net bargaining potential on the part of the less powerful group, making a negotiation process necessary. In short, the initial high power of the management to deploy the cellular phones was reduced in practice by the employees' capability for collective resistance, leading to a need for negotiations.

Illustration II: The Counseling Center and Centralized Scheduling

Unlike the previous organization, in the counseling center an initially shaky trust between management and staff was repaired allowing for completion of a negotiation process and an IT implementation that satisfied both parties. The initial intention of the center's management was to supplement their billing system with a centralized scheduling system for counselors and a system for managing client record information. In the idealized form presented by management, the new system would have integrated the various functions of the organization, reduced the need for archival storage of paper files, and facilitated billing procedures to improve the financial status of the organization. However, after consulting with various parties (i.e. vendors, IT consultants, and counselors), it was clear for the management that such extensive IT changes would not be feasible at that time. The scheduling system, however, was considered a priority because of its connection with billing and financial health. For the most part, counselors reacted to the introduction of the scheduling system with an attitude of skepticism and rejection. From an information boundary perspective, counselors felt protective of their personal schedules particularly insofar as giving up control over those schedules would reflect a reduction in autonomy. In the interviews, counselors described their hesitation to give up their current freedom to take care of some personal errands on occasion, fearing that the requirements of the new system might hinder these activities.

R: So I feel a little bit apprehensive of giving a schedule of all my free hours because I frequently, on my own can see people and reschedule during the week. So, that I would see as kind of a downside... I have so many hours I have to fill per week. So, I try to fill every hour, but I like the flexibility if I have to go pick my daughter at school because she's sick, I can just fly out of here in a free hour and get it done.

Part of the counselors' skepticism about the changes may also have stemmed from unclear communication: Some counselors clearly showed their confusion in the pre-implementation interviews. A typical reaction from a counselor appears below:

R: It is not clear to me yet how that (the centralized scheduling system) is going to happen or if it is not going to happen. I have heard that one of the advantages that the scheduling will cancel clients if I was ill for a day and reschedule clients, but they might have to let me know since I have to write it in my book. I am not clear how we are all going to do that if it is the system or if it is therapist driven. I think it is the latter but this has flipped flopped every time we talked about it for three months.

Complaints about the scheduling system were often not separated from complaints about working conditions in general. One counselor described their work situation as one of a "professional sweatshop," with poor pay and emotionally demanding work, but this was balanced by their relative autonomy, ability to manage their own schedules, and the opportunity to work with particular clients. Skepticism about the new scheduling system in part reflected skepticism that the organization had their best interests in mind. This counselor contemplated leaving her job if the new system was implemented in a certain way, and joked that she was currently not being allowed to perform her duties:

...I don't even know whether I want to stay here if someone would do it, and then they said well, we'll see. Ok, if they would just back up and let me do my job (laughs).

In light of the autonomy granted by the current system, she did not see the benefits of having someone else taking over the management of her schedule:

R: I am only one person with one book, what do I need it on a computer - you know what I mean? I don't have to coordinate with anybody else. I need to coordinate with myself, and if it's on computer then when I am on my phone and I am not near my computer... , you know it's going to be a pain in the neck -[long laugh]. That's how I feel.

Describing the exchange process, this counselor was not convinced that the new system would be to her advantage:

R: I hope the benefit to us is worth the extra steps for having to do it. That potentially giving up my scheduling, the extra work of having to clue somebody in every time I make my new change is uncomfortable, but it is uncomfortableness I am willing to tolerate for the benefits we are going to get, but it is not what I like.

After formal and informal negotiations, a compromise was reached that met most of the interests of both parties. The counselors submitted their appointment schedules with specific reference to the clients they were to see, but did not have to include information about non-appointment time. Satisfying the management's more pressing concern to expedite billing and improve communication with clients, this new system was able to address both issues without impinging on the independence of the employees. On the negative side, the counselors had to submit even more paperwork and time delays in input caused confusion, as staff members gave out mistaken or out-of-date information to clients about appointments. However, due to the compromises in the implementation, the counselors appeared to accept the system while continuing to control the amount of valuable information they wished to reveal about their work schedules. In the excerpt that follows, a counselor discusses the system after its implementation:

I: Do you have any problems with it (the new system)?

R: No, it works pretty well, because she (the clerical staff) really does her job. You know, if there is something funky there, she catches it. She is like a system in herself. She lets me know or she asks me or something... Um, I don't think there are any problems really. Sometimes the paperwork just hasn't gone through yet and the client comes, but that doesn't happen too often. They still get to us, but it makes us look unprofessional.

Both the first and second illustrations depict how employees did not passively accept the revelation of valuable information about themselves, but here, unlike in the first narrative, the employees participated successfully in a negotiation process. During this process, both parties compromised their interests and, although only a partial implementation of the new IT system occurred, employees displayed fewer complaints and a higher degree of compliance, while management was still able to benefit. This illustration aptly captures the combination of information boundaries and social exchange: The counselors were willing to give up some of their autonomy (as represented in the information contained in their daily schedules) in exchange for other benefits that management was able to supply via the change.

Illustration III: IT professionals at the Intersection

IT managers appear to have unique roles in these exchange processes because they find themselves at the intersection between employees and managers. Treated with resentment by staff because they become "surrogate managers," traditional ways of negotiating interests and protecting information have been changed or taken away by the new systems. The following example from the hospital laboratory shows an employee with IT management responsibilities who is "caught in the middle" between the other employees and the management.

I: You were saying that there are a lot of things that you like about your job. Are there some things that are frustrating about it?

R: Uh, yeah ... the inability of the staff to realize that I'm here to help and not to be ... you know, (pause) I'm not management but I'm not union ... So sometimes they get very defensive - if I'm trying to help they don't see it as a help - they see it as more of a "she's telling us what to do again". I'm here to help - I'm the one who has the computer experience, so that's very (pause) depressing and upsetting that ...

I: Why do they do that?

R: Because they have the mindset of a union - that, their boss is management and this is his secretary - she knows nothing ... No, granted I can't go in there and draw a patient but at least I can get you ready to go to that patient you know ...

