Personal Information, Borders, and the New Surveillance Studies [1]

5/27/07

Gary T. Marx[2]

Glenn W. Muschert[3]

Forthcoming in *Annual Review of Law and Social Science*, Vol. 3

Keywords: Borders, Personal Information, Surveillance, Social Norms

Running Head: Borders and Personal Information

[1] The authors wish to acknowledge the research assistance of Leah Janssen and Anne Johnston.

[2] Massachusetts Institute of Technology; Scottsdale and Bainbridge Island Bike and Kayak Club; email: gtmarx@mit.edu. A longer version of this article is at www.garymarx.net

[3] Miami University, Department of Sociology and Gerontology, Oxford, OH 45056; email: muschegw@muohio.edu

A. Strands of Research

The intersection of new technologies, borders and personal information offers law and society scholars a way to approach information technology questions. New surveillance and communication technologies such as the internet, data mining, video camera, biometric analysis, Radio Frequency Identification [RFID] chips and the ubiquitous, many-faceted cell phone raise issues at the very core of our understanding of society and the search for the good society. The topic involves fundamental social processes of rule making and breaking, differentiation and integration and conflict and cooperation. Much of human history can be read as a struggle involving borders, both spatial and metaphorical, and the access and symbolism that these imply. In domestic settings when surveillance technology is controversial, it is often because of the crossing of a personal border or of the failure to cross a border.

Since the 1980s, there has been a boom in social science and legal scholarship related to surveillance, privacy and technology. The surge in surveillance writing is particularly noticeable since 9/11 (e.g., Ball and Webster 2003; Heymann 2003; Lyon 2003a; Parenti 2003; Cate 2004; Rosen 2004; Wood and DuPont 2006;) but the breadth and depth of this interest preceded, and goes far beyond, security issues, even as these security concerns accelerated developments within the other areas. For better and worse, social inquiry is much driven by contemporary social issues and newsworthy events.

The presence or absence of barriers to information and technologies that can gain or block access are central elements in many settings. Scholarship on the new technologies can be tracked through conducting searches of "surveillance" and "privacy" as keywords in journals. For example, Table 1 illustrates key word searches of three academic databases for sociology, law, and communications journals reveal a sharp increase in such research, especially in the last two decades. [INSERT TABLE 1 ABOUT HERE.] We observe a sharp increase in research concerning surveillance and privacy that coincides with the increased use of electronic communications technologies and computers since the 1970s.

There is a vibrant and growing international network of scholars interested in surveillance questions. (Monahan 2006) There are frequent conferences, new research groups such as the Surveillance Project at Queens University in Canada and various groups supported by the European Community such as the Urban Eye Project and new journals such as *Surveillance and Society; Ethics and Information Technology; The Information Society; Information, Communication and Society; The Journal of Information, Communication and Ethics in Society; Communications, Law, and Policy; New Media and Society;* and *I/S: A Journal of Law and Policy for the Information Age; International Political Sociology.* There are special issues of traditional journals (e.g., Block 1992; Jermier 1998; Mack 2001; Marx 2002; Thiessen 2002; Marguilis 2003; van Harten and van Est 2003; Hillyard 2004 and 2007; *Social Text* 2005; *Contemporary Sociology* 2007; *University of Ottawa Law and Technology Journal* Forthcoming).

In 2005-06 alone, five significant edited sociological books were published with scores of contributors (Zureik and Salter 2005, Lace 2005, Haggerty and Ericson 2006, Lyon 2006, Monahan 2006) and many more monographs and edited volumes are on the way. Major public policy commission reports appeared in Britain and the U.S. (Wood 2006; National Research Council 2007) along with a comprehensive overview (Lyon 2007); an encyclopedia of privacy (Staples 2007) and a text book (Goold 2007). Universities increasingly offer courses in surveillance studies.

There are numerous strands of research in geographically and academically diverse areas, yet a boom in research does not necessarily mean an equivalent boon for broad understanding. Indeed it can instead be overwhelming and involve endless rediscovery. There is a lack of integration among literatures and studies do not sufficiently build upon each other. Work tends to be either unduly theoretical or empirical. There are relatively few middle range approaches involving systematic empirical inquiry guided by an effort to assess ideas.

B. Classifying the Field

There is no commonly held view of how to classify this research. One broad approach involves the discipline of the researcher. Among the most commonly represented fields: law, sociology, criminology, communications, cultural studies, science and technology studies, geography, planning, political science/international relations, psychology, history, economics, business and philosophy.

Perhaps the largest single category of "surveillance research" involves public health efforts. While much of this is biologically focused, there are also social and legal elements involving the spread of disease and control efforts mandating testing and quarantine. Foucault in a number of places wrote about control efforts with respect to the plague and other forms of illness (Elden 2003).

For law the emphasis is on constitutional, legislative and regulatory questions. A sampling of the voluminous literature with social science implications: (Froomkin 2000, Sharpe 2000, Slobogin 2002, Turkington and Allen 2002, Solove et al. 2006, Bharucha et al. 2006, Harcourt 2007, Mair 2006).

With respect to the privacy component, this work stands on foundations suggested by Warren and Brandeis (1890), Dash, Schwartz, and Knowlton (1959), Prosser (1960), Westin (1967), Fried (1968), Miller (1971), Bloustein (1979), and Gavison (1980).

Illustrative books in a sociological tradition with respect to historical developments and change include: Rule (1974), Cohen (1985), Beninger (1986), Dandeker (1990), Giddens (1990), Bauman (1992), Nock (1993), Lyon (1994), Bogard (1996), Ericson and Haggerty (1997), Brin (1998), Glassner (1999), Staples (2000), and Garland (2001). Classic studies such as Ellul (1964) and Mumford (1934) help ground the role of technology in society and society in technology.

Central topics for economics are the implications of information asymmetry for markets, new kinds of intellectual property and regulation (Stigler 1980, Noam 1997, Hermalin and Katz 2004). For geography new virtual space issues are prominent as well as new means of tracking and displaying data (Holmes 2001, Graham and Marvin 1996, Curry 1997, and Monmonier 2004).

In communications studies, researchers often focus on the increasingly mass mediated nature of social interactions and the meanings of this cultural shift (e.g., Loader & Dutton 2005), the asymmetrical nature of much supposedly interactive communications technology (Andrejevic, forthcoming), the cultural construction and marketing of fear and risk with surveillance offered as the solution (Altheide 2006). The increase in the use of media-related techniques in policing practices, such as phone taps and data mining has also been a focus in communications research (e.g., Fitsinakis 2003; Wise 2004).

Studies can be classified according to their level of attention to the presumed utopic promises or dystopic dangers of the technology and whether, when a problem is identified, it involves using or failing to use the technology. In the background here is literary work such as by Anthony Burgess, Aldous Huxley, Thomas More, George Orwell, and Yevgeny Zamyatin. Engineers, computer scientists, and business scholars are more likely to reflect optimism (e.g., Rushkoff 1999; Negroponte 1995; De Kerckhove, 1997; Mitchell 2003), while social scientists and artists, pessimism.

Inquiries can also be organized according to their substantive topics.
A frequently studied topic is individual privacy (Bok 1978 & 1982; Schoenman 1984; Barendt 2001; Nissenbaum 2004; Nissenbaum & Price 2004). But as the social fallout from unrestrained computerization has become clearer, studies considering implications for social stratification, consumption, discrimination, democracy, citizenship, identity, representation, and society more broadly have appeared (Gandy 1993, Agre and Rotenberg 1997, Gilliom 2001, Lyon 2003b, Regan 1995, Alpert 2003, Monahan 2006, Phillips 2006).

