*The Communication Review*, 10: 367–389, 2007

ISSN 1071-4421 print / 1547-7487 online
DOI: 10.1080/10714420701715456



# "WAR ROOMS" OF THE STREET: SURVEILLANCE PRACTICES IN TRANSPORTATION CONTROL CENTERS

**Torin Monahan**

Arizona State University, School of Justice & Social Inquiry

*This article investigates the surveillance dimensions of "intelligent transportation systems" in the United States, with a particular focus on the mediation of data by engineers in transportation control centers. These communication systems lend themselves to surveillance by means of "function creep" beyond their primary intended purposes and through the everyday collection and manipulation of data to manage mobilities. In the U.S., dominant system protocols privilege vehicular throughput and discipline those who deviate from that norm.*

Concerns over new surveillance technologies and security policies tend to focus on the most obvious systems or flagrant privacy breaches. These can include the proliferation of closed circuit television (CCTV) systems in urban areas, illegal government wiretapping programs, or liberal data sharing among private industries and government agencies. All the while, the rapid proliferation of digital technologies throughout everyday life creates affordances for surveillance capabilities that resist critical investigation or public awareness (Phillips, 2005; Gandy, 2006; Monahan, 2006c; Andrejevic, 2007; Lyon, 2007). This is true because of the ubiquity of the technologies, because their primary intended functions are not typically construed as being surveillance, and because the technologies are often embedded in infrastructures and thereby hidden from view (cf. Bowker & Star, 1999). Transportation infrastructures offer a case in

This material is based upon work supported by the National Science Foundation under grant no. SES 0423672. Special thanks to my research assistant, Jennifer Murray, for assisting with interviews and to David Murakami Wood and James Rule for providing helpful comments on an earlier draft of this article. I am additionally indebted to Shoshana Magnet and Kelly Gates for their support.

Address correspondence to Torin Monahan, Arizona State University, School of Justice & Social Inquiry, P.O. Box 870403, Tempe, AZ 85287-0403. E-mail: torin.monahan@asu.edu

point. Transportation flows are increasingly monitored and controlled with systems of diverse technologies, yet it is difficult to envision the data generated by traveling; how others might be interpreting, sharing, and responding to those data; and how mobilities or experiences might be altered based upon individual or automated reactions to those data.

In this article, I investigate the surveillance dimensions of "intelligent transportation systems" (ITS) in the United States, with a particular focus on the mediation of data by engineers in transportation control centers. Intelligent transportation systems are being—or have been—deployed, in some fashion, in most major cities around the world. A great deal of attention has been given to the rationalizing of transportation and tracking of passengers for purposes of efficiency, security, and commercial marketing (U.S. Department of Transportation, 1998; Accent Marketing and Research, 2004; BBC News, 2006). Especially for public transportation, global positioning systems (GPS) and "smart card" systems can be used to track the exact location of—and identity of each person on—trains and buses (Cameron, 2006). Similarly, radio frequency identification (RFID)-embedded smart cards allow for automated electronic toll collection for the use of highways and bridges (Reiman, 1995; Bennett, Raab, & Regan, 2003). License-plate recognition systems are deployed to minimize traffic congestion by limiting entry into cities (such as London) and assessing fines if entry time restrictions are violated (Glancy, 2004; Dodge & Kitchin, 2006). In-car systems such as black boxes, GPS units, or vehicle-to-vehicle communication technologies also open drivers up to increased scrutiny by insurance companies, marketers, rental car agencies, law enforcement, and potentially others (Vahidi & Eskandarian, 2003; Hay & Packer, 2004). Obviously, significant national and regional variation exists with ITS. It appears likely that the U.S. is prioritizing ITS for highways, roads, and bridges to maximize the throughput of vehicular traffic instead of—or as a supplement to—building additional roads or lanes, whereas other countries are prioritizing ITS for public transportation systems that have been operational for decades if not longer. The concentration in this article will be on publicly operated highway and road-based ITS in the U.S., and especially on the human mediation of these systems by control room operators in the southwestern U.S., where empirical research was conducted.

## *THEORETICAL ORIENTATION*

Transportation resonates as both a means of and powerful metaphor for communication. As James Carey (1992) explains, prior to electronic communication, transportation served as the dominant mode for facilitating communication through the physical delivery of messages. As a metaphor, this transmission model of communication persists in the public

imaginary and in much scholarship because of the ways in which it has been discursively conjoined with techno-scientific rationalities of progress, control, and efficiency. Additionally, the conquering of space and time made possible by both transportation and electronic communication is part of the mythology of the frontier; it is a mythology that privileges "enlightened," technological solutions to spatial and social problems, but often treats any concomitant externalities as mere unanticipated consequences or systems noise (Winner, 1977; Nye, 1996). As a partial corrective to this overreliance on transportation or transmission metaphors of communication, Carey (1992) encourages scholars to delve into the ritualistic sides of communication, to the analysis of symbols and everyday meaning-making practices in specific cultural contexts. Strange things happen, of course, with the artificial dichotomization of transmission and ritual, not the least of which is the eliding of conflict, power, and social exclusion, along with the troubling essentialization of communication rituals. Nonetheless, attention to the meaning-making practices and specific uses of communication systems is crucial to developing a deep understanding of emergent technological systems such as ITS.

The field of science and technology studies (STS) offers a complementary orientation for analyzing technological systems in their social and historical contexts. A starting premise is to understand technological systems as socially constructed. Rather than evolving in some unidirectional or predetermined way, technological systems are the result of complex negotiations among human actors, nonhuman "actants," and social institutions (Hughes, 1987; Law, 1987; Latour, 1992). They are shaped by technical and institutional constraints, inscribed with the dominant values of their origins, and modified by and given meaning through practice (Noble, 1977; Pfaffenberger, 1992; Eglash et al., 2004). In short, technologies are thoroughly social and contingent creations that acquire tenacity through their institutionalization and interlinking with other systems (Monahan, 2005). A second STS premise of relevance to the discussion of ITS is that of the "politics of artifacts." Langdon Winner (1986) coined this phrase to highlight the regulatory functions of technological systems, which exert (oftentimes silent, normalized, and unequal) control over people. Lawrence Lessig (1999) can be seen as offering a corollary argument with his compelling equation of computer "codes" with "laws" in his discussion of the constraints placed upon Internet activities. Although the idea that technologies embody values and control human behavior in nonneutral—or even discriminatory—ways strikes some STS scholars as being deterministic (e.g., Woolgar, 1991; Pinch, 1996; Joerges, 1999), urban studies researchers and philosophers (e.g., Jacobs, 1961; Lynch, 1984; Lefebvre, 1991) have long recognized the power of the built world over human action, be it intentional or accidental.

