The Communication Review, 10: 295–317, 2007

ISSN 1071-4421 print / 1547-7487 online
DOI: 10.1080/10714420701715365

Routledge
Taylor & Francis Group

SURVEILLANCE IN THE DIGITAL ENCLOSURE

Mark Andrejevic

Department of Communication Studies, The University of Iowa; and the Centre for Critical and Culture Studies, University of Queensland

Popular portrayals of ubiquitous computing downplay the surveillance implications of emerging forms of networked interactivity. This essay supplements such accounts by analyzing interactive spaces as digital enclosures which restrict access to the means of interaction to those who "freely" submit to the detailed forms of monitoring that take place within them. It supplements privacy-based critiques of surveillance with questions about the ownership and control of such data and the implications of this control for networked communication.

RECENTRALIZATION

Pronouncing the untimely death of the desktop computer in an interactive era, *Wired* magazine claimed that, "computing is moving off your machine and into the cloud" (Tanz, 2007). Thanks to Wi-Fi and other forms of always-on connectivity, the article reported, users will no longer need to store their data or even their software applications on personal computers—rather these will be relegated to the ether and conveniently accessed via an increasing range of networked devices: laptops, mobile phones, PDA's, and so on. Our portable storage devices will apparently multiply and then shrink to invisibility, as the information they store expands to fill the space through which we move. In the world of ubiquitous computing, we will dip into these invisible currents of information at will, connected by an electromagnetic umbilicus to an overarching matrix of information and communication. As the futurists at MIT put it, describing their ubiquitous computing initiative, "computation . . . will be freely available everywhere, like batteries and power sockets, or oxygen in the air we breathe" (MIT Project Oxygen, 2004).

Address correspondence to Mark Andrejevic, 105 BCSB, The University of Iowa, Iowa City, IA 52242. E-mail: mark-andrejevic@uiowa.edu

As William Gibson, famous for coining the term "cyberspace," has observed, the usefulness of the image of the internet "cloud," "lies in its vagueness, like cyberspace—a word which is also useful for its vagueness" (Holliday & Wieners, 1999). Apparently, one of the term's current uses is to obscure the very concrete shifts in control over information associated with the recentralization of information and communication resources envisioned by the architects of the internet "cloud." Consider, for example, the way in which this airy—or cloudy—rhetoric neatly elides the distinction between the "freedom" of the "oxygen we breathe" and that of electricity. Neither power nor batteries are "free" in the sense of being available to all without any consideration of the ability to pay or of access to economic resources. They both come with a charge, as it were, and so will mobile, ubiquitous, networked computing. The creation of ubiquitous "cloud" computing, which internet ideologist and conservative pundit George Gilder (2006) has described as the manifestation of a "newly recentralized computing architecture," is less a spontaneous eruption of convenience than a business model based on separating users from information and communication resources in order to restructure the terms of access to these resources.

The world envisioned by "cloud" computing is one in which users will rely on privatized communication networks and data storage facilities to access and manage an array of goods and services, from personal documents and music files to online shopping and e-mail. It is presaged by applications like Gmail and Google documents, which provide users with large amounts of storage space on Google's servers to store their personal documents and correspondence. In return for this convenience, Google reserves the right to mine its rapidly expanding databases for commercial purposes. If this business model is still in its infancy, one of its dominant emerging characteristics has become evident—a reliance on the interactive capability of networks to gather information about users. The terms of access to the "cloud" will include the capture and commodification of information about how, when, and where, we make use of its resources, a fact that renders the metaphor doubly misleading. The portrait of user activity made possible by ubiquitous interactivity will not be ephemeral, but increasingly detailed and fine-grained, thanks to an unprecedented ability to capture and store patterns of interaction, movement, transaction, and communication. Patterns of users' Web browsing, for example, could be correlated with those of online shopping, communication, and, eventually, advertising exposure. The information clouds here are far from ephemeral, fleeting forms: their details are captured and fixed in a manner that envisions a mechanical and more prosaic version of Jorge Luis Borges's fictional Funes, "who remembered the shapes of the clouds in south at dawn on the 30th of April of 1882, and . . . could compare them

in his recollection with the marbled grain in the design of a leather-bound book which he had seen only once, and with the lines in the spray which an oar raised in the Rio Negro on the eve of the battle of the Quebracho" (Borges, 1999, p. 130).