Research can be categorized based on particular techniques such as biometrics (Nelkin and Tancredi 1994), RFID chips (Garfinkle 2000) or cultural expression in art, film, drama, music, and landscape architecture (Marx 1996; Groombridge 2002; Pecora 2002; McGrath 2003; Gold & Revill 2003).

The field can also be organized around institutional areas beyond public health such as work (Jermier 1998; Maxwell 2005; Weckert 2005), consumption (Gandy 1993; Lace 2005), criminal justice (Brodeur & Leman-Langlois 2006; Elden 2003; Goold 2004), libraries (Minow & Lipinski 2003), military (Donahue 2006; Haggerty & Gaszo 2005), education (Webb et al. 2004), health (Nelkin & Tancredi 1994; Ghosh 2005), spatial design (Curry 1997; Flusty 2001; Monmonier 2004) and domestic and international security (Della Porta 1998, Cunningham 2004, Varon 2004, Davenport et al. 2005, Boykoff 2006, Bigo 2006; Cate 2004; Lyon 2003a; Monahan 2006). There is also work on particular subgroups such as children (Penna 2005; Mirabal 2006), the elderly

(Kinney et al. 2003; Kinney & Kart 2006), and the ill (Timmermans & Gabe 2002; Stephens 2005).

The primary goal of the scholar can be considered. Is it to advance basic knowledge (and then to document, explain or both), evaluate impacts, or to analyze legal and regulatory issues for public policy purposes? Such research contrasts with the generally descriptive, non-analytic work of most journalists (e.g., Davis 1990, Sykes 1999, O'Harrow 2005, Garfinkle 2000, Parenti 2003).

Within the basic research category we can often separate conceptual and theoretical efforts from those that involve systematic (or unsystematic) empirical research. Much of the empirical research is of the case study variety, relying on observation, interviews and the analysis of documents (McCahill 2002, Tunnell 2004, Gilliom 1994 & 2001). There is also a small quantitative evaluation literature on Closed Circuit Television [CCTV] use (particularly in the UK - e.g., Norris et al 1998; Newburn and Hayman 2002; Goold 2004; Hempel and Töpfer 2004; Welsh and Farrington 2004). However, relative to the ubiquity of, and vast expenditures on, CCTV there has been very little evaluation, particularly in the United States. The same holds for the paucity of independent studies of the impact of drug testing.

With respect to more theoretical, or at least conceptual, efforts the field has offered an abundance of similar concepts that seek to label the essence and/or account for the arrival of the new surveillance. Much of this work is in essay form and broadly in the tradition of Bentham and Foucault, as well as Taylor, Weber, Durkheim, Nietzsche, Marx, Hobbes and Machiavelli.

C. Surveying the Needs of the Field

Most surveillance essays illustrate their claims by reference to historical examples, newsworthy events and secondary empirical data. In an effort to be inclusive they generally sweep across technologies and contexts in offering macro-theoretical accounts. There is generally a failure to deal with variation or to indicate just what it is that is being explained beyond an implicit contrast between the earlier and new forms. In most cases we are offered little guidance with respect to how the ideas might be assessed or contrasted with alternative approaches.

There is need for more operationalized approaches which permit finer-grained contrasts and seek to explain diverse organizational and institutional settings, goals, technologies and varied national and cross cultural responses. As well we need to go beyond static structural approaches to studies of process, interaction, implementation, and diffusion and (sometimes) contraction in the careers of surveillance activities.

We even lack an adequate English term conveying the full meanings of surveillance. The Latin roots are *sur* = super, *vidre* = to look and *vigilare* = to keep watch. Super-watching conveys an important strand, but is awkward. For those uncomfortable with to *surveil*, the English term to *survey* which can involve either a

general overview or a critical inspection is the best we have. One can also play with prepositions –viewing and contrasting surveillance as looking over, under, above, below, beyond, back, out and for, as these apply to both agents and subjects and to position, time and goals.

In an interesting reversal, Mann et al. (2003) labels his use of video cameras to record the behavior of the more powerful *sous-surveillance.* It is that not only because it is done by those presumably socially below, but also because in probing underneath it may reveal taken for granted social worlds.

Holding apart a broad definition, a number of terms intended to capture modern and contemporary aspects have been suggested such as the gaze and bio-power, (Foucault 1977 & 1980); surveillance society, the new surveillance and maximum security society (Marx 1985 & 2004); dossier society (Laudon 1986); dataveillance (Clarke 1988); super-panopticon (Poster 1990); l'anamorphose de l'etat-nation (Palidda 1992); panoptic sort (Gandy 1993); minimum security society (Blomberg et al. 1993); synopticon (Mathiesen 1997); securitization (Waever 1995); telematic society (Bogard 1996); techno-policing (Nogala 1995); information empire (Hardt and Negri 2000); surveillant assemblage (Haggerty and Ericson 2000); post-panopticon (Boyne 2000); glass cage (Gabriel 2004); ban-opticon (Bigo 2006); high policing (Brodeur and Lehman-Langlois 2006); ubiquitous computing (Greenfield 2006); ambient intelligence (Wright et al. 2007); and safe society (Lyon 2007).

The creation of concepts such as the above and the theoretical essay are a necessary first step. Yet too often they fail to disentangle the multiple dimensions that make up the ideal types and to explore their distributions, correlations and interrelations.

Consider for example Torpey's (2007) differentiation of "thin" from "thick" surveillance. The former monitors movement and transactions (e.g., as with cell phones or credit cards) generally without constraining mobility, while the latter refers to confinement to delineated and frequently fortified spaces. While thin surveillance is universal, the thicker forms disproportionately affect lower status and marginal groups, as with the institutionalized. This increasingly involves the piling on and mutual reinforcement of surveillance forms which can engender additional inequitable restrictions, data and secondary deviance (Lyon 2003b; Newburn & Hayman 2002; Patillo et al. 2004; Neyland 2006).

This distinction usefully captures some aspects of the interaction and social distribution of these two forms of surveillance. "Starter datum" can, in the vocabulary of statisticians, generate breeder documents that become central for life chances. The tightening of stigmatic social control tentacles is taken to new heights or lows depending on one's perspective. This is particularly the case in total institutions with their spill over into the broader society as a result of remote electronic monitors and functional enclosures. Border breaking technologies have major implications for social stratification - re-enforcing and in some ways undermining traditional patterns (Marx 2005b, 2007).

Yet the distinction between thin and thick surveillance also collapses dimensions that should be separately studied such as types of access (e.g., physical mobility involving combinations of entering and leaving vs. opportunities for communication, or service) and the scale or comprehensiveness of surveillance (e.g., the intensity and extensity as seen in the number of areas of life considered and the degree of probing and the integration of data). Rule's (1974) work which contrasts the power of surveillance systems with respect to variables such as the size of their files, degree of centralization and the rapidity of communication between different systems suggests related variables.

Conclusions, whether explanatory or evaluative, require identifying the dimensions by which the richness of the empirical world can be disaggregated. To be sure we need broad ideal types, but we also need to identify specific dimensions in order to take systematic account of the variation whose causes, processes and consequences need to be understood. Marx (2004) for example suggests 27 dimensions by which any surveillance mean can be contrasted.

With respect to the new surveillance among the most important aspects: extends the senses, low visibility, involuntary, remote, lesser cost, multiple indicators, strategic, integrated, automated, real time data flows, attention to systems and networks as well as individuals, routinization of surveillance into everyday life, immediate links between data collection and action and emphasis on predicting the future and preventing some forms of it. When not hidden altogether, the new information gathering seeks to be soft, relatively non-invasive, unnoticeable, and to avoid direct coercion (Marx 2006).