Concerning issues of mobility, communication scholars, geographers, and others have begun the project of theorizing transportation in general—and ITS in particular—as systems of governance and control. Jeremy Packer (2006a, 2006b) is one of the communication scholars at the forefront of this drive, showing how in the name of efficiency and safety, especially in the post-9/11 environment, the autonomy of the driver is increasingly delegated to automated systems, thereby reconstituting automobile individuals as controllable units whose threat to themselves and others must be minimized. Other scholars have laid the foundation for this type of analysis by calling attention to the increasing informatization and automated regulation of spaces and practices (e.g., Castells, 1996; Graham, 1998; Lianos & Douglas, 2000; Thrift & French, 2002; Hommels, 2005; Murakami Wood & Graham, 2006). Although surveillance is central to this project of vehicle and body control, the emphasis in recent scholarship is upon new articulations of governmentality, upon the automated management of resources and risks, rather than upon any overt form of disciplinary intervention (Hay & Packer, 2004; Dodge & Kitchin, 2006; Sheller, 2007).

## *ITS OVERVIEW*

A heterogeneous network of technologies comprises ITS for highways and roads: video cameras, embedded or mounted traffic sensors, smart cards, smart card readers, GPS devices, license-plate readers, geographic information systems (GIS), computers, software, communications equipment, fiberoptic networks, wireless networks, electrical supplies, traffic signals, emergency vehicle detection devices, and so on. The most visible public interfaces for ITS are traffic signals, which regulate the flow of motorized vehicles, bicycles, and pedestrians on streets; "dynamic message signs," which can alert drivers to upcoming road conditions; and ramp meters, which regulate the flow of vehicles onto highways. Perhaps the most important ITS interfaces, however, are the one hidden from public view: traffic control centers, which monitor and respond to traffic conditions through remote manipulation of the system (and its data) as a whole. The hallmarks of these control centers are their impressive and oftentimes massive "video walls," which display road conditions in real-time, whether through a graphic representation of roads and signals, CCTV video feeds, or some combination of both (see Figure 1).

Typically speaking, departments of transportation for states, as well as for large cities, possess the most advanced ITS. In the U.S., a nationwide ITS program was established by the Intermodal Surface Transportation Efficiency Act of 1991 (U.S. DOT, 2006) and the government has invested over $1 billion in the systems over the past decade (Hay &

**Figure 1. ITS Video Wall for State Department of Transportation**

Packer, 2004). Although ITS is managed by the U.S. Department of Transportation, states and cities draw upon the ITS mission and protocols to implement their own systems, relying largely upon local resources to keep systems operational. For the region studied here, sensors are embedded every one-third of a mile on highways and are used to measure speed, volume, and density of traffic. Other nonvisual sensing systems include both sonar and radar detectors to fine-tune speed and volume readings. Installed every mile on the highways are high-end CCTV cameras equipped with pan, tilt, and zoom capabilities with a minimum range of half a mile. Local municipalities off of the highway system have less-developed but nonetheless impressive systems for their roads. These include sensors mounted at intersections for the detection of flow, speed, and density for each lane; sensors for the detection of emergency vehicle strobe lights, which when triggered will change traffic signals to give emergency vehicles "green" lights; and CCTV cameras at many, but definitely not all, intersections. The local ITS centers also receive information from the traffic signals throughout their cities and can alter signal times remotely and detect (and oftentimes fix) malfunctions. Finally, ITS operators at both the state and local levels routinely spot accidents and/or verify

accident locations reported by others and then convey that information to public safety and emergency personnel. It is important to note, especially for the discussion of surveillance to follow, that almost all these systems are interoperable and interconnected. Thus, not only can local and state ITS operators monitor and control each other's systems, which they do frequently, but so can law enforcement agencies tap into these systems and their data at will.

The key to ITS is the translation of transportation flows into data that can be acted upon, preferably in real-time or in advance, through predictive modeling. The systems in the U.S. are currently geared toward the management of aggregate flows: to time traffic signals for optimal vehicular throughput or to update traffic signs to let drivers know of alternate routes for avoiding congestion or accidents, for example. As with other forms of mobile communication (Lyon, 2006), the technological trajectory, however, is toward the atomization of aggregate flows: to monitor individual vehicles with road sensors, GPS, RFID tags, license-plate readers, and so on (Cameron, 2006; Dodge & Kitchin, 2006).

Although ITS officials draw clear lines of demarcation between the functions of their systems and those of law enforcement, as this article will show, in practice these lines are quite blurred and likely the functions will continue to converge. Mainly, the systems are interlinked and accessible by personnel beyond the specific control center with jurisdiction, whether for traffic control or public safety purposes. Some operators also relate stories of listening to police radios while performing their traffic-management duties and assisting police officers in locating suspects. Finally, many ITS centers have been slated as "emergency operations centers" to manage evacuation procedures or coordinate response teams in the event of terrorist attacks or natural disasters. The systems are always, if latently, oriented toward national security, such that the operators routinely monitor "critical infrastructure," such as bridges and tunnels, for suspicious activity (White House, 2003).