To counter the misleading image of the internet cloud, this essay proposes the model of *digital enclosure* as a way of theorizing the forms of productivity and monitoring facilitated by ubiquitous interactivity. The model of enclosure traces the relationship between a material, spatial process—the construction of networked, interactive environments—and the private expropriation of information critiqued by Schiller (2007), Boyle (2003) and Lessig (2004). Monitoring, in this context, refers specifically to the collection of information, with or without the knowledge of users, that has actual or speculative economic value. Whereas the promise of universal interactivity is portrayed by the popularizers of the rhetoric of the "digital sublime" (Mosco, 2004) at places like MIT's Media Lab and *Wired* magazine as a form of liberation—freedom from the fiber-optic fetters of the wired world—the model of digital enclosure suggests that ubiquitous interactivity also has the potential to facilitate unprecedented commodification of previously nonproprietary information and an aggressive clamp-down of centralized control over information resources.

Consider two examples of digital enclosures in action: Google's proposed business model for equipping the city of San Francisco with free wireless internet access, and the use of the interactive capability of the internet to enforce increasingly restrictive intellectual property regimes. Google and Earthlink's proposal for "free" Wi-Fi in San Francisco would be financed by the collection of information about the time-space paths of users who log on to their proprietary network. In addition to generating what Mosco (1989) calls "cybernetic commodities" (transactionally generated demographic information about user behavior), this information would allow Google to target users with so-called "contextual advertising"—ads based on their location throughout the course of the day. Google's hope is that users will be more likely to click on ads for nearby commercial outlets: "It could be the difference between seeing an advertisement for Macy's, if a user happens to be in Union Square, or a seafood restaurant if the user is near Fisherman's Wharf" (Kopytoff, 2006, p. C1). Moreover, thanks to its myriad interactive applications, the potential exists for Google to supplement its customization algorithms with information gleaned from users' search engine inquiries, their Gmail accounts, their map requests, and so on. Google has already filed a patent application that, as one account puts it, "involves a system in which targeted ads are served to wireless internet users based on the geographic location of the wireless access point (WAP), as well as the behavior and demographics of the WAP's users, and other criteria" (Telecommunications Industry

News, 2006). Behavior and demographics are, needless to say, umbrella terms wide enough to capture the expanding array of information about users that Google hopes to gather with its proliferating array of services. The creation of an interactive "enclosure"—in this case, one large enough to embrace the entire city of San Francisco—promises to be fantastically productive in terms of its ability to generate, capture, and store personal information. The proposed Wi-Fi network, combined with Google's rapidly expanding data storage and sorting capabilities, makes it possible to gather and process information previously too costly to capture and to transform it into demographic inputs for the marketing process.[1]

If proposed enclosures like Google's Wi-Fi network facilitate information gathering, they also enable unprecedented levels of centralized data control. Consider the example of a friend of mine who stumbled across the limits imposed by interactivity when he tried to play a high-definition DVD he had purchased legally in the United States and then carried halfway around the world with him to Australia. When he attempted to play the high-definition version of the DVD (one of the bonus features) on his laptop computer—which he had also brought with him from the U.S., the region for which the DVD was coded—he was greeted with a pop-up box instructing him to register online. Upon doing so, and entering the code on the DVD case as instructed, he was informed that the movie would not play because he wasn't in the appropriate region: the version he had purchased was to be played exclusively in the US. He did not have to enter his location when he logged on—the network had located him. By going online, he had entered a virtual enclosure that could pinpoint him in space and time in order to regulate his access to data that he had purchased perfectly legally thousands of miles away.