Goals are another area where analytical differentiation is required. One approach considers variation in surveillance means and goals as these relate to different types of institution. The interaction between surveillance means and goals and the extent to which they independently or reciprocally change has been little studied. There is of course rarely only one goal. Marx (Forthcoming) outlines 12 major goals associated with surveillance practices, including compliance, documentation, management/coordination, discovery, publicity, symbolism, and curiosity.

The presumed rationality of goals must also be analyzed. Tunnell (2004) for example argues that the emergence of urine drug tests had more to do with the behaviors of moral entrepreneurs than with any rational evidence that drug use was increasing in its prevalence and consequences

D. A Sociology of Information Framework

An emphasis on the rules about information in general and personal information in particular, constitutes one part of a broader field of *the sociology of information.*

Defining the Framework: Central questions broadly within such a normative approach are: what are the rules governing the protection and revelation of information, how are they created, what are their consequences and how should they be judged? Who has access to personal information and under what conditions? How do factors such as

the type of physical, temporal and cultural border, the type of relationship among actors, the roles played, the type of information involved, the form of its presentation, the characteristics of the means used and the goals sought effect rules about information and the distribution of various surveillance forms?

What factors condition varying connections between the rules and actual behavior? How do normatively sanctioned and coercively supported data extractions (or data protections) differ from softer, seemingly voluntary (and often seductively elicited) revelations (or protections - e.g., industry favoring self-regulation)? How is information treated once it has been gathered (e.g., security, repurposing, alteration, retention and destruction)? What types of sanctions with what consequences are attached to rules about information?

What does surveillance focus on --individuals, groups, organizations, or environments? And, once focused, what does it look for (e.g., rule compliance, eligibility, wanted persons, purity, networks, location) and what actions, if any flow from the activity? How are results assessed, where are the lines drawn, how valid are the instruments used, both in general and as applied in a given context?

Borders are central factors for understanding surveillance. They of course may include or exclude as they facilitate or restrict the flow of information, persons, goods, resources and opportunities (Zureik and Salter 2005, Andreas and Nadelmann 2006). The literal and symbolic role of border surveillants as guardians, gate keepers, spotters, cullers and sorters needs to be better understood, as well as subject responses. The ability of the new technologies to pierce previously impenetrable physical borders and create new borderes offers a rich field for studying the emergence of new prescriptive and proscriptive norms.

The directionality of personal border crossings can also be considered. Most attention is on taking information *from* the person. But this needs to be contrasted with impositions *upon* the person –whether sound, images, smells or unwanted messages (e.g., much telemarketing and spam). These of course may be joined as with Orwell's telescreeen or in current terms when the monitoring of internet behavior leads to spam. Note also forms such as TIVO which transmit data to the viewer and also receive data on the viewer and blur the communication-surveillance distinction.

Privacy and *publicity* are major concepts here as they form polar ends of a continuum involving rules about withholding and disclosing, and seeking or not seeking, information. Depending on the context, social roles and culture, individuals or groups may be required, find it optional, or be prohibited from engaging in these activities, whether as subjects or agents of surveillance and communication.

Rules are at the heart of publicity and privacy. When the rules specify that information is not to be available to others (whether the restriction is on the surveillance agent not to discover or less often, on the subject not to reveal or on the means) we can speak of *privacy norms*. When the rules specify that the information must be revealed by

the subject or sought by the agent and that particular means are to be used, we can speak of *publicity norms*

A sociology of information approach emphasizing norms permits joining freedom of information and right to know issues with the right to control personal information – a logic reflected in some European and Canadian privacy commissions (Flaherty 1989, Bennett and Raab 2006). Table 2 outlines our proposed sociology of information approach. [INSERT TABLE 2ABOUT HERE.]

Let us additionally illustrate some social structural and process aspects. With respect to structures and roles we can note the *surveillance agent* (watcher, observer, seeker, surveyor) is distinct from the person about whom information is sought is a *surveillance subject*. The activity may be *agent-initiated* vs. *subject-initiated.* Contexts of *cooperation* where goals overlap or are shared, as against those where agents and subjects are in *conflict* Surveillance can be analyzed with respect to whether it is *non-reciprocal* or *reciprocal*. Surveillance that is reciprocal may be *asymmetrical* or *symmetrical*. *Organizational surveillance* is distinct from the *non-organizational surveillance* done by individuals. The *internal constituency surveillance* found in organizations contrasts with *external constituency surveillance* present when those who are watched have some patterned contact with the organization (e.g., as customers) or are otherwise of interest to it –whether or as clients or competitors. With respect to personal *surveillance* we can differentiate *role relationship surveillance* as with family members from *non-role relationship surveillance* as with the voyeur whose watching is unconnected to a legitimate role. The surveillance function may be *central* or *peripheral* or *peripheral* and can involve those who are a party to the generation and collection of data (*direct participants*) or *third parties*.

Rather than being static and fixed at one point in time, surveillance needs to be viewed as a fluid, ongoing dynamic process involving interaction and strategic calculations over time. Among surveillance processes are efforts to create the *myth of surveillance, surveillance creep* and *surveillance commodification. Behavioral techniques of neutralization* –strategic moves by which subjects of surveillance seek to subvert the collection include: direct refusal, discovery, avoidance, switching, distorting, counter-surveillance, cooperation, blocking and masking (Marx 2003).

An important and little studied aspect involves a life history of surveillance events in which we analyze a variety of outcomes between the development of a tactic and the way it is implemented (if it is) and applied, as well as patterns of diffusion across institutions, goals and societies.

A more micro issue is the link between the allocation of surveillance resources, the collection of the information and the subsequent action in individual cases. The dynamic nature of the topic calls for cases studies of interaction, beyond the formal content of law and policies or correlations devoid of context. This is the location for studying surveillance and equity - not only with respect to the allocation of the tools but also outcomes.

The political economy of the environment is central for such questions and we must attend to power and negotiation. Phillips (2006) calls attention to the surveillance infrastructure within which actors use rhetoric, technology and economic and legal resources to pursue their goals. He suggests a processual model involving identification, tracking, monitoring, analysis and response.

The production and use of knowledge hardly ushers forth from a virgin spring of technique. Rather different outcomes will be seen depending on interaction between technical social and cultural factors. Law (1992) for example calls attention to a dynamic socio-technical network involving actors, agents, artifacts, institutions and beliefs within which technologies are understood and applied through interaction.

Applying the Framework: Once concepts are defined and variables identified, the next step is the generation of hypotheses and the specification of conditions under which they apply. As noted, the field has lagged here. Table 3 offers a sampling of tested (or testable) hypotheses for democratic societies. [INSERT TABLE 3 ABOUT HERE.]

Broader hypotheses from other areas such as political economy with respect to workers' rights and management practices or the sociology of law and social control can no doubt also be adopted fit the specific case of surveillance (which, of course, can itself be broken down into various components). In the case of the latter for example, the greater the scale and heterogeneity of a social setting the more we might expect not only formal law (Black 1976), but accompanying surveillance to discover compliance and to locate infractions and monitor penalties and subsequent behavior.

E. Emergent Value Conflicts

Too much of the work in this field reflects a misguided *either/or* fallacy. This didactic way of thinking is called forth by the search for simplicity, disciplinary socialization and specialization and fashion. It receives a boost from the binary logic of computerization that is central to so much surveillance, but which can distort the richness of social understanding.