The lines between the functions and interests of private industry and public agencies, on the other hand, are much less clear, even in principle. This is so because public-private "partnerships" are integral to the official ITS mission, whereby private companies are contracted to install and service equipment or to implement and manage entire subsystems, such as electronic oll collection (Bennett et al., 2003). Increasingly, state governments are selling to private companies the management rights for public highways that since their inception have been seen as essential public goods. Indiana, for instance, recently sold operating rights to all 157 miles of its primary interstate highway (I-90) to a consortium of foreign construction companies for $3.8 billion (Schulman & Ridgeway, 2007). The consortium stands to gain $11 billion in toll revenues over the 75-year life

of the contract (Schulman & Ridgeway, 2007). Many other states and countries are following suite and embracing this neoliberal rationality, which is so clearly articulated by Indiana's governor, Mitch Daniels: "any businessperson will recognize our decision here as the freeing of trapped value from an underperforming asset, to be redeployed into a better use with higher returns" (cited in Schulman & Ridgeway, 2007, p. 52). With some of the management duties and individual transportation data in the hands of industry, privacy concerns may be amplified because companies have an interest in using or selling those data for the marketing of products and services (Regan, 1995; Zimmer, 2007).[1] Less obviously, social inequalities may be aggravated as companies restrict access to public highways through tiered toll-payment schemes or build private highways that are inaccessible to the general public, thereby constraining the mobility of the poor who cannot afford the added expense but often need to travel farther to work than do the relatively affluent (Press, 2000; Graham & Marvin, 2001; Patton, 2004).

Similarly, the management of abstract flows by ITS operates as a type of surveillance with unequal effects on the ground. I understand surveillance to be practices of identification, tracking, monitoring, or analysis that enforce degrees of social control.[2] The acknowledged goal of ITS operators is to collect and analyze data to manage transportation flows, or to manage the mobilities of others. The privacy of those individuals may not be at risk, as such, but they are nonetheless subjected to surveillance and their actions are influenced by it. This mode of surveillance may be more controlling than others because of its relative invisibility, as it is embedded in infrastructure and managed remotely, increasingly by automated computer software (Lianos & Douglas, 2000; Thrift & French, 2002; Murakami Wood & Graham, 2006). Furthermore, this surveillance may be more insidious because it is not seen as such by ITS operators; they perceive the systems as neutral even as the systems actively abstract complex social practices into discrete data for impersonal intervention.

Nonetheless, ITS and its operators engage in activities of social sorting (Lyon, 2007), valorizing certain mobilities over others, while normalizing unequal experiences of space. The control made possible with ITS should be seen as part of a larger transformation in the regulation of mobilities, spaces, and spatial experiences, from ideals of universal access to experiences of differential access based largely on socio-economic status (Caldeira, 2000; Low, 2003; Monahan, 2006a; Sheller & Urry, 2006; Adey, 2006). The dominant rationality of "flow" pervades the discourse and practice of ITS operators and infuses the systems with certain politics, which are enforced and felt on the level of bodies and materialities, even if they do not achieve representation in the systems.

## METHODOLOGY

It is tempting to base one's analysis of ITS solely upon provocative industry reports, advertising campaigns, media proclamations, and political rhetoric about the highway systems of the future. No matter how critical one is of this content, however, the risk of relying on such intentionally produced documents is that the field of analysis will be circumscribed by the content available and that the hegemony of automobility will remain unchallenged. Put differently, there are many analytic blind spots in the media sources propelling ITS "solutions," so one needs to search for difference and disconnection in order to avoid reifying the automobile, the driver, or the process of automation as the primary units of analysis.

For example, ITS systems clearly operate (or can operate) as surveillance infrastructures, but they and their surveillance functions must be understood through social practices—or what James Carey (1992) might call communication "rituals." How such systems are designed, interpreted, and acted upon matters. Whereas the tendency in existing scholarship on social practices and software automation is to project the most extreme possible cases of control decoupled from human mediation and then to theorize the social or ethical implications of such automated worlds (e.g., Lianos & Douglas, 2000), this approach flirts too dangerously with technological determinism and may overlook, as a result, ever present degrees of human agency, whether in the design, use, navigation, or appropriation of such systems.

As a partial—and admittedly incomplete—corrective, this article draws primarily upon qualitative methods of ethnographic observation and interviews at ITS traffic control centers, attending to what traffic engineers do and say. This research was conducted from 2004–2005 in the southwestern United States. In addition to observational site visits and interviews, I reviewed government documents and industry reports on ITS goals and effectiveness. For the observational component, I made four site visits to city and state departments of transportation, where I observed demonstrations of street monitoring systems designed for the optimization of traffic flows. Traffic engineers or administrators walked me through the functions of their systems, showing me the systems' capabilities and limitations and relating to me their own—and others'—involvement in the monitoring processes. At every site, I took photographs of their elaborate video walls, computers, rooms for servers and routers (i.e., the hardware for receiving, sending, and processing data), and the monitoring facilities or spaces where they conduct their work. This served as an important data-collection method because it encouraged informants to relate candid stories to me about the development of the systems and the multiple uses to which the systems have been, or could be, put.

Eighteen semi-structured interviews were conducted, usually with small groups of traffic engineers or administrators each time. Interviewing people in groups instead of individually turned out to be propitious for data collection because in every case at least one person was extremely cautious and reserved, while another person was loquacious and candid, telling me stories that he—all of the operators were men—found to be of interest. This revealed both points of tension among interviewees and obvious negotiations of discourse, or of the "facts" that they wanted me to have. The second reason that interviewing more than one person at a time was especially effective was because it allowed interviewees to cue each other for stories that they thought I should know about, whereby they helped each other construct the narrative without too much prodding on my part. The average length for each interview was 90 minutes. The questions were crafted to elicit information about the uses of the systems, the management and cost of them, the potentials they envisioned for them, and the social contexts that might be affected by them.

Government documents and industry reports were reviewed to gain an understanding of the long-term objectives for ITS, the systems' development over time, the degree to which the systems were thought to be meeting those objectives, and the myriad technologies and processes that comprise ITS. It was especially helpful for this research project to perceive how certain assumptions about the problems of transportation (e.g., insufficient vehicular throughput) were codified in the official mission for ITS and then reproduced by the systems and their operators. Also interesting were the discrepancies between ITS documents, which do occasionally advocate for holistic (or even multimodal) solutions to transportation problems, and the dominant uses of ITS in the U.S., which prioritize the flow of cars and trucks over any public transportation option. The review of documents and reports provided essential background information for conducting site visits and interviews.