In the excerpt above, the respondent began by creating three categories within the organization: people from management, union members, and people like herself who were neither. Through the uses of these categories, she revealed each party's interests, responsibilities and in particular, how aspects of their jobs that are related to IT are shaped by it. In situations where she provided troubleshooting services for union member staff, they responded with skepticism and "defensively" to her, assuming that she was management. With the introduction of the new IT, employees could no longer use the familiar mechanisms for responding to change because the system and the IT person provided a new layer of indirection to management. From a staff standpoint, the IT system and those who tend it are natural extensions of management. The IT system (alias surrogate manager) not only imposes new demands and expectations on employees but also assesses their activity level and knowledge. In this excerpt, we could indirectly see the employee response in the form of frustration addressed to IT personnel.

IT managers explained that although they have access to a great deal of information, they wanted to control its use and they made efforts to communicate to employees about their access to the information. In this excerpt, the IT director at the hospital explains that he does not want to use monitoring in his organization.

R: Another case, where the local cosmetics rep would be selling with the use of the company email system. That kind of thing could be discovered, and probably would be discovered eventually, on a case-by-case basis. It wouldn't require a mass monitoring for that. And it wouldn't be a major threat to the organization either. That's my attitude. I don't want to monitor, or even have people to think we are. I would like to make these tools encourage the most efficient forms of communication- quick, fast, and okay as long as it goes by certain guidelines.

The primary IT director at one of the academic units in the university explains that he found himself in troubling situations because of this access:

I: Do people ever wonder how much access you have to their information, to their email?

R: No I make sure everybody knows that me and one other person has access to everything. You got to understand that because we have to have access, and I assure them whenever of my personal ethics on confidentiality and all that stuff. I never let them become compromised... I'll share an incident with you that was a little troubling to me... I worked for a company where there was a disgruntled employee and there was a lawsuit involved. I got a call from person above me that they wanted me to capture all of this person's email and make it available to them. I know legally that all mail in an electronic system owned by a corporation, business, is a property of that business. But I thought I felt badly about walking a fine ethical line. I felt I would compromise that employee. It was troublesome to me. I don't hide that I have access to everything. I control various levels of access in my department; I make sure people, I want them to know how much access we have. So there are no surprises.

This excerpt suggests the importance that this IT professional ascribed to the ethicality of his behavior. The fact that he dealt with a large amount of sensitive information related to surveillance and monitoring made him vulnerable to possibly inappropriate requests from above. In addition, however, he hints that his access was a cloaked source of power. In a kind of “Santa Clause” assertion he mentions that, “I want them to know how much access we have,” as a way of signifying to any who might misbehave that he is able to see and respond to their misdeeds. Together, these two points represent a kind of dilemmatic bind: Access to information provides the potential for power over those who might misuse organizational resources, but exercising this access (e.g., by granting it to management) must be carefully guarded lest it be misused.

In contrast to the previous excerpt, however, in which the IT professionals described their roles with reference to monitoring proscribed behavior, the following excerpt pertains to the performance of regular work tasks:

R: I think it (the new system) will help...with a lot of feelings in some departments that this person works harder than I do or I work harder than this person, but it will help stop the rumor mill because it will say you've processed 8 and she's processed 20. Uh, there's something wrong with this picture, the workload isn't equal, let's distribute it a little more equal.

Here, the IT director (from the utility firm) indicated that her access to performance information enhanced the possibility of ensuring fair, performance-based outcomes for the employees involved. Note that establishing the contingency between performance and outcomes has traditionally been within the purview of management, so this excerpt again hinted at the IT professional's new intermediary role between staff and management.

Illustration IV: Managers and IT

Managers often seemed interested in the potential of electronic monitoring and surveillance as a management tool, believing that it would improve their ability to track events and thus protect the organization. For example, under requirements to comply with federal regulations, the director of the hospital laboratory describes the use of monitoring to fulfill this need as a necessity that results from the weakness of written policies:

R: Yes, we have written policies, and there's confidentiality, and we have compliance, that's the buzzword now, corporate compliance, so they yearly have to sign this thing about confidentiality and corporate compliance, and everything else (sounds bored). Words on paper, you know: "Hey, I'll sell you some results for 5 dollars, and if I get caught, I'll go somewhere else." I mean, they (the employees) don't do that, but that possibility is there for anybody to do. Just signing a statement isn't a big thing. You don't have to be big brother, but you have to have a means of tracking who was in what, where, and you can figure out why.

Interested in the potential benefits for the organization, this manager (an IT manager with primarily management responsibilities) from the public utility explains that the transaction log capabilities in the new system will help her find and correct mistakes:

R: Well, I don't think (monitoring) is a bad thing... because if you make an error and no one tells you about it, how do you know you made that error and how do you correct it? For those people who get bent of shape because you told them that they made mistakes- you know what, everyone makes mistakes- everybody needs to know how they can fix their mistakes.

At the same time, despite the potential gains (and prevention of losses) that they ascribed to the new systems, some managers described themselves as unknowledgeable from a technical standpoint and thus dependent on their IT directors and other IT personnel for the deployment of IT. Rather than being an obstacle to their work, they sometimes described their lack of formal technical training as an asset:

R: I think it's dangerous to have a technological expertise...If you are a Novell person, you see all of the solutions in terms of Novell solutions. If you are a UNIX person, you see it as a UNIX. If you are an information systems person, you tend to think about things that way... There are some advantages to not coming out of any of that, and sort of learning from each of them.

Counting on others a great deal for the direction of the changes and the implementation, these high-level managers describe their reliance and trust on the people who work directly under them, as well their awareness of the power dynamics found within these interactions:

R: ...whenever there is a decision to be made about this, I make it but I make it in their (my directors') presence. So anybody's who's uncomfortable with it, I try to explain my decision...I guess it's hard to speak up in a group against the boss, but to me it's important that they do that, when it's necessary.

R: Well, I trust... the [IT] people that are in charge, and I think they share that philosophy...So I don't have to pose any kind of discipline on them... The amount (of money) they get is (my decision), but, you know, how they spend it, I don't get involved in. I just occasionally, if it affects me personally, I weigh in.

This latter excerpt affirms that this manager gives a high degree of decision-making autonomy to the IT professionals that work for him ("...I don't have to pose any kind of discipline..."). As the IT professionals narrative implied, however, this autonomy constitutes a two-edged sword because it leaves the regulation of valuable information in the IT professional's control, with a consequent need to ensure ethical use of the information.