F. Scott Fitzgerald suggests that, "the test of a first rate intelligence is the ability to hold two opposed ideas in the mind at the same time, and still retain the ability to function." In an unacknowledged borrowing, George Orwell called the malignant version of that *doublethink.* But when complex and complicated topics are involved it is well, with Whitehead, to not find clarity and consistency at a cost of, "overlooking the subtleties of truth". We need to transcend rigid dichotomies in social analysis and to identify the conditions which permit their opposition or the conditions under which only one will be accepted.

Understanding requires the capacity to see both (and more) sides of an issue and to note dialectical processes. Unlike beauty, truth isn't quite in the eye of the beholder, but it is powerfully conditioned by where, when and what one looks with and for.

Beyond receptivity to competing or contradictory methods and ways of approaching the field, our analysis suggests the importance of attending to opposing tendencies in the world. Sometimes the best answer is "both" or "yes" and "no." The key then is of course specifying the conditions likely associated with different outcomes. Below we consider this with respect to conflicts in both values and empirical patterns.

There are enduring value conflicts and ironic, conflicting needs, goals and consequences which make it difficult to take broad and consistent positions regarding surveillance, borders and personal information.

Thus we value both the individual and the community. We want both liberty and order. Consider the folk claim "those who have nothing to hide have nothing to fear" in light of the rival claim in the Bill of Rights that there must be reasons before personal borders are crossed in a search.

The broad universalistic treatment citizens expect may conflict with the specific treatment made possible by fine-honed personal surveillance data (although perhaps the more data that is gathered the more room there is for errors). The expectation that one should be judged as an individual and in context may conflict with the greater rationality and predictive success believed to be found in responding to aggregates. Individuals expect to be treated accurately and yet to have privacy respected. Depending on their role and social location individuals and groups will differ in the relative importance given to privacy vs. accuracy.

We seek privacy and often anonymity, but we also know that secrecy can hide dastardly deeds and that visibility can bring accountability. But too much visibility may inhibit experimentation, creativity and risk taking. And while we value disclosure, we also believe in redemption and new beginnings after individuals have been sanctioned for misdeeds or overcome limitations.

In our media-saturated, impression-management societies we also want to be seen and to see, (even as we also sometimes want to be left alone). Consider the desire to reveal as seen in popular talk shows and celebrity tell-all books and public relations activities.

We value freedom of expression and a free press but do not wish to see individuals defamed or harassed or unduly self-humiliated. We desire honesty in communication and also civility and diplomacy. We value the right to know, but also the right to control personal information (note the high degree of expressed concern over privacy invasions (if not always behavior consistent with this) revealed by public opinion polls).

We desire systems that are user-friendly, fast, easy to use and less expensive. The value of a network is maximized when it is widely available. Yet these goals can conflict with the needs for security and privacy.

Many discussions between those who look optimistically at information technology as the solution and those who view it as the problem reflect the Hindu tale about blind persons and the elephant, in which each observer offers a plausible

identification for one part of the elephant (e.g., the tail as rope). A legitimate goal or social trend is identified but other confounding ones are ignored or denied.

Let us next note some contradictory empirical patterns and processes. Technology can simultaneously be value neutral and reflect partisan interests. On the one hand there is a democratizing element to surveillance in that it can capture whatever is *available to be captured* (e.g., video cameras are indifferent to gender and race). But the location and use of the cameras is socially and personally, rather than randomly patterned.

It is important to acknowledge the sense in which information invasive technologies are (and can be) neutral. Yet the actual use needs to be considered apart from its *potential* use. Part of the neutrality or equality-of-technology argument is equivalent to Anatole France's observation that the rich and the poor are both forbidden to sleep under bridges or steal a loaf of bread.

Certainly the camera, audio recorder, or motion detector will capture *whatever* is encountered. But this egalitarian potential of the new technology does not mean that all persons and settings have an equivalent chance of being surveilled. Nor are the resources (whether cultural or physical) to defend, resist, and challenge equally distributed in stratified settings and societies.

The notion of accountability and deterrence through visibility is a major justification for crossing personal information borders (Etzioni 1999, Allen 2003). In the New Testament we read, "Everyone who does evil hates the light, and will not come into the light for fear that his deeds will be exposed. But whoever lives by the truth comes into the light, so that it may be seen plainly that what he has done has been done through God." (John 3:20-21). Here surveillance both rewards and prevents (or at least leads to hiding).

Yet for others differently motivated, surveillance may fail not only in the sense of not deterring, but it may actually help the violator. If surveillance is to deter, potential violators must be told of the threat. Beyond this functional aspect, fair information practices require notice. This can be exploited. Those highly motivated to infraction may adjust their behavior accordingly. In the case of video surveillance for example this can involve displacement to areas without cameras. Others may seek notoriety and sanctioning (whether exhibitionists, attention seekers or would-be martyrs). In that sense visibility may have an opposite effect. The heterogeneity in motives among subjects of surveillance requires study.

F. Toward an Emergent Sociology of Information Technology

While much contemporary surveillance is partly defined by its ability to root out the unseen and unknown, it also paradoxically may reveal itself through electrical and chemical and other forms of data. That which silently gathers the emanations of others, if not exactly a mirror image, none-the- less emanates itself, offering discovery possibilities

and means of neutralization to technically competent adversaries. The watchers may also be watched by the same means they apply to others.

Note also operational conflicts as seen in diverse goals such as apprehension and deterrence. The need for concealment supports apprehension ("caught in the act"). While visibility may support temporary prevention but lead to displacement. Consider literature such as Norris and Armstrong (1999) or Sewell and Barker (2006) on the protective and caring aspects of organizational surveillance.

There is the tension between trying to regulate risky tactics versus ignoring them in the hope that the absence of legitimation will curtail their use. A legalistic or bureaucratic codification may restrict them, but also serves to sanctify them, if under limited and reviewable circumstances. The absence of a formal mandate may inhibit the use of a tactic.

A technology's characteristics and social and cultural factors need to be appreciated as independent, as well as interdependent causes. The ability to collect personal data offered by miniaturized, sense-extending devices capable of remote transmission creates a potential for surveillance apart from the awareness or consent of the subject. Yet the technology is found in a social setting in which prior social and cultural factors determined the technology's development and condition the way it is used. Contrast the extensiveness of undercover police and drug testing in the United States with their minimal (if expanding) use in Europe, or the much greater use of video cameras in Britain than elsewhere (although again a difference that appears to be lessening) (Marx 1995). Or consider the Supreme Court's ruling in the Kyllo case which found that a thermal search which so easily and passively took information radiated from the interior of a house was none-the-less a search falling within the Fourth Amendment for constitutional purposes.

The either/or debate between strong versions of technological and social determinism is misplaced. Rather we need to specify conditions under which these are independent or causally linked. Legal changes may spark technical innovations as well as the reverse. For example, Constitutional and legislative limits on searches and interrogation stimulated federal funding for non-invasive ways of discovering personal information. Just as technical developments in wiretapping and hidden recording have led to laws limiting these but also create markets for new counter-technologies. Given the vastness of the field and variety of relevant variables more often than not, it is a monumental challenge to be able to order these in a temporal fashion and to control for the multiplicity of causal influences.

There is a significant expansion in the ways and categories for measuring and classifying individuals and contexts, both retrospectively and prospectively. We increasingly see the integration of life activities with the generation of personal data. More and more we live in ways that automatically provide personal information as part of the activity – i.e., the use of credit cards, communication and driving. Wright et al. (2007) presents some imaginative (yet science and technology based) dark scenarios with

respect to what might go wrong given this reliance on technology.