## *CULTURE OF SECRECY*

It is more difficult than one might expect to obtain access to ITS control centers. Whereas news media occasionally run stories about control centers,[3] otherwise a culture of secrecy predominates. In most cases, operators or administrative personnel would speak with me or my research assistant when we first called but would quickly clam up when they discovered that we wanted to visit the control rooms and interview them. Many centers refused to return our phone calls or respond to our e-mails after the initial contact. Several sites agreed to participate in the research and then had a change of heart after talking with their "legal departments." The sites to which we did get access strung us along for some

time while obtaining approval from their supervisors or legal staff. Given that these are publicly funded programs, the sites are in public buildings, the operators are government employees, and the researcher possessed some cultural credibility as a professor at a large public university, the obstacles to learning about ITS were inordinately high. Part of that may have to do with concerns over having insufficient time for an interview or the general "firewall culture" of government employees trying to avoid unnecessary scrutiny (Monahan, 2005, p. 151–154). It soon became apparent, however, that ITS operators knew that their centers had the look of surveillance and that they wanted to distance themselves from that characterization of their work.

Upon arriving at one city department of transportation, an engineer escorted me quickly to a small, drab conference room where another operator met with us for the scheduled interview. While my escort went to check the conference room schedule for any conflicts, I asked the other engineer if we would have time to see the control center as well, the sophistication of which I had heard about from engineers at another nearby city. He nervously vacillated, saying that things were probably too busy today, but that maybe I could view it through the glass of a secure door before I left. At that moment, the other person returned and informed us that there was a scheduling conflict in the conference room, so we would have to conduct the interview in the control room after all. The vast control center – referred to as the "war room" by the engineers—boasted the largest video wall I had seen apart from those at state-level DOT centers, which can be as large as movie screens. As we sat at the elegant control desk, with its embedded, flip-up monitors, another engineer emerged from a connected back office and joined the interview. Throughout the interview, one portion of the video wall displayed my interviewees and me sitting at the desk, while other portions displayed a map of the city's roads, CCTV feeds, computer video displays, and "Fox News" (see Figure 2).

Before the interview could begin, however, I needed to convince the engineers to sign informed consent forms, which were required for this project by my university's institutional review board for human subjects research. They were reluctant to sign because the forms indicated that I was conducting research on public surveillance systems. Even though government documents on ITS devote pages to describing the sensing and CCTV technologies as "surveillance" (U.S. DOT, 1998), the operators of the systems were loathe to see their technical work in that light. For them, surveillance implied the intention to monitor or spy on individuals, whereas all they cared about was rationalizing vehicular throughput in a completely disembodied and impersonal way. They did sign the forms after I explained that I was using surveillance as a generic term. Nonetheless,


**Figure 2. ITS Video Wall for Local City.**

their objections demonstrated worries about negative public attention. The objections and our discussion of them also revealed assumptions on their part that intentionality is required for "surveillance" to take place and that ITS is purely technical, not political or social in any way, and therefore should certainly not be seen as surveillance.

Because their systems rely upon CCTV cameras, which are conspicuous and increasingly ubiquitous on city streets, ITS engineers anticipate questions about privacy and have prepared software-based answers to them. As an example, when I was concluding the interview previously described, one engineer prompted one of the others saying, "You got to show him the little preset thing." It turns out that the "preset thing" was a programmed grey patch that could be applied to individual cameras so that operators could not view into people's houses or apartments. Once the software is running, if an operator zooms in too far, to the point where one might be able to view people in their private spaces, a grey box suddenly appears to block the view. The engineer explained:

> **All I care [about] is the traffic there: is it moving, is it not moving, is it backed up, is it not backed up? And one of the issues you have is, you**

> **put a camera on an intersection, and invariably people live near intersections. The biggest problem with cameras is a lot of times they'll lose power to them, they'll swing over and go to a preset, a default preset, and a lot of times it'll point right into somebody's house. Yeah and it's like aaaaah I don't wanna see that! Yeah, the camera just, the camera decided to be silly and got some capability. And a lot of the newer ones [cameras] will allow you to program a preset on them, and our newest ones will allow you to program areas that you can't even view.**

It is interesting that by switching the privacy patch off and on at will, just to demonstrate to me what "before" and "after" might look like, the engineers are tipping their hand, revealing that the software is indeed a façade. They have complete control over whether to employ it, implying that its main function is to prove to outsiders that they care about privacy, even if everyone must trust them not to take advantage of the system's privacy-violating capabilities. At the same time, it is fascinating to observe how engineers discursively recognize the unpredictable agency of the systems, whereby a camera "decided to be silly and got some capability." Because the systems have acquired some agency, their surveillance modalities must be mediated by the engineers or the systems must be further automated with corrective software patches. Related to this concern over surveillance is the mantra of all the interviewees that they do not record any video footage. Yet interviewees confessed that it was technically easy to do, if one so desired, and their digital systems are constantly "capturing" data in any event.[4] Although I completely believed the engineers that they had no interest in watching individual people, at least not as a daily practice, the systems possess vast potential for "function creep," meaning use for purposes that were not originally intended.

## *EXCEPTIONS TO THE RULE*

As ITS becomes ubiquitous, the primary rationales for the systems may shift to accommodate secondary rationales of police or security functions, or of commercial marketing. This was a point candidly acknowledged by ITS operators: "I think that what you're seeing here is an infancy of deployment of this type of equipment. I think once the equipment becomes operational and there's a lot of it, then they'll find every kind of use possible for it." Many of these potential uses are already extant. In interviews, examples of obvious cases of surveillance accumulated slowly, usually offered as anecdotal asides to the dominant message of traffic management. Although the history of communication technologies and transportation systems illustrates that the control properties of new systems have often been taken advantage of for police purposes (Hay &

Packer, 2004, p. 220), for my informants, these capabilities emerge as serendipitous discoveries. As one traffic engineer recounted:

> **I heard on the radio that somebody had assaulted a Circle K [convenience store] manager, and we had a camera at that location where we could see the Circle K. The gentleman came out of the Circle K and walked down the street and fit the description perfectly of what they were saying he was. I watched him come out and go into a bar around the corner, and the whole time I'm on the radio with the officer who responded. And I said "He's here; he's in the bar." And then he came out of the bar and got on the bus. And there was only one bus going westbound at the time. So, [the police] didn't have any problem. They pulled the bus over about a quarter mile down the road and hauled him off.**

Here, one of the same traffic engineers who initially objected vociferously to me talking about ITS as "surveillance" described in detail how he tapped into the explicit surveillance functions of the system to assist the police. Whereas this surveillance occurred through real-time processing of information and active coordination of different communication media, other publicized cases of ITS lending itself to function creep are more retrospective and data-driven, as with Great Britain's recent admission of secretly spying on people by sorting through the data generated by individuals' "smart cards," which they use to access public transportation (BBC News, 2006).