This type of control is made possible by the broadening reach of a digital enclosure that increasingly encompasses erstwhile "stand-alone" devices. If personal computers were once relatively self-contained, the architects of recentralization at places like Google, Yahoo, and Microsoft, envision a networked world in which the governing assumption will be that our machines are in constant contact with a broader network that can be used not just to access information, but to monitor its proper use. One apparent solution to the perceived threat posed by file-sharing to the movie and recording industry is not less interactivity, but *more*. When the devices we use to access content are networked, we may find not only that our consumption patterns can be digitally recorded, but that approved forms of access—such as the type of geographic limitations built into my friend's DVD—can be enforced via computer code (Lessig, 1999) rather than reliance on the goodwill of consumers. When the video iPod goes wireless and interactive by enfolding itself within the embrace of an iTunes-controlled digital enclosure, the likelihood that users will be able

to play illegally downloaded or shared movies will plummet. In the era of digital enclosure, information does not "want to be free," it (and the "it" here fetishizes the imperatives of those who control the enclosure) wants to stand and be counted. It also wants to go forth and multiply by disclosing details about itself to those with the technology to monitor, record, store, and manage the resulting metadata. A networked iPod will be able to do more than block unlicensed content, it will also be able to keep track of every detail of users' viewing preferences. Consumers will likely have only the vaguest idea of exactly how much information is being gathered about their listening habits and even less control over what Apple does with the proprietary information about individual behavior it has collected in the "privacy" of its digital enclosure.

This is not an argument about the invasive character of the technology *per se*. It is certainly possible to create networks that do not collect and store detailed information about users. Rather this is an argument about the forms of productive data gathering enabled by private ownership of and control over interactive enclosures, wired or wireless, that render an increasing array of spaces interactive. The model of enclosure highlights the ongoing importance of structures of ownership and control over productive resources in determining the role they play in what Schiller (2007) has described as "the struggle against continuing enclosures of non-proprietary information" (p. 56). The attempt to foreground questions of ownership counters the determinism of those who insist on the *inherently* empowering character of interactive networks and the revolutionary *telos* of the digital era. Such accounts run across the political spectrum from figures like Rupert Murdoch who, upon purchasing MySpace for a half billion dollars observed that, "Technology is shifting power away from the editors, the publishers, the establishment, the media elite. Now it's the people who are taking control . . ." (Reiss, 2006) to mainstream liberals like political consultant Joe Trippi ("the technology is finally here to allow people to reject what they're being given and demand what they want") (Trippi, 2004, p. 235) to left-leaning academics and artists like Celia Pearce ("The digital age introduces a new form of international socialism") (Pearce, 1997, p. 180). The rhetoric of "Third Wave," cyber-euphoric futurism invokes the promise of a silicon revolution that painlessly eliminates the inequities attendant upon the concentration of control over wealth and productive resources by economic and political elites. The key to this hypothetical revolution is not the redistribution of control over material resources, but their supposed irrelevance in an emerging information economy. In the preamble to their "Magna Carta for the Knowledge Age," for example, futurists Esther Dyson, George Gilder, and Alvin Toffler (1996), blithely proclaim that "The central event of the 20th century is the overthrow of matter" (p. 295). The

implication of course, is that resource ownership no longer matters. This triumphant idealism persists in the popular media's focus on the gee-whiz gimmickry of ubiquitous computing as well as in the hip radicalism of books like *Netocracy: The New Power Elite and Life after Capitalism* (Bard & Söderqvist, 2002), which proclaims the coming irrelevance of property rights and "ownership of the means of production" (p. 255). Against these persistent remainders of the "digital sublime," the model of digital enclosure seeks to explain why much still depends on who owns and controls the networks, who sets the terms of entry, and who gathers and sorts this information for what ends.