There is a blurring of lines between public and private places making personal information more available. Note the privatization of places traditionally seen as "public" such as shopping malls and industrial parks (with legal means of collecting personal information) and the blurring of the lines between home and work (Shearing and Stenning 1986; Nippert-Eng 1996; Marx 2001 & 2005a). Note also the parallel restrictions and (for some) opportunities found with new forms of electronic-digital enclosures (Boyle 2003, Andrejevic, forthcoming). Here user's transparently generate data regarding the transaction itself (e.g., who, where, when, path taken and content) and this often goes to unknown agents using it for we know not what.

Simultaneously and not unrelated to the above, there have been major developments in technologies that enhance the borders that protect information. With encryption and audit trails for example there is the potential for a degree of confidentiality in communication, and enhanced accountability and data protection never before seen. Technologies and services for protecting personal information are increasingly available, from shredders to home security systems to various software and privacy protection services.

We see new normative protections and awareness as well. There has been a significant expansion of laws, policies and manners that limit and regulate the collection of personal information and its subsequent treatment. Bennett and Raab (2006) note this as a world wide trend and the frequently revised list of laws published by Privacy Journal (Smith 2002) has grown extensively over recent decades. There has been some growth in choice and opt-in systems and greater awareness that fair information practices can be good for business. This also ties to the broader 20th Century expansions of civil liberties and civil rights, as well as to particular crises. Whether these go far enough, are effective, and how they compare across institutions and cultures are important research questions.

Another type of conflict can be seen in the rival empirical claims of proponents and opponents of particular technologies, uses and rules about enabling, controlling or prohibiting these. For example does drug testing deter drug use or push it to new drugs not detected by the test or lead to neutralization means that permit deceiving the test? Do burgeoning interactive communication media extend democratic participation (e.g., of consumers relative to producers) or asymmetric manipulation?

The value conflicts and opposing trends noted work against sweeping generalizations beyond this one against sweeping statements. Considered together some of the above developments are ironic and contradictory, we take this as a sign of reality's ability to overflow our either/or categories and the need to avoid simplistic theorizing, as well as suggesting the need for empirical research.

These enduring tensions do not lend themselves to glib imperatives (unless it is the imperative of rejecting imperatives), and they are more challenging, if less provocative than the gathering herds of one-trick ponies, as a result.

G. Concluding Moral Mandates

Over the last decades, we have observed the rapid development of technologies of surveillance and communication. The resultant changes these have sparked related to borders of personal information have been of great interest to scholars in a variety of fields. In an attempt to unify and direct the field, we have proposed suggestions for a sociology of information framework (Table 2) and illustrative testable hypotheses (Table 3). Given the frequent link between social control and normative direction found with the topic, we conclude with an old AR tradition of moral mandates for scholars of surveillance (for the tradition cf. Marx and Wood 1975, 415-7). The field would be stronger and future literature reviewers will be able to engage in *more* reviewing, summarizing and building and *less* question raising, concept defining and critiquing than we have done here, to the extent that these are followed.

Disaggregate and then aggregate! We need to break the world down into manageable analytic and empirically measurable bites, but it also must be put back together. There must be greater emphasis on integrating knowledge from the many strands of surveillance inquiry.

Adopt a systems approach. Rather than restricting attention to either superordinates or subordinates (a factor often determined by the politics and support of the analyst) view both as part of a broader system. Study both the subjects and the agents of surveillance and their interaction. Be alert for unsullied literal independent variables, but also to feedback and reciprocal influences. Avoid simplistic determinism/reductionism.

Recognize that things change but also stay the same. Start by locating the broad constants found in any surveillance information context and within these, the major areas where variation and re-occurring forms and processes can be identified.

Study surveillance practices as an interaction process. Research too must be continually in process, responding to changes in the game and moves of the players. The effort to understand atrophy, entropy, neutralization, escalation, evolution, devolution, contraction, displacement, and border changes must be central to inquiry.

Naming names is not enough! Disentangle the multiple dimensions frequently found with ideal types and suggest ways of measuring these so their distribution and interrelations can be empirically documented and assessed.

Validate empirical findings from surveillance technologies, particularly when life chances are involved and do not assume that meaning is self-evident. Correlation does not necessarily represent causality or guilt. A correlation may be invalid because of weak measures or incompetent application of strong measures. Even when valid, inferences from a correlation or a match may be spurious. The facts do not speak for themselves. Never underestimate the significance of street level applicators in defining what results means (Paik 2006).

Don't assume that the reasons publicly offered for a given behavior are necessarily the real reasons. It is important to consider expressed motives in understanding behavior and we show respect for those studied by listening to their accounts. Yet causes can be found at many levels beyond the rhetoric of actors, even when they are being truthful within the limits of their understanding.

Don't confuse probabilistic (aggregate) predictions/statistics about groups with predictions about any given individual or event. This can involve conflict between efficiency and order for the group as against fairness or liberty for the individual. Actions that are rational in the aggregate on a statistical basis may be unjust for the individual (what Robinson in 1950, in anticipating profiling errors called the ecological fallacy).

The days of judgment are here now! Offer the reader logical and empirical criteria by which arguments and results can be evaluated. This necessitates clear definitions and, when appropriate, specification of independent and dependent variables. We need to develop more systematic empirical and logical ways of assessing normative issues of equality, ethics and law as they involve personal informational borders. Marx (2005a) suggests 20 questions to be asked when evaluating any surveillance technology.
In a democratic society soft, manipulative and non- or quasi-consensual forms that transcend the unaided senses are of particular interest. Much research focuses on the conditions surrounding the data collection. Greater attention should be given to the actual use, particularly where this involves asymmetrical border sites with implications for social stratification and fairness.

Neither a pessimist nor an optimist be, in the absence of good data! Don't let fears and hopes confound your analysis of the empirical record. Keep distinct statements about the world as it now is from predictions or descriptions of what *might* happen. But don't ignore the latter.

Maintain truth in scholarship (and activism). What team are you on? What game are you playing? Try to separate statements of fact from those of value, even as we appreciate how interwoven these may be, given the importance of values and passion in social inquiry

References

Agre P, Rotenberg M, ed. 1997. *Technology and Privacy: The New Landscape.* Cambridge, MA: MIT

Allen A. 2003. *Accountability for Private Life*. Lanham, MD: Rowman and Littlefield

Alpert S. 2003. Protecting medical privacy. *Journal of Social Issues* 59(2): 301-22

Altheide D. 2006. *Terrorism and the Politics of Fear*. Lanham, MD: AltaMira

Andreas P, Nadelman E. 2006. *Policing the Globe*. New York: Oxford Univ.

Andrejevic M. Forthcoming *iSpy: Surveillance and Power in the Interactive Era.* Lawrence, KS: Univ. Press of Kansas

Ball K, Webster F, ed. 2003. *The Intensification of Surveillance*. London: Pluto

Barendt EM, ed. 2001. *Privacy*. Ashgate, UK: Aldershot

Bauman Z. 1992. *Imitations of Postmodernity*. New York: Routledge

Beniger JR. 1986. *Control Revolution*. Cambridge, MA: Harvard Univ.

Bennett C, Raab C. 2006 *The Governance of Privacy.* Cambridge, MA: M.I.T.

Bharucha A, et al. 2006. Ethical considerations in the conduct of electronic surveillance research. *Journal of Law, Medicine & Ethics* 34(3): 611-9

Bigo D. 2006. Globalized-in-secutiry. In *Translation, Biopolitics, Colonial Difference*, ed. N Sakai, J Solomon, London: Eurospan

Black D. 1976. *The Behavior of Law.* New York: Academic

Block A. 1992. Special issue: issues and theories on covert policing. *Crime, Law & Social Change* 10(1-2)

Blomberg T, Bales W, Reed K. 1993. Intermediate punishment: redistributing or extending social control? *Law & Human Behavior* 17(1):187-201

Bloustein EJ. 1979. *Individual and Group Privacy*. New Brunswick, NJ: Transaction

Bogard B. 1996. *The Simulation of Surveillance*. New York: Cambridge Univ.