The interoperability and interconnection of systems signal another obvious avenue for function creep. When I asked operators and administrators about the logistics of verifying accident locations for public safety, they admitted that public safety personnel often simply tap into the system to control the cameras without the need for ITS engineers to get involved. In fact, the design preference for all new control centers is to combine ITS and public safety departments within the same building so that access to the systems will be identical. In interviews with police, for a related research project, they admit that they occasionally use ITS for police purposes, even if it is less precise than surveillance that they would set up for specific investigations. One detective viewed ITS video cameras as important inoculation for the American public to become desensitized to public surveillance systems that the police would like to use. Barring any technical or legal safeguards (such as encryption for privacy protection or new laws governing ITS use, respectively), secondary uses of the systems will likely continue to grow without much public awareness or oversight.

National security concerns, especially in the post-9/11 context, provide another strong rationale for secondary ITS functions. In the years

following September 11, 2001, most—if not all—U.S. government agencies have transformed their missions to prioritize national security and/or have incorporated security responsibilities (Monahan, 2006b). Departments of transportation are no exception. As might be expected, the monitoring of "critical infrastructures," such as bridges and tunnels, is part of the responsibility of many ITS control centers. Moreover, many control rooms are slated to become emergency operation centers in the event of terrorist attacks or natural disasters. As emergency operations centers, they could coordinate evacuation procedures and response teams, including police and fire departments, and possibly hazardous material teams or military units. An engineer for one city-level department of transportation center explained:

> **Right now the State has its own state emergency operation center [EOC], so, if the Governor declares a state of emergency, it is the Division of Emergency Management that handles [the Governor's] directives . . . But actually our IT department and some other parts of our city have identified this facility as being an important facility that needs to keep running in case anything happens, and we're kind of worked into that whole process. Because we do have some of the backup systems and, so there is some recognition in the value of what we do here and keeping it live and well. We've only been here a year and the EOC is just really kinda getting off the ground, and over the next few years, I can just see a lot of growth in working out all those [coordination] issues . . . Yeah, and that would be, you know, kinda again one of those Homeland Security concepts, you got your police and your fire and if anything unpleasant were to happen, they've got their secured command center [the ITS center] to dispatch the resources that are needed.**

The responsibilities for critical infrastructure monitoring and emergency operations management provide insight into the multi-dimensional character of ITS, whereby the analytic distinction between primary and secondary functions is too facile a characterization of the systems, even if it is an accurate description of the daily practices of engineers. Given the definition of surveillance offered above (as enacting forms of control), these security functions point to the inherent, and in this case intentional, surveillance capabilities of ITS.

These examples of function creep highlight to the lack of explicit protocols or collective conversations about the surveillance functions of these systems or the desirability of tapping into those functions. Instead the surveillance modalities are exploited because the systems allow them to be. The discourse of abstract control of flows at a distance illustrates an

approach to the systems that denies the existence of these alternative uses, as well as social context (Monahan, forthcoming). Nonetheless these systems, along with their discourses and practices, actively shape the world and sort bodies in very biased ways. It is to this social sorting that I next turn.

## *THROUGHPUT RATIONALITY*

Whereas the police and security applications of ITS may be the most visible instantiations of surveillance, the active management of people and their mobilities should also be considered as such. Both existing ITS and dominant throughput rationalities are coproductive and hegemonic, oftentimes to the detriment of other experiences of space or modes of transport. As one engineer put it:

> **As the *cities mature*, and the right of way is used up, we lack the ability to add more pavement, add more lanes, add more capacity to the roadway. But with the ITS Smart Technology, we're moving towards a traffic control system that will make and manage the capacity more efficiently. And so you know, when you reach build-out, you know, there's nothing else you can do, save for using the capacity, *using the pipe* way more intelligently [emphasis added].**

There are many assumptions embedded in such an articulation. First, "mature" cities are those that have reached a threshold with the number of vehicles its roads can carry and with the space available for the construction of new roads or lanes. The history of a city, its cultures, and institutions are subordinated to the development of its roadways in any evaluation of a city's evolution. Second, rather than question the automobile as the dominant form of transportation or criticize development patterns that lead to increasing distance between places of living and work, the logical solution advanced by ITS is to utilize existing infrastructures more "intelligently," meaning in a more efficient, informatized way. Finally, from this perspective, streets and highways are reduced to metaphorical "pipes," serving as conduit from one place to another, rather than as places in their own right.

Within this discursive framework, and within these "smart" infrastructures, alternative mobilities or experiences of space are often marginalized. The infrastructures themselves, once analytically reduced to "pipes," become intolerant of, or actively hostile to, difference. Of course, this is true of the history of road development more generally, especially in the U.S., but as the roads achieve greater throughput of vehicles, there is a corresponding diminishment of nonvehicular space, or gaps between

vehicles (Patton, 2004). For instance, maximum throughput makes it much more difficult to back out of a driveway on a busy street, turn onto such a street, or cross streets, especially as a pedestrian.