It is crucial, for the purposes of critiquing interactive surveillance practices and regimes of centralized control over information, to consider the physical and dynamic aspects of the notion of enclosure: to describe the construction of, for example, cellular wireless networks as expanding interactive overlays that endow the world around us with interactive capabilities. Such networks might be described as physical enclosures to the extent that they define a particular space and are able to both provide functionality and gather information within the confines of the geographically delimited area they cover. These enclosures are not exclusive—they can overlap with, contain, and be contained by other delimited spaces that facilitate information gathering and transmission. Rather than thinking in terms of unitary exclusive enclosures we can discern layers of enclosures, both virtual and physical, with varying spatial reaches and information scopes—cellular networks overlapping Google's Wi-Fi networks, both of which embrace smart homes or offices equipped with radio-frequency indentification (RFID) systems and are in turn encompassed by GPS satellite systems.

These various enclosures facilitate vastly different types of information gathering and transmission. Whereas the enclosure or "cell" encompassed by a mobile phone network might be able to gather pings from and transmit carrier signals to handsets that pass in and out of range, Google may be able to track movements to a much higher degree of resolution and to correlate these with the content of search engine requests and e-mail correspondence. It is also worth noting that different types of enclosures operate with varying levels of symmetry and transparency: book shoppers who go on Amazon.com are able to view why particular recommendations are being made for them: the information-gathering process is relatively transparent to individual users. This is not always the case when, for example, cell phones are used to gather geographic data about users, or even when Amazon.com conducted an experiment in variable pricing, offering a DVD for a lower price to a user who had not logged on as a repeat customer than to a friend of his who had. In many cases—as when search engines gather information about our Web-surfing behavior—we

are largely unaware of what information is being gathered, how, and for what purposes. Every now and then we are provided with a reminder of the monitoring capacity of interactivity—perhaps when we log on to the internet in a foreign country and get a different version of Google news, or find an advertisement related to the content of our e-mail messages on Gmail, and so on.

While futurists celebrate the potentially subversive, empowering, or revolutionary character of the internet, commercial entities are working hard to establish the conditions for what Paul Virilio (2005) has described as the contemporary incarnation of "the great Locking Up of the seventeenth century . . . this time, not on the scale of the asylums or prisons of the Ancient Regime, but on a scale encompassing the whole world" (p. 40). If the creation of enclosures such as those of the prison, the factory, and the asylum referenced by Virilio (following Foucault) facilitated the disciplinary monitoring of inmates and workers, that of the digital enclosure extends the monitoring gaze beyond such institutional walls to encompass spaces of leisure, consumption, domesticity, and perhaps all of these together. If this sounds a touch hyperbolic, consider the ambitious scope of one marketer's prediction about the future of radio-frequency ID tagging—yet another type of interactive enclosure that allows objects to be tracked as they move through space: "Ultimately, we'll be tagging every item in the universe" (Bond, 2003, p. A1). The fantasy of total interactivity, in other words, is also one of complete enclosure.

A DIGITAL ENCLOSURE MOVEMENT

Digital enclosures literalize the physical metaphor of what legal scholar James Boyle (2003) has described as a "second enclosure" movement devoted to the "enclosure of the intangible commons of the mind" (p. 37). In more concrete terms, this process of enclosure refers to a variety of strategies for privatizing, controlling, and commodifying information and intellectual property. As Yochai Benkler (2006) and Dan Schiller (2007) have argued, this process relies not just on expropriation of previously nonproprietary information, but on the construction of an increasingly restrictive legal regime for the enforcement and extension of property rights over a growing range of information. Boyle (2003) offers the example of patent claims for human genes, which has been expanded to include life forms—not just strains of wheat or corn, but also, for example, cats with hypo-allergenic fur. The movement he describes, driven by attempts to profit from the commodification of information, is omnivorous and Borg-like in its drive toward total assimilation: "In the new vision of intellectual property . . . property should be extended everywhere—more is better. Expanding patentable and copyrightable subject matter, lengthening

the copyright term, giving legal protection to 'digital barbed wire' [encryption] even if it is used to protect against fair use" (Boyle, 2003, p. 40). Schiller (2007) describes the privatization of collective or shared knowledge, as in the case, for example, of patent claims on traditional medicines, and the commodification of publicly subsidized or not-for-profit intellectual labor in the university. The expanded role of information in the era of "digital capitalism" has been met with what Schiller refers to as "elite programs of political-economic reconstruction" devoted to "enclosing the immensity of global communication and information provision . . . the paradigm for which was set via enclosure of common lands in England during the epochal transition to agrarian capitalism hundreds of years ago" (Schiller, 2007, p. 43).