Bok S. 1978. *Lying*. New York: Pantheon

Bok S. 1982. *Secrets*. New York: Pantheon

Boyle J. 2003. The second enclosure movement and the construction of the public domain. *Law and Contemporary Problems* 66(Winter/Spring): 33-74

Boyne R. 2000. Post-panopticism. *Economy and Society* 29: 285-307

Boykoff J. 2006. *The Suppression of Dissent: How the State and Mass Media Squelch American Social Movements.* New York: Routledge

Boyne R. 2000. Post-panopticism. *Economy and Society* 29(2): 285-307

Brin D. 1998. *The Transparent Society*. Reading, MA: Perseus

Brodeur JP, Leman-Langlois S. 2006. Surveillance fiction or higher policing. In *The New Politics of Surveillance and Visibility,* ed. K Haggerty, R Ericson. Toronto: Univ. of Toronto

Cate F. 2004. *Safeguarding Privacy in the Fight against Terrorism*. Washington, DC: Department of Defense

Clarke R. 1988. Information technology and dataveillance. *Communications of the ACM* 31(5): 498-512

Cohen S. 1985. *Visions of Social Control*. Cambridge, UK: Polity

Contemporary Sociology. 2007. Taking a look at surveillance studies: a symposium featuring essays by David Lyon, Elia Zureik, John Torpey, David Cunningham, and G.T. Marx. 35(2)

Cunningham D. 2004. *There's Something Happening Here: The New Left, the Klan, and FBI Counterintelligence.* Berkeley: Univ. of California

Curry M. 1997. *Digital Places*. London: Routledge

Dandeker C. 1990. *Surveillance, Power, and Modernity*. New York: St. Martin's

Dash S, Schwartz R, Knowlton R. 1959. *Eavesdroppers*. New Brunswick, NJ: Rutgers Univ.

Davenport C, Johnson H, Mueller C. 2005. *Repression and Mobilization.* Minneapolis: Univ. of Minnesota

Davis M. 1990. *City of Quartz*. London: Verso

Della Porta D, Reiner H. 1998. *Policing Protest: The Control of Mass Demonstrations in Western Democracies.* Minneapolis: Univ. of Minnesota Press.

De Kerckhove D. 1997. *Connected Intelligence: The Arrival of the Web Society.* Toronto: Sommerville House

Donahue LK. 2006. Anglo-American privacy and surveillance. *Journal of Criminal Law & Criminology* 96(3): 1059-208

Elden, S. 2003. Plague, panopticon, police. *Surveillance and Society* 1(3): 240-53

Ellul J. 1964. *The Technological Society*. New York: Knopf

Ericson R, Haggerty K. 1997. *Policing the Risk Society*. Toronto: Univ. of Toronto

Etzioni A. 1999. *The Limits of Privacy*. New York: Basic

Fijnaut C, Marx G, ed. 1995. *Undercover: Police Surveillance in Comparative Perspective.* Norwell, MA: Kluwer

Fitsinakis J. 2003. State-sponsored communications interception. *Information, Communication & Society* 6(3): 404-29

Flaherty D. 1989. *Protecting Privacy in Surveillance Societies*. Chapel Hill, NC: Univ. of North Carolina

Flusty S. 2001. The banality of interdiction: surveillance, control and the displacement of diversity. *International Journal of Urban & Regional Research* 25(3): 658-64

Foucault M. 1977. *Discipline and Punish*. New York: Pantheon

Foucault M. 1980. *History of Sexuality*, vol. 1. New York: Vintage

Fried C. 1968. Privacy, *Yale Law Journal*. 77: 475-93

Froomkin M. 2000. The death of privacy? *Stanford Law Review* 52: 1461-543

Gabriel Y. 2004. The glass cage. In *Self, Social Structure, Beliefs*, ed. J Alexander, GT Marx, C Williams, Berkeley: Univ. of California

Gandy O. 1993. *The Panoptic Sort*. Boulder, CO: Westview

Garfinkle S. 2000. *Database Nation*. Sebastapol, CA: O'Reilly

Garland D. 2001. *The Culture of Control*. Chicago: Univ. of Chicago

Gavison R. 1980. Privacy and the limits of law. *Yale Law Journal* 89: 421-71

Giddens A. 1990. *The Consequences of Modernity*. Cambridge, UK: Polity

Gilliom J. 1994. *Surveillance, Privacy, and the Law*. Chicago: Univ. of Chicago

Gilliom J. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy.* Chicago: Univ. of Chicago

Ghosh S. 2005. Surveillance in decolonized social space. *Social Text* 23(2): 55-69

Glassner B. 1999. *The Culture of Fear: Why Americans Are Afraid of the Wrong Things*. New York: Basic

Gold J, Revill G. 2003. Exploring landscapes of fear: marginality, spectacle and surveillance. *Capital & Class* 80: 27-50

Goold B. 2004. *CCTV and Policing*. New York: Oxford Univ.

Goold B. 2007. *Surveillance*. Oxford, UK: Oxford Univ.

Graham S, Marvin, S. 1996. *Telecommunications and the City. Electronic Spaces, Urban Places.* London: Routledge

Greenfield A. 2006. *Everyware*. Berkeley: New Riders

Groombridge N. 2002. Crime control or crime culture TV? *Surveillance and Society* 1(1): 30-46

Haggerty K, Ericson R. 2000. The surveillant assemblage. *British Journal of Sociology* 5: 605-22

Haggerty K, Ericson R, ed. 2006. *The New Politics of Surveillance and Visibility*. Toronto: Univ. of Toronto

Haggerty K, Giszo A. 2005. Seeing beyond the ruins: surveillance as a response to terrorist threats. *Canadian Journal of Sociology* 30(2): 169-87

Harcourt B. 2007. *Against Prediction: Profiling, Policing and Punishing in an Actuarial Age.* Chicago: Univ. of Chicago

Hardt M, Negri A. 2000. *Empire*. Cambridge, MA: Harvard Univ.

Hempel L, Töpfer E. 2004. *CCTV in Europe.* Berlin: Centre for Technology and Society

Hermalin B, Katz M. 2004. Sender or receiver: who should pay to exchange electronic messages? *RAND Journal of Economics* 35(3): 423-47

Heymann P. 2003. *Terrorism, Freedom, and Security: Winning without War*. Cambridge, MA: MIT

Hillyard D. 2004. Technology and privacy. *Knowledge, Technology and Policy* 17(1)

Hillyard D. 2007. Technology and privacy II. *Knowledge, Technology and Policy* 20(2)

Holmes D, ed. 2001. *Virtual Globalization: Virtual Spaces/Tourist Spaces.* London: Routledge

Jermier J. 1998. Critical perspectives on organizational control, *Administrative Science Quarterly* 43: 235-510

Kinney J, Kart C, Murdoch L, Ziemba T. 2003. Challenges in caregiving and creative solutions: using technology to facilitate caring for a relative with dementia. *Ageing International* 28(3): 295-313

Kinney J, Kart C. 2006. Not quite a panacea. *Generations* 31(2): 64-6.

Lace S, ed. 2005. *The Glass Consumer*. Bristol, UK: Policy Press

Laudon KC. 1986. *Dossier Society*. New York: Columbia Univ.