Consistent with the idea that these managers and high-level administrators feel that their expertise and priorities must be in other areas, there is a perception on the part of many IT personnel that management's primary interests ignore technical concerns. An IT specialist explained this divergence:

R: They're speaking different languages. They have different perspectives on the world. There's a lot of animosity. You know, the techies are the bitheads. You know, they're the network people... (They) are like, "It's my network," you know, "We run this stuff for you." And there's always sort of been this source of contention... On the other hand you have the business people who don't really understand what IT can do, and think they can just snap their fingers and something will happen. And that doesn't work either.

Together, these data suggested that the manager group is removed from the technical dimensions of monitoring in terms of expertise with the technology, that in some cases they see this distance as advantageous, and that they provide strategic direction while relying on IT professionals to provide access to the specific benefits that IT can generate.

Summary

The narrative above described findings for each of the three categories of individuals affected in different ways by IT driven change and resultant changes in employee monitoring capabilities. Looking across the whole corpus of interviews, IT changes seemed to affect traditional modes of interaction between employees and executive management. Traditional negotiation processes surrounding duties, rights, procedures, and policies including security and surveillance were redefined by the presence of the new IT system and its technical providers. The development and implementation of new processes to capture valuable information became new loci for negotiation. Due to the

direct and continuous interaction of the IT personnel with employees during the implementation and management of the IT systems, IT personnel were often perceived as responding to management's interests. As a result, staff sometimes believed that IT personnel had established a new channel for communication with management.

IT personnel without formal management responsibilities were often responsible for directly carrying out the technical implementation of the new technology. They were expected to manage and maintain the IT system and compile and report surveillance data. The variety of their activities led to intensive interaction with general staff, creating new loci for negotiation and modes of communication. Those at the top of the hierarchy of IT professionals had usually been hired to design and implement IT systems and given a relatively large amount of budgetary and decision making discretion to do so. Together these elements amounted to an extensive degree of independence and responsibility. This appeared to create a dilemma: In order to guarantee success, they were required to respond sensitively to various interest groups along with making delicate adjustments throughout the various implementation processes. These dual responsibilities (implement IT as requested by management; be sensitive to the concerns of general staff) placed them in a conflicted position.

Regardless of their prior IT expertise or degree of interest, senior administrators had as part of their responsibilities the analysis of costs and benefits of new technologies. They hired and relied upon IT experts to help them understand the capabilities of IT systems and to help with the technical details associated with implementing IT. They demonstrated sensitivity to the increased information collecting and monitoring capabilities of the new IT systems, but their reliance on IT experts to help "translate" technical issues into non-technical perspectives may have limited their ability to anticipate the full range of possible consequences.

Discussion and Conclusion

Our interview data provided some support for our synthesized framework of information privacy, power, and social exchange. In these six organizations employees did not appear to passively accept the capture of valuable information about them, but rather engaged in negotiatory processes in which they, along with managers and IT professionals, set some of the boundaries around how new IT would be used to manage valuable information flows. Next, the roles of the IT professionals in these processes were not inconsistent with the notion of intermediation between employees and managers. The high degree of information access that IT professionals had was viewed both in terms of the power it conferred and in terms of its potential for use and abuse by management. Finally, the proposed dependency of management on IT professionals for access to the valuable information from the new IT also manifested in our analysis of the interview data. Taking all these results together, the proposed triadic social exchange configuration worked well as an explanatory framework for examining the dynamics of power and information control within these organizations.

Our respondents talked about the knowledge gaps and alternative knowledges that could potentially hurt them in the event of the changes (Ditton, 2000). Specifically, they showed an awareness of how the surveillance aspect of the technological changes, rather than enhancing total knowledge about them, might easily cause misunderstandings and knowledge gaps that could potentially hurt them and the quality of their work lives. An example of is the scheduling system for counselors that would bring more attention to the time that they are not in their offices. For example, respondents explained that much of their work is done at home in their free time, and that the new system will give an inaccurate picture of their dedication to their work. Although some of their activities will come under closer scrutiny, these activities may not reflect their actual workloads, commitment to the organization, or ability to accomplish the tasks expected of them. As we saw most clearly in the social service agency and the counseling center, employees actively participated in assigning of meaning to the new surveillance processes.

In the case of some predictions that we derived from the synthesized theory, we found no explicit themes in the interview data to provide support or refutation. We expected to uncover some linkage between regulatory foci and social exchange whereby managers promoted organizational gains in alignment with employees' gains, but avoided organizational losses in conflict with employees' motivations. Specifically, we expected employees to see gains in the revelation of positive information about performance outcomes, and losses associated with the revelation of non-performance information. We expected managers to align with employees on the former and conflict on the latter, but we found no explicit evidence either way in the interviews. The absence of evidence may reflect a problem in the framework or trouble with our method of semi-structured questioning.

On a more general note, it is important for the reader to carefully consider some of the other limitations of our methods when interpreting these results. Because the number of organizations was small, and the set of organizations was limited to non-profits, one should only cautiously project the relevance of these findings onto for-profit organizations or organizations in general. Likewise, the interview data we collected, though reflecting the responses of more than 100 individuals, should be interpreted as suggestive of the beliefs, attitudes, and feelings of a subset of U.S. workers. Most of the individuals we interviewed were college trained, experienced professionals working in small or medium service-oriented organizations. Thus, our findings may not apply to other kinds of workers. Relatedly, although our cross-section of IT professionals included employees at a variety of levels in their respective organizations, we know that we have not fully represented the variety of ways in which the roles of IT professionals are evolving with respect to the implementation and management of monitoring and surveillance technologies in work organizations. Finally, our use of semi-structured interviewing excelled in providing a rich description of thoughts that respondents wished to publicize in the confidential interview setting, but it is likely that behavioral observations, anonymous self-reports, or other less intrusive methods might have yielded different points of view on the questions we explored.

Despite these limitations, however, we believe that the theory development and preliminary support that we have described in this paper have value both for future research and for humane practice in organizations. From a research perspective, the initial formulation of a framework that merges a theory of privacy with a theory of power seems to provide a useful starting point for further development and research. Privacy, in particular, though extensively studied as a legal and philosophical concept (e.g., Garret, 1974; Gavison, 1980), receives insufficient theoretical attention within the social and behavioral sciences (cf. Foddy, 1984; Newell, 1995). From a practice perspective, we believe that the evidence of employee resistance to the new IT systems described in this paper underscores the point that the introduction of monitoring and/or surveillance into an organization most “profitably” occurs within the context of a negotiatory process that brings management, employees, and IT professionals to the same table. Without recognition of and attention to the power dynamics surrounding new information technology by all involved stakeholders, the likelihood of effective, beneficial use of organizational monitoring and/or surveillance seems low.