The ways in which ITS traffic engineers speak of pedestrians illustrates the symbolic marginalization of difference, which is informed and reproduced by the systems. First, there is a sense of frustration with pedestrians for slowing down the traffic flow—or, more precisely, for forcing engineers to slow down traffic flow to ensure that signals will be "synced"[5] in the eventuality that a pedestrian pushes the "walk" button:

> **If you have to accommodate a lot of ped time, it means the intersections are going to take a longer time to get around [i.e., for the signal lights to cycle from red to green to red], and the longer it takes an intersection to get around, typically, the slower the drive speed is, so then you end up with intersections where the speed limit's 45 miles an hour, and there's no way you can time it for that speed so you end up timing it for a lower speed.**

This concern with limiting throughput in order to accommodate pedestrians compels some engineers to take shortcuts, timing intersections for a higher vehicle speed in the hopes that few pedestrians will cross the streets and that the signals will remain synced. Invariably, this approach fails, traffic gets backed up, and the signal times need to be recalibrated. A second approach is to limit the amount of time allotted for pedestrians to cross the street, forcing them to move quickly or face increased risk of being hit. In the cities I studied, pedestrians were assumed to walk at a rate of 4 feet per second, and the signals were timed accordingly. Obviously, the handicapped, elderly, and children may not be able to achieve the necessary speed to make it across streets, some of which are up to seven lanes wide. This is one very real danger introduced by a transportation system rationalized for vehicles and destinations, rather than people and places (Jain, 2004).

A final example, this time of a pedestrian getting hit by a car, reveals the tendency of ITS surveillance to objectify people and privilege vehicles as primary units of analysis. A control room operator related:

> **Unfortunately, I watched a lady get hit by a car one day . . . A man made a right turn right in front of her, as she was walking across the street, and she literally walked into the van and got caught by it. I'm like, "how in the hell could that happen," and I was sitting here watching it the whole time, and I couldn't believe what I was watching.**

In this instance, the operator who witnessed the accident strangely elects to fault the lady for somehow walking into a moving car, rather than

saying that the person in the moving car violated the pedestrian's right-of-way by cutting across her path and hitting her. While it is common for most people to lend agency to vehicles by saying things such as "the car went through the light," when filtered through the lens of ITS, the operator takes this tendency a step further to blame the pedestrian who was in the right, at least according to the law. Given the sordid history of U.S. transportation systems and their tendency—or the tendency of engineers and planners—to divide neighborhoods, displace people, and discriminate against nondrivers in extremely racist and classist ways (Lewis, 1997; Bullard, Johnson, & Torres, 2004; Patton, 2004), ITS builds upon rather than replaces these previous biases. Similarly, the perspective of the engineer relating this story is undoubtedly shaped by the logics of the systems he oversees and his professional training. Intelligent transportation system present themselves, therefore, as a lens for perceiving the rearticulation of throughput rationalities in digital and increasingly automated forms.

In summary, as ITS is integrated into existing transportation infrastructures, it reproduces and modulates a rationality of maximum vehicular throughput at the expense of other experiences or values. It monitors and regulates flows retrospectively, in real time, and prospectively. Currently, this largely invisible and normalized form of social control occurs mostly at the level of aggregate data, but more and more it is individualized, with systems tracking and storing unique identifiers (from smart cards, GPS devices, license plates, etc.) for future scrutiny and intervention. As the examples in this article demonstrate, neither ITS nor the social orders established by it are value-neutral. They carve up the world in very particular ways according to the contexts within which they are applied, oftentimes reinforcing inequalities that are not represented by the transportation grids, flow diagrams, or software codes that define the parameters of the systems.

## *CONCLUSION*

The proliferation of digital technologies throughout everyday life enables new modalities of surveillance. Whether the technologies are mobile phones, smart cards, GPS units, or video cameras, they tend to create and store data as a default, thereby lending themselves to surveillance uses. If the key to determining whether surveillance is occurring rests in the criterion of "control," as I have asserted, then one must look to the *social practices* surrounding such systems and analyze them in *spatial context* to see how control is or is not manifested. One must also attend to how various assemblages of digital technologies become embedded in infrastructure and hidden from view, such that certain rationalities of movement or spatial experience are normalized, depoliticized, and hidden from view. In

this article, I have added to previous theorizations of ITS and software-based productions of space to highlight the surveillance dimensions of ITS, as seen through the discourse and practice of control center operators. While it is apparent that ITS performs at the level of infrastructure to control and sort people in nonneutral ways, much more empirical research needs to be done to better understand the physical and symbolic negotiations of ITS by people in other domains and across multiple mobilities.

The difficulty of obtaining information on the actual work of ITS engineers and the functions of the systems is itself revealing. Engineers understand that what they do can be perceived as surveillance, mostly because of dominant cultural meanings associated with video cameras. As a result, these government workers seek to insulate themselves from scrutiny by preventing access to their spaces. They articulate a pure, technical version of their activities (i.e., managing flows) that strips people from the equation entirely. Their implied rhetorical argument is that without people, or even representations of them beyond the unit of the car, surveillance cannot be occurring. This is true, from their viewpoint, because surveillance is perforce a social, intentional, and interested activity; what they do is technical, whereby any attention to individual people is unintentional and disinterested. This, of course, is a highly problematic distinction. Technical operations are always social and embodied practices (Haraway, 1997; Slack & Wise, 2005; Monahan & Wall, 2007). Moreover, surveillance can operate on the level of groups—or upon groups of mobilities, as the case may be—without any explicit intention or interestedness on the part of those running the systems (Fisher, 2006; Fisher & Monahan, forthcoming). Surveillance does not have to be intended to be felt.

Even if one were to accept engineers' initial description of ITS as rational traffic management, their narratives betray the polyvalence of ITS, which is also the case with all communication technologies. They proudly talk of listening to police radios and using the system to assist police with the apprehension of criminals. They admit that personnel from public safety control centers access and direct their systems at will, and while ITS engineers do not record any video footage, they cannot prevent others with access from doing so. Finally, many ITS centers serve a dual function of being emergency operations centers in the event of terrorist attacks or natural disasters. Given the fact that the interstate highway system, which ITS helps to regulate, was initially conceived of as a national security infrastructure, these security functions of ITS should not be that surprising—they are part of the historical trajectory of the U.S. highway system. On one hand, these secondary uses illustrate the function-creep potential of ITS. On the other, perhaps the differentiation between primary and secondary uses is dangerous; it may serve to inoculate such systems against critique because one could always say that any problematic

uses are not the primary or intended ones. At the very least, these few examples do signify the valence of such systems toward explicit surveillance and security applications.