The model of England's land enclosure movement is pivotal to critical accounts of capitalism because it illustrates the transformation of violent expropriation into a freely agreed-upon contractual arrangement. The forcible separation of workers from the means of production—a process that Marx (1992) describes as "primitive" accumulation, is, he argues, a necessary precondition for the institution of wage labor insofar as it creates a working class "freed" up to sell control over its labor power:

> **. . . the theft of the common lands, the usurpation of feudal and clan property and its transformation into modern private property . . . all these things were just so many idyllic methods of primitive accumulation. They conquered the field for capitalist agriculture, incorporated the soil into capital, and created for the urban industries the necessary supplies of free and rightless proletarians. (p. 895)**

As Kazanjian (2002) points out, freedom, in this context, is to be understood in a distinctly negative sense: "Writes Marx: "The free workers are therefore free from, unencumbered by, any means of production of their own" (p. 170). This form of freedom from the means of securing their own sustenance underlies a second form of so-called freedom: that of "freely" agreeing to enter into a labor contract under terms advantageous to employers and exploitative to workers (that is to say terms that workers wouldn't voluntarily agree to absent the coercion imposed by the expropriation of the commons).

Free acquiescence to the surrender of control over one's own productive activity is secured by depriving workers of any other option for sustenance—this is the version of freedom that underlies capitalist exchange relations. It is a form of freedom that is, in turn, reliant upon a spatial reconfiguration: workers must be *separated* from the land so that their access to it can be contractually regulated. With the advent of industrialization, entry into a labor contract also meant entry into a physical space

operated and controlled by its owners. As Kazanjian puts it, Marx interprets enclosure as "one of the systems that . . . manufactures capitalists and wage-laborers" (2002, p. 172). The spatial correlative of the emergence of a "free" working class in the capitalist era is the formation of clearly bounded, privately owned, and operated enclosures to which worker access is strictly monitored and regulated.

However, the notion of *primitive* accumulation can be misleading insofar as it implies enclosure is a temporally discrete and prior process—one that takes place only in particular periods of capitalist or precapitalist development—rather than an ongoing process. A more satisfactory account—and one that bears closely on the process of digital enclosure—is provided by De Angelis (1998), who notes that the enclosure process, "is an inherent and continuous element of modern societies and its range of action extends to the entire world" (p. 3). In addition to the everyday process of wage labor and market exchange, capitalism is characterized by ongoing struggles over so-called "primitive" accumulation: attempts, for example, to privatize the national parks and transfer control over their resources to private control, the forcible expulsion of indigenous populations in Africa and Latin America from mineral or oil-rich homelands, and the eviction of farmers from communal lands in Nigeria, "to make way for plantations owned and managed by the World Bank" (Midnight Notes Collective, 2001, p. 2).

As a crucially important productive resource, land plays an important rule in accounts of enclosure—continuous, contemporary, and otherwise—not least because of the central role of agriculture during the early transition to capitalism. However, as De Angelis points out, land enclosure is but one example of the more general form of "primitive accumulation," understood as "an accumulation of capital claims—of titles to existing assets which are accumulated primarily for speculative reasons" (1998, p. 4). Once resources are recognized to be actually or potentially productive, they become subject to attempts to subsume them to capitalist social relations through an appropriation process that—and this is the core of "primitive accumulation" according to De Angelis—results in the "*separation between producers and means of production*" (1998, p. 5). As a strategy for providing capitalism with the basis for accumulation (both the private ownership of resources and a "free" workforce compelled to sell access to its labor) and for reproducing (and expanding) the forms of separation it relies upon, primitive accumulation in turn depends upon a "working class which by education, tradition and habit looks upon the requirements of that mode of production as self-evident laws" (Karl Marx, as quoted in De Angelis, 1998, p. 15). Thus, one of the triumphs of the enclosure movement and a crowning ideological achievement of capitalism has been its ability to win popular consent to, and the consequent

naturalization of, the distribution of property crucial to the exploitation of waged labor. Much the same might be said of the emerging information economy, in which privatization of networks and databases and, therefore, of control over both the means of interaction and the information it generates has become the norm, despite the publicly subsidized character of the original Internet.