References

- 9 to 5 / Working Women Education Fund (1990) *Stories of Mistrust and Manipulation: the Electronic Monitoring of the American Workforce*. Cleveland, OH: 9 to 5 / WWEF.
- Adams, J.S. (1965) Inequity in social exchange. In L. Berkowitz (ed.) *Advances in Experimental Social Psychology* (Vol. 2). New York: Academic Press.
- Alder, G.S. (1998) Ethical issues in electronic performance monitoring: a consideration of deontological and teleological perspectives. *Journal of Business Ethics*, 17: 729-743.
- Alder, G.S., and P.K. Tompkins, (1997) Electronic performance monitoring: an organizational justice and concertive control perspective. *Management Communication Quarterly*, 10: 259-288.
- Altman, I. (1975) *The Environment and Social Behavior*. Monterey, CA: Brooks/Cole.
- Altman, I. (1976) Privacy: a conceptual analysis. *Environment and Behavior*, 8: 7-29.
- Arkin, R.M. and J.A. Shepperd, (1989). Strategic self-presentation: an overview. In M. J. Cody and M. L. McLaughlin (eds.) *The Psychology of Tactical Communication*. Clevedon, U.K.: Multilingual Matters, 175-193.
- Ball, K. (2003 forthcoming) Elements of Surveillance: a new framework and future directions. *Information Communication and Society*, 5(4).
- Bennahum, D.S. (1999) Daemon seed: old email never dies. *Wired*, May: 100-111.

- Blau, P.M. (1964) *Exchange and Power in Social Life*. New York: Wiley.
- Brockner, J. and E.T. Higgins (2001) Regulatory focus theory: implications for the study of emotions at work. *Organizational Behavior and Human Decision Processes*, 86: 35-66.
- Cook, K.S., L.D. Molm, and T. Yamagishi (1993) Exchange relations and exchange networks: recent developments in social exchange theory. In J. Berger and M. Zelditch, (eds.), *Theoretical Research Programs: Studies in the Growth of Theory*. Stanford, CA: Stanford University Press, 296-322.
- Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13: 319-339.
- Ditton, J. (2000) Do we expect too much of open-street CCTV? *CCTV Today*, 7(1): 20-24.
- Emerson, R.M. (1972) Exchange theory part I: a psychological basis for social exchange. In J. Berger, M. Zelditch Jr., and B. Anderson (eds.), *Sociological Theories in Progress* (v. 2). Boston: Houghton-Mifflin.
- Ethics Officer Association (1997) *Sources and Consequences of Workplace Pressure: Increasing the Risk of Unethical and Illegal Business Practices*. Belmont, MA: EOA.
- Foddy, W.H. (1984) A critical evaluation of Altman's definition of privacy as a dialectical process. *Journal for the Theory of Social Behavior*, 14: 297-307.
- French, J.R.P. (1956) A formal theory of social power. *Psychological Review*, 63: 181-194
- French, J.R.P. and B. Raven (1959) Bases of social power. In D. Cartwright (ed.) *Studies in Social Power*. Ann Arbor, MI: University of Michigan, 150-167.
- Garrett, R. (1974) The nature of privacy. *Philosophy Today*, 89: 421-472.
- Gavison, R. (1980) Privacy and the limits of law. *Yale Law Journal*, 89: 421-471.
- Greene, R.W. (1998) Internet addiction: is it just this month's hand-wringer for worrywarts, or a genuine problem? *Computerworld*, 32(September): 78-79.
- Greengard, S. (1999) Web-based training yields maximum returns. *Workforce*, 78(2): 95-96.

- Grossman, M. (1998) Pithy answers to important questions: just what can employers do when it comes to monitoring their employees' cyber activity? *The Connecticut Law Tribune*, 7 September: 1.
- Haggerty, K.D. and R.V. Ericson (2002) The surveillant assemblage. *British Journal of Sociology*, 51(4): 605-622.
- Hale, R. (1998) Keeping the Firm's Network Safe Requires More Than Passwords. *New York Law Journal*, 28 December: 5.
- Hatch, D.D. and J.E. Hall (1997). Video surveillance presents HR challenges. *Workforce*, 76(8): 67.
- Higgins, E.T. (1997) Beyond pleasure and pain. *American Psychologist*, 52(12): 1280-1300.
- Higgins, E.T. (1998) Promotion and prevention: regulatory focus as a motivational principle. *Advances in Experimental Social Psychology*, 30: 1-16.
- Homans, G.C. (1958). Social behavior as exchange. *American Journal of Sociology*, 63: 597-606.
- International Labour Office (1993) *Workers' privacy. Part 2: Monitoring and surveillance in the workplace*. Geneva: ILO.
- Lind, E.A. and T.R. Tyler, (1988) *The Social Psychology of Procedural Justice*. NY: Plenum.
- Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. London: Routledge.
- Marx, G.T., J. Moderow, S. Zuboff, B. Howard, and K. Nussbaum (1990) The case of the omniscient organization. *Harvard Business Review*, 68(2):12-30.
- Mayer-Schönberger, V. (1999) Generational development of data protection in Europe. In P.E. Agre and M. Rotenberg (eds.) *Technology and privacy: The New Landscape*. Cambridge, MA: MIT Press, 219-241.
- Molm, L.D. (1991) Affect and social exchange: satisfaction in power dependence relations. *American Sociological Review*, 56(4): 475-493.
- Molm, L.D. (1994) Dependence and risk: transforming the structure of social exchange. *Social Psychology Quarterly*, 57: 163-176.
- Newell, P.B. (1995) Perspectives on privacy. *Journal of Environmental Psychology*, 13: 87-104.