The social-sorting ramifications of ITS should not be overlooked, even if they are the most difficult to perceive. The dominant rationality of efficient vehicular throughput pervades American culture as a whole, dramatically affecting experiences of mobility, space, and place (Patton, 2004; Jain, 2006). When streets are perceived as conduit from one place to another, instead of as places in their own right, the imperative for speed subordinates that of sociality, or of a sense of collective responsibility for social well-being (Demerath & Levinger, 2003). In this way, ITS can be seen as sustaining ongoing neoliberal development patterns by emphasizing "pipes" over places, maximizing the flow of privately owned vehicles through those pipes, and facilitating the privatization of highways and industry (and state) profits through tiered toll schemes and the abrogation of public rights to access. Control manifests in the unequal privileging and (infra)structural support of certain mobilities over others: private over public transportation, driving over walking or bicycling. Control also manifests in the largely invisible governing of mobilities, directing where one can go, by what means, and under what conditions. Thinking about ITS in terms of surveillance can ground it analytically, opening it up for further critical investigation and intervention.

## *NOTES*

1. Michael Zimmer (2005) expands upon the discussion of privacy threats introduced by such systems, arguing convincingly that such systems challenge the "contextual integrity" of personal data in public places.
2. It is important to note that not all surveillance should be viewed as negative. As David Lyon (2001) has argued, the control dimensions of surveillance can be interpreted as "care" or watching out for those in need, such as children, the elderly, or stranded motorists. Obviously, classifying surveillance practices along the control-care continuum is a highly subjective exercise, whereby even the most obvious examples of care-based surveillance can be viewed as paternalistic and controlling from the perspective of those scrutinized, or from the perspective of scholars studying the scrutiny, as the case may be.
3. Additionally, some news networks broadcast traffic reports from state-level ITS control centers. When they do so, they typically display CCTV feeds of traffic conditions, and not footage of the centers themselves.
4. The term *capture* is a loaded one that I use here in accordance with how the systems are described by my informants. Although it is common to refer to information systems as oriented toward data "capture" (e.g., Agre, 1994), it would be more accurate to focus on the act of data "creation" that occurs with such

systems. They restructure social practices and categories in an active way that is elided by the somewhat positivistic term *capture*.

5. The system for emergency vehicle preemption (where green lights are triggered for emergency vehicles) is perceived similarly as a threat to the synchronization of traffic signals.

## *REFERENCES*


Accent Marketing and Research. (2004). *Town Centres Survey 2003–4: Summary report*. London.

Adey, P. (2006). "Divided we move": The dromologics of airport security and surveillance. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 195–208). New York: Routledge.

Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society, 10*, 101–127.

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence, KS: University Press of Kansas.

BBC News. (2006, March 13). Oyster data is "new police tool." *BBC News*.

Bennett, C., Raab, C., & Regan, P. (2003). People and place: Patterns of individual identification within intelligent transportation systems. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk, and digital discrimination* (pp. 153–175). New York: Routledge.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

Bullard, R. D., Johnson, G. S., & Torres, A. O. (2004). *Highway robbery: Transportation racism & New routes to equity*. Cambridge, MA: South End Press.

Caldeira, T. P. R. (2000). *City of walls: Crime, segregation, and citizenship in São Paulo*. Berkeley: University of California Press.

Cameron, H. (2006). Using intelligent transport systems to track buses and passengers. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 225–241). New York: Routledge.

Carey, J. W. (1992). *Communication as culture: Essays on media and society*. New York: Routledge.

Castells, M. (1996). *The Rise of the Network Society*. Cambridge, MA: Blackwell Publishers.

Demerath, L., & Levinger, D. (2003). The social qualities of being on foot: A theoretical analysis of pedestrian activity, community, and culture. *City and Community, 2*, 217–237.

Dodge, M., & Kitchin, R. (2006). *Code, vehicles and governmentality: The automatic production of driving spaces* (No. 29). Maynooth, Ireland: NIRSA Working Papers Series, No. 29 (March).

Eglash, R., Croissant, J. L., Di Chiro, G., & Fouché, R. (2004). *Appropriating technology: Vernacular science and social power*. Minneapolis: University of Minnesota Press.

Fisher, J. A. (2006). Indoor positioning and digital management: Emerging surveillance regimes in hospitals. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 77–88). New York: Routledge.

Fisher, J. A., & Monahan, T. (forthcoming). Tracking the social dimensions of RFID systems in hospitals. *International Journal of Medical Informatics*.

Gandy, Jr., O. (2006). Data mining, surveillance, and discrimination in the post-9/11 environment. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 363–384). Toronto: University of Toronto Press.

Glancy, D. J. (2004). Whereabouts privacy. *STS Nexus*, Spring.

Graham, S. (1998). Spaces of surveillant simulation: New technologies, digital representations, and material geographies. *Environment and planning D: Society and space, 16*, 483–504.

Graham, S., & Marvin, S. (2001). *Splintering urbanism: Networked infrastructures, technological mobilities and the urban condition*. New York: Routledge.

Haraway, D. J. (1997). *Modest_witness@second_millennium.femaleman_meets_oncomouse: Feminism and technoscience*. New York: Routledge.

Hay, J., & Packer, J. (2004). Crossing the media(-n): Auto-mobility, the transported self and technologies of freedom. In N. Couldry & A. McCarthy (Eds.), *Mediaspace: Place, scale and culture in a media age* (pp. 209–232). New York: Routledge.

Hommels, A. (2005). Studying obduracy in the city: Toward a productive fusion between technology studies and urban studies. *Science, Technology, and Human Values, 30*, 323–351.

Hughes, T. P. (1987). The evolution of large technological systems. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: The MIT Press.

Jacobs, J. (1961). *The death and life of great American cities* (2002 ed.). New York: Random House.

Jain, S. (2006). Urban violence: Luxury in made space. In M. Sheller & J. Urry (Eds.), *Mobile technologies of the city* (pp. 61–76). New York: Routledge.