Law J. 1992. Notes on a theory of the actor network: ordering, strategy and heterogeneity. *Systems Practice* 5: 379-93

Loader BD, Dutton WH. 2005. *Information, Communication & Society* 8(1): 5-199

Lyon D. 1994. *The Electronic Eye*. Minneapolis: Univ. of Minnesota

Lyon D. 2003a. *Surveillance after September 11th*. Cambridge, UK: Polity

Lyon D, ed. 2003b. *Surveillance as Social Sorting*. New York: Routledge

Lyon D, ed. 2006. *Theorizing Surveillance*. Devon, UK: Willan

Lyon D. 2007. *Surveillance Studies*. London: Polity

Mack A. 2001. Privacy. *Social Research* 68: 1-333

Mair G. 2006. Electronic monitoring, effectiveness, and public policy. *Criminology & Public Policy* 5(1): 57-108

Mann S, Nolan J, Wellman B. 2003. Sousveillance. *Surveillance and Society* 1(3): 331-55

Margulis S. 2003. Privacy as a social issue and behavioral concept. *Journal of Social Issues* 51(2): 243-453

Marx GT. 1985. The surveillance society. *The Futurist* 19(3)

Marx, GT. 1995. "Undercover in comparative perspective: some implications for knowledge and social research. In *Undercover: Police Surveillance in Comparative Perspective* ed. Fijnaut C, Marx GT. Norwell, MA: Kluwer

Marx GT. 1996. Electric eye in the sky: some reflections on the new surveillance and popular culture. In *Computers, Surveillance, and Privacy*, ed. D Lyon, E Zureik, 193-236. Minneapolis: Univ. of Minnesota

Marx GT. 1999. Ethics for the new surveillance. In *Visions of Privacy: Policy Choices for the Digital Age*, ed. C Bennett, R Grant. Toronto: Univ. of Toronto

Marx GT. 2001. Murky conceptual waters: the public and the private. *Ethics and Information Technology* 3(3)

Marx GT. 2002. Essays and commentaries on technology, surveillance, and gender. *Sociological Quarterly* 34(3): 407-78

Marx GT. 2003. A tack in the shoe: neutralizing and resisting the new surveillance. *Journal of Social Issues* 59(2): 369-90

Marx GT. 2004. What's new about the "new surveillance?" *Surveillance and Society* 1(1): 9-29

Marx GT. 2005a. Seeing hazily (but not darkly) through the lens: some recent empirical studies of surveillance technologies. *Law and Social Inquiry* 30: 339-99

Marx GT. 2005b . Some conceptual issues in the study of borders. In *Global Surveillance and Policing*, ed. Zureik E, Salter M. Portland: Willan

Marx GT. 2006. Varieties of personal information as influences on attitudes toward surveillance. In *The New Politics of Surveillance and Visibility*, ed. K Haggerty, R Ericson. Toronto: Univ. of Toronto

Marx GT. 2007. Privacy and equality. In *Encyclopedia of Privacy*, ed. W Staples. Westport, CT: Greenwood

Marx GT. Forthcoming. *Windows into the Soul: Surveillance and Society in Age of High Technology.* Chicago: Univ. of Chicago

Marx GT, Wood J. 1975. Strands of theory and research in collective behavior. *Annual Review of Sociology* 1: 363-428

Mathiessen T. 1997. The viewer society. *Theoretical Criminology* 1: 215-34

Maxwell R. 2005. Surveillance: work, myth, and policy. *Social Text* 23(2): 1-19

McCahill M. 2002. *The Surveillance Web*. Devon, UK: Willan

McGrath J. 2003. *Loving Big Brother*. Oxford: Routledge

Minow M, Lipinski T. 2003 *Library's Legal Answer Book.* Chicago: American Library Assoc.

Miller A. 1971. *The Assault on Privacy*. Ann Arbor, MI: Univ. of Michigan

Mirabal B. 2006. Homicides among children and young adults-Puerto Rico, 1999-2003. *JAMA: Journal of the American Medical Association 296*(5): 510-1

Mitchell W. 2003. *Me++: The Cyborg Self and the Networked City*. Cambridge, MA: MIT

Monahan T, ed. 2006. *Surveillance and Security*. New York: Routledge

Monmonier M. 2004. *Spying with Maps*. Chicago: Univ. of Chicago

Mumford L. 1934. *Technics and Civilization*. New York: Harcourt & Brace

National Research Council. 2007. *Engaging Privacy and Information Technology in a Digital Age*. Washington, DC: National Academies

Negroponte N. 1995. *Being Digital*. New York: Knopf

Nelkin D, Tancredi L. 1994. *The Social Power of Biological Information*. Chicago: Univ. of Chicago

Neppert-Eng C. 1996. *Home and Work: Negotiating Boundaries through Everyday Life.* Chicago: University of Chicago Press.

Newburn T, Hayman S. 2002. *Policing, Surveillance and Social Control*. Portland: Willan

Neyland D. 2006. *Privacy, Surveillance, and Public Trust*. New York: Palgrave Macmillan

Nissenbaum H. 2004. The meaning of anonymity in an information age. In *Readings in Cyberethics*, ed. RA Spinello, HT Tavani. Sudbury, MA: Jones & Bartlett

Nissenbaum H, Price M, ed. 2004. *Academy & the Internet*. New York: Peter Lang

Noam EM. 1997. Privacy and self-regulation: markets for electronic privacy. Retrieved January 12, 2007 from the World Wide Web: http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#lB

Nock S. 1993. *The Costs of Privacy Surveillance: Surveillance and Reputation in America.* New York: Aldine de Gruyter

Nogala D. 1995. The future role of technology in policing. In *Comparisons in Policing: An International Perspective*, 1st ed*,* ed. JP Brodeur, 191-210. Avebury, UK: Aldershot

Norris C, Armstrong G. 1999. *Maximum Surveillance Society*. New York: Berg

Norris C, Moran J, Armstrong G. 1998. *Surveillance, Closed Circuit Television, and Social Control*. Aldershot, UK: Ashgate

O'Harrow R. 2005. *No Place to Hide*. New York: Free Press

Paik L. 2006. Organizational interpretations of drug test results. *Law and Society Review* 40(4): 931-62

Palidda S. 1992. L'amamorphose de l'etat-nation. *Cahiers Internationaux de Sociologie* 43: 269-98

Parenti C. 2003. *The Soft Cage*. New York: Basic

Patillo M, Weiman D, Western B, ed. 2004. *Imprisoning America: The Social Effects of Mass Incarceration.* New York: Russell Sage Foundation.

Pecora V. 2002. The culture of surveillance. *Qualitative Sociology* 25(3)

Penna S. 2005. The Children Act 2004: Child protection and social surveillance. *Journal of Social Welfare* 27(2): 143-57

Phillips D. 2006. Cyberstudies and the politics of visibility. In *Critical Cyberstudies Trends in Digital Media and Culture*, ed. D Silver. New York: NYU

Poster M. 1990. *The Mode of Information*. Chicago: Univ. of Chicago

Prosser W. 1960. Privacy. *California Law Journal* 48(2): 383-423

Regan P. 1995. *Legislating Privacy*. Chapel Hill: Univ. of North Carolina

Robinson WS. 1950. Ecological correlations and the behavior of individuals. *American Sociological Review* 15(3): 351-7

Rosen J. 2004. *The Naked Crowd: Reclaiming Security and Freedom*. New York: Random House

Rule J. 1974. *Private Lives and Public Surveillance*. London: Allen Lane

Rushkoff D. 1999. *Playing the Future: What We Can Learn from Digital Kids*. New York: Riverhead

Schoenman F, ed. 1984. *Philosophical Dimensions of Privacy*. Cambridge, UK: Cambridge Univ.