- Orthmann, R. (1998) Workplace Computer Monitoring. *Employment Testing - Law and Policy Reporter*, December:182.
- Petronio, S. (1991) Communication boundary management: a theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, 1: 311-335.
- Ross-Flanigan, N. (1998) The virtues (and vices) of virtual colleagues. *MIT Technology Review*, 101(2): 52-59.
- Simon, H.A. (1965). *The Shape of Automation: For Men and Management*. New York: Harper and Row.
- Sipior, J.C., and B.T. Ward (1995) The ethical and legal quandary of email privacy. *Communications of the Association for Computing Machinery*, 38(12): 8-54.
- Smith, H.J. (1993) Privacy policies and practices: inside the organizational maze. *Communications of the Association for Computing Machinery*, 36(12): 105-122.
- Society for Human Resource Management (1991) *Privacy in the Workplace Survey Report*. Alexandria, VA: SHRM.
- Stanton, J.M. (1998) Validity and related issues in web-based hiring. *The Industrial-Organizational Psychologist*, 36(3): 69-77.
- Stanton, J.M. (2002) Information technology and privacy: a boundary management perspective. In S. Clarke, E. Coakes, G. Hunter, and A. Wenn (eds.) *Socio-Technical and Human Cognition Elements of Information Systems*, London: Idea Group, 79-103.
- Stanton, J.M., and E.M. Weiss (2000) Electronic monitoring in their own words: an exploratory study of employees' experiences with new types of surveillance. *Computers in Human Behavior*, 16: 423-440.
- Stanton, J.M., and E.M. Weiss (In Press) Technology and personnel data: Contrasting the concerns of human resource managers and employees. *Behaviour and Information Technology*.
- Stephoe and Johnson (1999) Seeing and hearing evil, *West Virginia Employment Law Letter*, 4(1).
- Stone, E.F., and D.L. Stone (1990) Privacy in organizations: theoretical issues, research findings and protection mechanisms. *Research in Personnel and Human Resources Management*, 8: 349-411.

- Taylor, G.S. and J.S. Davis (1989) Individual privacy and computer-based human resource information systems. *Journal of Business Ethics*, 8: 569-576.
- Thibaut, J.W. and H.H. Kelley (1959) *The Social Psychology of Groups*. New York: Wiley.
- Thurston, R.J. and J.R. Jones (1994) Health-care reform warrants HRIS updates. *Personnel Journal*, 73(5): 42-46.
- Vangelisti, A.L. (1994) Family secrets: forms, functions and correlates. *Journal of Social and Personal Relationships*, 11: 113-135.
- Whitener, E.M, S.E. Brodt, M.A Korsgaard and J.M. Werner (1998) Managers as initiators of trust: an exchange relationship framework for understanding managerial trustworthy behavior. *Academy of Management Review*, 23: 513-530.
- Woodman, R.W., D.C. Ganster, M.K. McCuddy, P.D. Tolchinsky, and H. Fromkin (1982) A survey of the perceptions of information privacy in organizations. *Academy of Management Journal*, 25: 647-663.
- Zakaria, N., J.M. Stanton and S. Sarkar-Barney, (Accepted for Publication) Designing and implementing culturally-sensitive IT applications: the interaction of culture values and privacy Issues in the Middle East. *Information Technology and People*.

Appendix A: More Details about Flows of Worker Information

Technology, particularly networked computers and the Internet, has affected information flow and control many areas of organizations. For example, in staffing, organizations use the Internet to capture resumes and screen recruits with tests (Stanton, 1998). In training, organizations use online curricula and certification to assess employees' skills (Greengard, 1999). In performance management, electronic monitoring and surveillance of employees has increased, especially the monitoring of email and web browsing (Sipior and Ward, 1995). In benefits, organizations use information systems to send worker data to insurance companies, payroll companies, etc. (Taylor and Davis, 1989; Thurston and Jones, 1994). Although each use of technology has an ostensible goal of benefiting the organization (e.g., through cost reduction), each use also changes who controls information about workers. Table 2 lists a handful of representative citations and an illustrative issue pertaining to new flows of worker data.

Table 2:

Examples of problems at the intersection of organizations, technology, and data about workers.

Citation	Problem Described
Bennahum (1999)	Unintentional/unplanned collection/storage of email and subsequent legal discovery led to increased liability for sued organizations.
Ethics Officer Association (1997)	66% of surveyed computer workers reported having performed one or more unethical actions at work during the previous year.
Greene (1998)	Employees were disciplined and/or fired for "Internet Addiction" detected via computer monitoring.
Grossman (1998)	Firms monitored employee use of pirated software to avoid legal liability.
Hale (1998)	Network security breaches made employment records vulnerable.
Hatch and Hall (1997)	Video surveillance of employees led to lawsuits and management-union disputes.
Ross-Flanigan (1998)	Distance collaboration with colleagues undermined trust within work groups.
Sipior and Ward (1995)	Organizational needs for liability and trade secret protection conflicted with privacy of employees' email.
Steptoe and Johnson (1999)	Covert audio and videotaping of employees created legal pitfalls and undermined trust among workers and managers.

Each of the examples in Table 2 shows a different way in which a change in the flow of worker information shifted the organizational landscape, primarily by providing some actor(s) with increased access to sensitive or valuable information about workers. In 1990, Marx *et al.* painted a picture of an omniscient organization with data collection systems that infiltrated every aspect of employees' work lives. Although this dystopian vision has not manifested in its entirety, Orthmann (1998) reported that over two thirds of companies surveyed by the American Management Association used some type of monitoring or surveillance. Instead, the use of technology to collect data about workers

has evolved haphazardly. As Smith (1993) aptly showed in his case studies, in following such evolutionary paths organizations usually fail to consider the possibility of unintended consequences from new technologies, and thus are in a reactive stance when a legal, ethical, or labor problems arise. Shifting from a reactive stance to a proactive one could enhance the well being of both workers and their organizations. In part, we believe that such an approach requires anticipating and understanding how control of worker information in the organization affects the nature of social exchanges and power dynamics among the various stakeholders. In the following sections we propose a synthesis of theoretical perspectives that provide at least a starting point for exploring the intersection of technology, information, and power in organizations.