Jain, S. S. (2004). "Dangerous instrumentality": The bystander as subject in automobility. *Cultural Anthropology, 19*, 61–94.

Joerges, B. (1999). Do politics have artefacts? *Social Studies of Science, 29*, 411–431.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W. E. Bijker, & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 225–258). Cambridge, MA: The MIT Press.

Law, J. (1987). Technology and heterogeneous engineering: The case of Portuguese expansion. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: The MIT Press.

Lefebvre, H. (1991). *The production of space* (D. Nicholson-Smith, trans.). Cambridge, MA: Blackwell.

Lessig, L. (1999). *Code: And other laws of cyberspace*. New York: Basic Books.

Lewis, T. (1997). *Divided highways: Building the interstate highways, transforming American life*. New York: Viking.

Lianos, M., & Douglas, M. (2000). Dangerization and the end of deviance. *British Journal of Criminology, 40*, 261–278.

Low, S. M. (2003). *Behind the gates: Life, security and the pursuit of happiness in fortress America*. New York: Routledge.

Lynch, K. (1984). *Good city form*. Cambridge, MA: MIT Press.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham UK: Open University.

Lyon, D. (2006). Why where you are matters: Mundane mobilities, transparent technologies, and digital discrimination. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 209–224). New York: Routledge.

Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity Press.

Monahan, T. (2005). *Globalization, technological change, and public education*. New York: Routledge.

Monahan, T. (2006a). Electronic fortification in Phoenix: Surveillance technologies and social regulation in residential communities. *Urban Affairs Review, 42*, 169–192.

Monahan, T. (2006b). Securing the homeland: Torture, preparedness, and the right to let die. *Social Justice, 33*, 95–105.

Monahan, T. (Ed.). (2006c). *Surveillance and security: Technological politics and power in everyday life*. New York: Routledge.

Monahan, T. (forthcoming). Dreams of control at a distance: Gender, surveillance, and social control. *Cultural Studies < = > Critical Methodologies, 8*(4).

Monahan, T., & Wall, T. (2007). Somatic surveillance: Corporeal control through information networks. *Surveillance & Society, 4*, 154–173.

Murakami Wood, D., & Graham, S. (2006). Permeable boundaries in the software-sorted society: Surveillance and differentiations of mobility. In M. Sheller & J. Urry (Eds.), *Mobile technologies of the city* (pp. 177–191). New York: Routledge.

Noble, D. F. (1977). *America by design: Science, technology, and the rise of corporate capitalism*. New York: Oxford University Press.

Nye, D. (1996). *American technological sublime*. Cambridge, MA: MIT Press.

Packer, J. (2006a). Becoming bombs: Mobilizing mobility in the war of terror. *Cultural Studies, 20*, 378–399.

Packer, J. (2006b). Rethinking dependency: New relations of transportation and communication. In J. Packer & C. Robertson (Eds.), *Thinking with James Carey: Essays on communications, transportation, history*. New York: Peter Lang.

Patton, J. W. (2004). *Transportation worlds: Designing infrastructure and forms of urban life*. Unpublished doctoral dissertation, Rensselaer Polytechnic Institute, Troy, NY.

Pfaffenberger, B. (1992). Technological dramas. *Science, Technology, and Human Values, 17*, 282–312.

Phillips, D. J. (2005). From privacy to visibility. Context, identity, and power in ubiquitous computing environments. *Social Text, 23*, 95–108.

Pinch, T. (1996). The social construction of technology: A review. In R. Fox (Ed.), *Technological change: Methods and themes in the history of technology* (pp. 17–35). Amsterdam: Harwood Academic Publishers.

Press, J. E. (2000). Spatial mismatch or more of a mishmash? Multiple jeopardy and the journey to work. In L. D. Bobo, M. L. Oliver, J. H. Johnson Jr., & A. Valenzuela (Eds.), *Prismatic metropolis : Inequality in Los Angeles* (pp. 453–488). New York: Russell Sage Foundation.

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill: University of North Carolina Press.

Reiman, J. H. (1995). Driving to the panopticon: Philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara Computer and High Technology Law Journal, 11*, 27–44.

Schulman, D., & Ridgeway, J. (2007). The highwaymen. *Mother Jones, 32*, 48–55, 84.
Sheller, M. (2007). Bodies, cybercars and the mundane incorporation of automated mobilities. *Social & Cultural Geography, 8*, 175–197.
Sheller, M., & Urry, J. (2006). *Mobile technologies of the city*. New York: Routledge.
Slack, J. D., & Wise, J. M. (2005). *Culture + technology: A primer*. New York: Peter Lang.
The White House. (2003). *National strategy for the physical protection of critical infrastructures and key assets*. Washington, DC.
Thrift, N., & French, S. (2002). The automatic production of space. *Transactions of the Institute of British Geographers, 27*, 309–335.
U.S. Department of Transportation. (1998). *Developing traffic signal control systems using the national ITS architecture* (No. FHWA-JPO-98–026). Washington, DC: U.S. Department of Transportation.
U.S. Department of Transportation. (2006, November 7). Frequently Asked Questions: Intelligent Transportation Systems. http://www.its.dot.gov/faqs.htm. Last accessed January 9, 2007.
Vahidi, A., & Eskandarian, A. (2003). Research advances in intelligent collision avoidance and adaptive cruise control. *IEEE Transactions on Intelligent Transportation Systems, 4*, 143–153.
Winner, L. (1977). *Autonomous technology: Technics-out-of-control as a theme in political thought*. Cambridge, MA: MIT Press.
Winner, L. (1986). *The whale and the reactor: A search for limits in an age of high technology*. Chicago: University of Chicago Press.
Woolgar, S. (1991). The turn to technology in social studies of science. *Science, Technology, & Human Values, 16*, 20–50.
Zimmer, M. (2005). Surveillance, privacy and the ethics of vehicle safety communication technologies. *Ethics and Information Technology, 7*, 201–210.
Zimmer, M. (2007). *The quest for the perfect search engine: Values, technical design, and the flow of personal information in spheres of mobility*. Unpublished doctoral dissertation, New York University, New York.