Sewell G, Barker J. 2006. Coercison versus care: using irony to make sense of organizational surveillance. *Academy of Management Review* 31(4): 934-61

Sharpe S. 2000. *Search and Surveillance*. Aldershot, UK: Ashgate

Shearing CD, Stenning PC, ed. 1986. *Private Policing*. Beverly Hills, CA: Sage

Slobogin C. 2002. Public privacy: camera surveillance of public places and the right to anonymity. *Mississippi Law Journal* 72: 213-98

Smith RE. 2002. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal.

Social Text. 2005. 23(2): 1-153

Solove D, Rotenberg M, Schwartz P. 2006. *Privacy, Information, and Technology*. New York: Aspen

Staples W. 2000. *Everyday Surveillance*. Lanham, MD: Rowan & Littlefield

Staples W, ed. 2007. *Encyclopedia of Privacy.* Westport, CT: Greenwood

Stephens M. 2005. Surveillance through care and control: the case of the mentally ill in Madison and Britain. *Internet Journal of Criminology*. Web accessed 2/06/07: http://www.internetjournalofcriminology.com/Stephens - Surveillance Through Care and Control.pdf

Stigler G. 1980. Introduction to privacy in economics and politics. *Journal of Legal Studies* 9(4): 623-44

Stone Romero E, Stone D, Hyatt D. 2003. Personnel selection procedures and invasions of privacy. *Journal of Social Issues* 59(2): 343-68

Sykes C. 1999. *The End of Privacy*. New York: St. Martin's

Thiessen T, ed. 2002. *Denver University Law Review* 79(4): 513-98

Timmermans S, Gabe J. 2002. Introduction: connecting criminology and sociology of health and illness. *Sociology of Health & Illness* 24(5): 501-16

Torpey J. 2007. Through thick and thin: surveillance after 9/11. *Contemporary Sociology* 35(2)

Tunnell K. 2004. *Pissing on Demand*. New York: New York Univ.

Turkington R, Allen A. 2002. *Privacy Law*, 2nd Ed. St. Paul, MN: West Group

University of Ottawa Law and Technology Journal. 2006. 3(1): 1-327

van Harten D, van Est R. 2003. Privacy in an information society. *Journal of Contingencies & Crisis Management* 11(1)

Varon J. 2004. *Bringing the War Home: The Weather Underground, the Red Army Faction, and Revolutionary Violence in the Sixties and Seventies.* Berkeley: Univ. of California

Waever O. 1995. Securitization and desecuritization. In *On Security*, ed. R. Lipschultz. New York: Columbia Univ.

Warren S, Brandeis L. 1890. The right to privacy. *Harvard Law Review* 4(5): 193-220

Webb L, McCaughtray N, MacDonald D. 2004. Surveillance as a technique of power in physical education. *Sport Education and Society* 9(2): 207-22

Weckert J, ed. 2005. *Electronic Monitoring in the Workplace: Controversies and Solutions.* Hershey, PA: Idea Group

Welsh BC, Farrington DP. 2004. Surveillance for crime prevention in public space: results and policy choices in Britain and America. *Criminology & Public Policy* 3(3): 497-525

Westin A. 1967. *Privacy and Freedom*. New York: Columbia Univ.

Wise JM. 2004. An immense and unexpected field of action. *Cultural Studies* 18(2/3): 424-42

Wood D, ed. 2006. *A Report on the Surveillance Society*. UK: Surveillance Studies Network

Wood J, DuPont B, ed. 2006. *Democracy, Society and the Governance of Security.* New York: Cambridge Univ.

Wright D, Gutwirth S, Friedewald M, Vildjiounaite E, Punie Y. 2007. *Safeguards in a World of Ambient Intelligence.* Berlin: Springer

Zureik E, Salter M, ed. 2005. *Global Surveillance and Policing*. Portland: Willan

Table 1: Academic Use of "Surveillance" and "Privacy" as Article Keywords, 1950-Present

Database	Soc. Abstracts *		Legal Collection **		Comm. and Mass Media Complete ***	
Time Period	Surveillance	Privacy	Surveillance	Privacy	Surveillance	Privacy
2000s	519	341	61	324	124	272
1990s	563	612	21	155	40	196
1980s	151	452	3	58	14	110
1970s	79	334	5	33	9	39
1960s	6	74	2	12	4	18
1950s	n/a	n/a	n/a	n/a	1	6

Notes: * Search of Sociological Abstracts was limited to refereed journals published 1963-2005. ** Search of Legal Collection was limited to refereed journals, and covers the period 1965-2005. *** Search of Communication and Mass Media was limited to refereed journals 1950-2005.

Table 2: Elements of a Sociology of Information

1) operationally defines and keeps distinct (yet notes relations among) a family of concepts encompassing personal information—e.g., privacy and publicity, public and private, personal and impersonal data, surveillance and surveillance neutralization, secrecy, confidentiality, anonymity, pseudo-anonymity, identifiability, and confessions

2) identifies the characteristics of the data gathering technique –both those inherent and socially determined by policy and practices.

3) identifies the stated goals and latent consequences

4) identifies norms, role relationships and other social structural aspects including types of borders and directional flows and content of information and information accessibility (reciprocity and symmetry)

5) identifies spatial and locational aspects

6) identifies the type of personal information involved

7) identifies the form of the data

8) identifies cultural themes and symbols which provide meaning and direction in telling us why surveillance is needed, or is itself the problem, and how we should experience it as both watcher and watched

9) identifies the social process aspects

Table 3: Illustrative Hypotheses

In contexts where monitors have local knowledge, individual rather than categorical targeting is more likely than in contexts where such knowledge is lacking (McCahill 2002).

Individuals are most likely to feel the collection of personal information is wrong when it occurs involuntarily and without consent and when it crosses a border –whether personal, social, temporal or spatial that is presumed to be protective of information (Marx 1999).

In employment contexts perceptions of inappropriate personal border crossings will be related to tactics that probe mind and body, communicate distrust, and where validity is questioned (Stone-Romero and Stone 2003).

As surveillance practices become widespread, information displaces evidence in adjudication processes (Sharpe 2000).

The more generous a system of exchange (information in return for something the individual wants) the more likely it is to be tolerated (Gilliom 2001).

Surveillance practices bringing new goals are more likely to be questioned than those merely involving new means to meet established goals (Newburn and Hayman 2002).

The greater the restrictions on overt means of interrogation and search the greater the use of soft and covert means. (Marx 1988)

As the competitiveness of an environment and/or the perception of risk increase, mandatory flows of information from subordinates to superordinantes increase, and flows of data in the other direction decrease.

The development of non-labor intensive surveillance means is likely to lead to an increase (not a decrease) in employment in the surveillance sector of the economy

New means of identifying unique individuals (e.g., by DNA, face or walk) will lead to the creation of new data bases covering entire populations such that the distinctive individual can be found by name and likely location.

In the U.S. relative to Europe with respect to regulation, greater emphasis is placed on the specific characteristics of a technology and the risks and rewards the subject is willing to assume. In Europe greater emphasis is given to broad principles regarding the dignity of the person –apart from the characteristics of the technique and the will of the subject.

In the United States there is greater concern over government than private sector surveillance and there is greater opposition to providing personal information to government than to the private sector, while in Europe this is reversed.

In the U.S. relative to Europe there is a greater expectation of data flows from government to citizens, and this is reversed in Europe.

Nations with adversarial systems and strong judicial review will be more tolerant of invasive surveillance than nations without these.