Appendix B: Bibliography on Privacy, Monitoring, and the Workplace

- Adler, P.A., C.K. Parson, and S.B. Zolke (1985) Employee privacy: legal and research developments and implications for personnel management. *Sloan Management Review*, Winter:13-25.
- Agre, P.E. (1997). Introduction. In P.E. Agre and M. Rotenberg (eds.) *Technology and Privacy: the New Landscape* Cambridge, MA: MIT Press, 1-28.
- Allen, A. (1988) *Uneasy Access: Privacy for Women in a Free Society*. New Jersey: Rowan and Littlefield.
- Altman, I., A. Vinsel, and B.B. Brown (1981) Dialectic conceptions in social psychology: an application to social penetration and privacy regulation. *Advances in Experimental Social Psychology*, 14: 107-160.
- Attewell, P. (1987) Big brother and the sweatshop: computer surveillance in the automated office. *Sociological Theory*, 5: 87-99.
- Attewell, P., and J. Rule (1984) Computing and organizations: what we know and what we don't know. *Communications of the Association for Computing Machinery*, 27: 1184-1192.
- Chang, C.Y. (1997) Using computer simulation to manage the crowding problem in parks: a study. *Landscape and Urban Planning*, 37: 147-161.
- Clement, A. (1996) Considering privacy in the development of multimedia communications. In R. Kling (ed.), *Computerization and Controversy*. San Diego: Academic Press, 848-869.
- Culnan, M.J. (1993) How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, September: 341-361.
- Dunlop, C., and R. Kling (1991) *Computers and Controversy*. Boston: Academic Press.
- Duvallearly K, and J.O. Benedict (1992) The relationships between privacy and different components of job-satisfaction. *Environment And Behavior*, 24: 670-679.
- Eddy, E.R., D.L., Stone, and E.F. Stone (1999) The effects of information management policies on reactions to human resource information systems: an integration of privacy and procedural justice perspectives. *Personnel Psychology*, 52: 335-358.
- Ehn, P. (1989) *Work-Oriented Design of Computer Artifacts*. Stockholm: Arbetlivscentrum.

- Flynn, G. (1997) How much medical disclosure is too much? *Workforce*, 76(10): 89-92.
- Freedman, W. (1987) *The Right of Privacy in the Computer Age*. New York: Quorum.
- Frey, B.S. (1993) Does monitoring increase work effort? The rivalry with trust and loyalty. *Economic Inquiry*, 31: 663-670.
- Fusilier, M.R., and W.D. Hoyer (1980) Variables affecting perceptions of invasions of privacy in a personnel selection situation. *Journal of Applied Psychology*, 65: 623-626.
- Goffman, E. (1959) *The Presentation of the Self in Everyday Life*. Garden City, N.Y., Doubleday.
- Goffman, E. (1963). *Behavior in Public Places: Notes on the Social Organization of Gatherings*. New York: Free Press.
- Grant, R.A., C.A. Higgins and R.H. Irving (1988) Computerized performance monitors: are they costing you customers? *Sloan Management Review*, 29: 39-45.
- Greenberg, J. (1986a) Determinants of perceived fairness of performance evaluations. *Journal of Applied Psychology*, 71: 340-342.
- Greenberg, J. (1986b) Organizational performance appraisal procedures: what makes them fair? *Research on Negotiation in Organizations*, 1: 25-41.
- Greenberg, J. (1986c) The distributive justice of organizational performance evaluations. In H.W. Bierhoff, R. L. Cohen, and J. Greenberg, *Justice in Social Relations*. New York : Plenum Press, 337-351.
- Greenberg, J. (1987) Using diaries to promote procedural justice in performance appraisals. *Social Justice Research*, 1: 219-234.
- Greenberg, J. (1993) The social side of fairness: interpersonal and informational classes of organizational justice. In R. Cropanzano (ed.) *Justice in the Workplace: Approaching Fairness in Human Resource Management*. Hillsdale, NJ: Erlbaum.
- Gross, H. (1971). Privacy and autonomy. In J.R. Pennock and J.W. Chapman (eds.) *Privacy: Nomos XIII*, New York: Atherton Press, 169-181.
- Hacker, S.L. (1987) Feminist perspectives on computer based systems. In G. Bjerknes, P. Ehn, and M. Kyng (eds.). *Computers and Democracy*, Aldershot: Avebury, 177-190.
- Hammit, W.E. and M.A. Madden (1989) Cognitive dimensions of wilderness privacy: a field test and further explanation. *Leisure Sciences*, 11: 151-166.

- Hammitt, W.E. (1982) Cognitive dimensions of wilderness solitude. *Environment and Behavior*, 14: 478-493.
- Hammitt, W.E. and G.F. Brown (1984). Functions of privacy in wilderness environments. *Leisure Sciences*, 6: 151-166.
- Harris, L. and Associates, and A.F. Westin, (1981) *The Dimensions of Privacy*, New York: Garland.
- Hawk, S. (1994) The effects of computerized performance monitoring: an ethical perspective. *Journal of Business Ethics*, 13: 949-957.
- Hoylman, F. (1977) The effect of personal control and instrumental value on the experience of invasion of privacy. Unpublished doctoral dissertation. West Lafayette, IN: Purdue University.
- Ingulli, E., and T. Halbert (1998) Electronic monitoring of employees: an ethical analysis. *Employment Testing - Law and Policy Reporter*, September: 129.
- Inness, J.C. (1992) *Privacy, Intimacy, and Isolation*. New York: Oxford University Press.
- Iwata, O. (1980) Territoriality orientation, privacy orientation and locus of control as determinants of the perception of crowding. *Japanese Psychological Research*, 22: 13-21.
- Jenero, K.A. and L.D. Mapesriordan, (1992) Electronic monitoring of employees and the elusive right to privacy. *Employee Relations Law Journal*, 18(Summer): 71-102.
- Kirchner, W.K. (1966) A note on the effect of privacy in taking typing tests. *Journal of Applied Psychology*, 50: 373-374.
- Kling, R. (1987) Computerization as an ongoing social and political process. In G. Bjercknes, P. Ehn, and M. Kyng (eds.) *Computers and Democracy*, Aldershot: Avebury, 117-136.
- Kling, R. (1994) Organizational analysis in computer science. In C. Huff and T. Finholt (eds.) *Social Issues in Computing: Putting Computing in its Place*, New York: McGraw-Hill, 18-37.
- Kling, R. (1996a) *Computerization and Controversy*. San Diego: Academic Press.
- Kling, R. (1996b) Beyond outlaws, hackers, and pirates: ethical issues in the work of information and computer science professionals. In R. Kling (ed.) *Computerization and Controversy*, San Diego: Academic Press, 848-869.

- Kling, R., and S.L. Star (1998) Human centered systems in the perspective of organizational and social informatics. *Computers and Society*, 28(1): 22-29.
- Klitzman, S. and J.M. Stellman, (1989). The impact of the physical environment on the psychological well being of workers. *Social Science Medicine*, 29: 733-732.
- Kraut, R.E. (1987) Predicting the use of technology: the case of telework. In R. Kraut (ed.) *Technology and the Transformation of White Collar Work*, Hillsdale, NJ: Erlbaum, 113-133.
- Kupritz, V.W. (1998) Privacy in the work place: the impact of building design. *Journal of Environmental Psychology*, 18: 341-356.
- LePoire, B.A., J.K. Burgoon and R. Parrott, (1992) Status and privacy restoring communication in the workplace. *Journal of Applied Communication Research*, 20: 419-436.
- Marshall, N.J. (1974) Dimensions of privacy preferences. *Multivariate Behavioral Research*, 9: 255-272.
- Marx, G.T. (1998) An ethics for the new surveillance. *The Information Society*, 14: 171-185.
- Milberg, S.J., S.J. Burke, H.J. Smith, and E.A. Kallman (1995) Values, personal information, privacy and regulatory approaches. *Communications of the ACM*, 38: 65-74.
- Parent, W.A. (1983) Recent work on the concept of privacy. *American Philosophical Quarterly*, 20: 341-354.
- Pedersen, D.M. (1997) Psychological functions of privacy. *Journal Of Environmental Psychology*, 17: 147-156.
- Pincus, L.B., and C. Trotter (1995) The disparity between public and private sector employee privacy protections: a call for legitimate privacy rights for private sector workers. *American Business Law Journal*, 33: 51-89.
- Powers, M. (1996) A cognitive access definition of privacy. *Law and Philosophy*, 15: 369-386.
- Preston, D. (1998) Business ethics and privacy in the workplace. *Computers and Society*, 28(4): 12-18.
- Priest, S. and R. Bugg, (1991) Functions of privacy in Australian wilderness environments. *Leisure Sciences*, 13: 247-255.

- Prosser, W. (1984) Privacy: a legal analysis. In F.D. Schoeman (ed.) *Philosophical Dimensions of Privacy*, Cambridge: Cambridge University Press, 107-142.
- Rehnquist, W.H. (1974) Is an expanded right to privacy consistent with fair and effective law enforcement? *Kansas Law Review*, 23: 1-15.
- Rule, J., D. McAdam, L. Stearns and D. Uglow (1980) *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*. New York: Elsevier.
- Rustemli, A. and D. Kokdemir (1993) Privacy dimensions and preferences among Turkish students. *Journal of Social Psychology*, 133: 807-814.
- Schein, V.E. (1977) Individual privacy and personnel psychology: the need for a broader perspective. *Journal of Social Issues*, 33: 154-167.
- Schwartz, B. (1968) The social psychology of privacy. *American Journal of Sociology*, 73: 741-752.
- Seifman, D.H. and C.W. Trepanier, (1996) Evolution of the paperless office: legal issues arising out of technology in the workplace. 1. e-mail and voicemail systems. *Employee Relations Law Journal*, 21(Winter): 5-36.
- Sipior, J.C., B.T. Ward, and S.M. Rainone (1998) Ethical management of employee e-mail privacy. *Information Systems Management*, 15: 41-47.
- Smith, H.J., S.J. Milberg and S.J. Burke, (1996) Information privacy: measuring individual's concerns about organizational practices. *MIS Quarterly*, June: 167-195.
- Stanton, J.M., and J.L. Barnes-Farrell (1996) Effects of electronic performance monitoring on personal control, task satisfaction and task performance. *Journal of Applied Psychology*, 81: 738-745.
- Stanton, J.M. and L.M. Sulsky (1999) Big and little brothers: recent findings on electronic performance monitoring. Symposium presented at the annual meeting of the Society for Industrial-Organizational Psychology, Atlanta, GA, 29 April - 2 May.
- Stanton, J.M., C.D. Daniels, and G.T. Kumkale (1998) Development and application of an instrument to measure privacy expectations in the workplace. Presentation at the 24th International Congress of Applied Psychology, San Francisco, CA, 9-14 August.
- Stone, D.L. (1986). Relationship between introversion/extraversion, values regarding control over information, and perceptions of invasion of privacy. *Perceptual and Motor Skills*, 62: 371-376.

- Stone, D.L. and D.A. Kotch (1989) Individuals' attitudes toward organizational drug testing policies and practices. *Journal of Applied Psychology*, 74: 518-521.
- Stone, D.L. and E.F. Stone (1987) Effects of missing application blank information on personnel selection decisions: do privacy protection strategies bias the outcome? *Journal of Applied Psychology*, 72: 452-456.
- Stone, D.L. and P. Vine (1989) Some procedural determinants of reactions to drug testing. Paper presented at the annual conference of the Society for Industrial and Organizational Psychology, Boston, MA, April.
- Stone, E.F. (1980) *Testimony presented at U. S. Labor Department hearings on workplace privacy* (Working Paper 7). West Lafayette, IN: Purdue University, Information Privacy Research Center.
- Stone, E.F. and D.L. Stone (1990) Privacy in organizations: theoretical issues, research findings and protection mechanisms. *Research in Personnel and Human Resources Management*, 8: 349-411.
- Stone, E.F., H.G. Guetal, D.G. Gardner and S. McClure, (1983) A field experiment comparing information privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68: 459-468.
- Stone, E.F., D.L. Stone and D. Hyatt (1989) Personnel selection procedures and invasion of privacy. In R. Guion (Chair), *Privacy in organizations: Personnel selection, physical environment, and legal issues*. Symposium conducted at the annual conference of the Society for Industrial and Organizational Psychology, Boston, MA, April.
- Strickland, L. (1958) Surveillance and trust. *Journal of Personality*, 26: 245-250.
- Tepper, B.J. and C.K. Braun (1995) Does the experience of organizational justice mitigate the invasions of privacy engendered by drug testing? An empirical investigation. *Basic and Applied Social Psychology*, 16: 211-225.
- Thomson, J.J. (1975) The right to privacy. *Philosophy and Public Affairs*, 4: 295-314.
- Tolchinsky, P. D., M. McCuddy, J. Adams, D.C. Ganster, R. Woodman, and H.L. Fromkin (1981) Employee perceptions of invasion of privacy: a field simulation experiment. *Journal of Applied Psychology*, 66: 308-313.
- Turkington, R.C. (1990) Legacy of the Warren and Brandeis article: the emerging unencumbered Constitutional right to informational privacy. *Northern Illinois University Law Review*, 10: 479-520.

- U.S. Congress, Office of Technology Assessment (1987) *The Electronic Supervisor: New Technology, New Tensions*. OTA-CIT-333, Washington, DC: U.S. Government Printing Office.
- Vest, J. M., M.J. Vest, S.J., Perry and F. O'Brien (1995) Factors influencing managerial disclosure of AIDS health information to coworkers. *Journal of Applied Social Psychology*, 25: 1043-1057.
- Wagner, I. (1996) Confronting ethical issues of systems design in a web of social relationships. In R. Kling (ed.) *Computerization and Controversy*, San Diego: Academic Press, 889-902.
- Warren, S.D. and L.D. Brandeis (1890) The right to privacy: the implicit made explicit. Reprinted in F.D. Schoeman (ed.) (1984) *Philosophical Dimensions of Privacy: An Anthology*, Cambridge: Cambridge University Press, 75-103.
- Westin, A.F. (1970) *Privacy and Freedom*. New York: Atheneum.
- Westin, A.F. (1992) Two key factors that belong in a macroergonomic analysis of electronic monitoring: employee perceptions of fairness and the climate of organizational trust or distrust. *Applied Ergonomics*, 23: 35-42.

Appendix C: Sample Interview Protocol (Workers at Social Service Agency)

Before we begin, I need to mention a couple of formalities about this interview. I am working with Dr. Jeffrey Stanton at Syracuse University on a project that has been funded by the National Science Foundation. This research has been approved Syracuse University's institutional review board and given project number 01123. In this research we are looking at some effects of technology on the workplace and the changes that occur with the introduction of new information systems and practices. We would like to get your perspectives on these issues during this 50-minute interview.

All of your responses will remain confidential. We will aggregate information from many individuals to develop our research conclusions. Neither you personally nor your organization will be identified in any of our research. We will protect your identity in any reports that are provided as feedback to your organization.

With your agreement, we would like to tape record this interview. For this reason we ask that you try to avoid naming specific individuals associated with your organization. Remember that your participation is voluntary and you are free to not answer any question that does not fit your circumstances or that you feel is inappropriate; you may also withdraw from the interview at any time. As you know, I have already obtained approval to ask for your voluntary participation. If you wish to participate, please read and sign the attached informed consent forms. Please keep one signed copy of the form for your records.

General Questions

1. What is your **position**? Can you tell me a bit about what you do here?
2. **How long** have you been with the organization?
3. How do you **feel** about your job? What do you like about it? What do you dislike?
4. What are your **current responsibilities** in your organization?
5. In brief, what is your "**workflow**" now? (Optional: What kinds of records do you keep? What is the process for keeping these records – timing and so forth?)
6. What is **troublesome** about these tasks? How might these be improved? (Optional: What are the problems you are having right now? What other records do you need to access that you cannot conveniently obtain now? How often would you need those data?)
7. How do **computers** (e.g., laptops) fit into this process now? Do you use a computer at work? At home?

Communication

8. How do you **communicate** with other people in your job? With clients? Other caseworkers? Supervisors? Office staff? Other departments?
9. **With whom** do you communicate most often and about what topics?
10. **How important** do you judge these communications?

11. How much do you **count on information** from other people in order to be able to do your job?
12. How do other people in the organization **communicate with you**?
13. What **kinds of information** is communicated and **how frequently**?
14. Are there any **barriers** to communication between you and specific individuals (no names, please)? Within the organization as a whole?
15. Can you think of any ways these could be **overcome**?

Changes due to Information Technology

You may have heard that your organization is planning to introduce a new software program and the use of laptops in the field, which will change the way you do your job. Now I would like to ask you some questions about these changes.

16. What have you **heard** about the proposed changes?
17. What are your **concerns** about the proposed changes?
18. How would using a **new information system** affect your **relationship with clients**? Other **caseworkers**? **Supervisors**? **Office staff**? **Administration**? **Anyone else** in the organization?
19. How would using **laptops in the field** affect your **relationship with clients**? Other **caseworkers**? **Supervisors**? **Office staff**? **Administration**? **Anyone else** in the organization?
20. How do you think **your coworkers** will react to the proposed changes?
21. How do you think **your clients** will react? What makes you think this?
22. What **benefits** can you see of having this **new information system**? What **benefits** can you see of having **laptops in the field**?
23. In what ways might it make your work life easier? More difficult?
24. What features or capabilities would the “**perfect**” system include?
25. How do you **feel about learning** the new system?
26. How do you feel about **learning how to use a laptop** in the field? (Or if you do not have computer experience, how do you feel about learning to use a computer in general)
27. In an ideal world, how would you get your training on computers, the new system, and for using laptops in the field?
28. Would it be useful to have some **training in how to explain** the laptops to clients?
29. What ways do you have, in general, to **cope with change** that occurs in your department?
30. If you have worked in **a similar setting**, can you talk about how you handled information **differently** there?
31. How **confident** are you that this new system will actually **be successful** at improving the effectiveness of the work done by your office?
32. How do you see the new system increasing or decreasing some of your current **job related stress**?
33. How do you see the system affecting your **job satisfaction**?

34. Based on your experiences in other employment settings, where does this organization stand in terms of **using technology** to help staff members do their work more effectively?

Information Boundaries

35. Think about the information that will be stored in the new system that we've been discussing. What, if any, of this information is **sensitive**? For example, what kinds of sensitive information will the system have about clients, you personally, or about your work activities?
36. In your opinion, how should **access to this information** be **controlled and protected**? For example, who should have access to it and what procedures should they have to follow to get access?
37. Do you feel that the **planning** that is going into this information system and its reported capabilities will be **sufficient** to deal with your **concerns about sensitive information**?

Barriers and IT language: User perspective

38. Who are the people here who are directly responsible for information technology (IT) in this organization? (If they are not familiar with IT, you can ask them about computers in general)
39. How much contact do you have with these people or that person?
40. What is it like working with them? In what ways do you depend on that person's expertise?
41. How do they communicate with you about IT issues?