As conceptualized in this essay, the process of digital enclosure combines the spatial characteristics of land enclosure with the metaphorical process of information enclosure described by Schiller (2007), Boyle (2003), and Benkler (2006). As information commodities become increasingly valuable resources in the era of digital capitalism (Schiller, 1999), the construction of privately owned and operated interactive enclosures serves to separate users from the means of interaction, transaction, communication, and expression. This process of separation is what the resurgent model of server-client computing envisioned by the Internet cloud achieves. Constant connectivity in the contradictory world of contemporary capital, relies on the separation of users from their data. To the extent that information generated by consumers as they interact with one another, surf the Web, shop online and off, and interact with networks throughout the course of the day becomes economically valuable, the creation of interactive spaces facilitates its capture. Thus, the construction of privatized infrastructures for ubiquitous computing has become one of the economic drivers of investment in the digital media industries. According to the chief of research at computer-chip manufacturer Intel, the company has devoted most of its $4 billion annual research and development budget to products that anticipate the advent of an era of ubiquitous and "proactive" computing (Intel, 2005). In South Korea, a consortium of private developers in partnership with the tech company LG CNS, plan to raise $25 billion to build New Songdo City—the first comprehensive urban digital enclosure in which wireless computing will be ubiquitous (O'Connell, 2005). In the U.S. and Western Europe, mobile telephone companies are spending billions of dollars to develop "third-generation" wireless networks that will enable cell phones to serve as mobile Internet connections and data storage devices.

Investment in the construction of such interactive enclosures is testimony to the anticipated productivity of what Hardt and Negri (2000) describe as "immaterial labor" and Terranova (2000) calls "free labor"—or at least the subset of such labor that I have elsewhere described as "the work of being watched" (Andrejevic, 2004): willing or unknowing submission to monitoring practices that generate economic value in the form of information commodities. The value of transactionally generated information about the use of information technologies derives in large part from its anticipated uses in rationalizing the marketing process through

the customization of goods, services, and advertising. In anticipation of the value of such labor, the proprietary claim made by private companies upon transactionally and interactionally generated information might be considered a form of accumulation of "titles to existing [and anticipated] assets . . . for speculative reasons" (De Angelis, 1998, p. 4). Consider, for example, the patent filed by Google, proposing to custom tailor advertising to online computer game players based on detailed observation of their style of play. According to the patent proposal, both player dialogue and play preferences will be analyzed "to characterise the user (e.g., cautious, risk-taker, aggressive, non-confrontational, stealthy, honest, cooperative, uncooperative, etc.)" (Bantick, 2007). The goal is to use this information to provide in-game ads, in real time, customized to fit the player's psychographic profile. Google's wager is that interactively generated game-player data will have economic value—value that may well increase when it is combined with other information captured by its various services (e-mail content, time-space path, search engine requests, and so on). The more ubiquitous access is to video games, the more comprehensive will be the data gathered by Google, and the harder consumers will be working as they play.

Microsoft has patented a similar plan to customize advertising to users based on the applications and data running on their personal computers. It is an ambitious plan to enclose information not by having it stored on centralized servers, but by inserting a layer of networked interactivity between users and the data on their own machine. In the scenario envisioned by the patent, in order to access our documents and run our applications, we will need to rely upon an operating system that communicates with the network and serves ads based on the information portrait we craft out of our own data: "the software is like adware that figures out what ads to display based on files on the hard drive and what's being displayed on the screen at a given moment" (Hoover, 2007). It is an ambitious plan to go Google one better by offloading even the data storage function onto users: "the software could conceivably gather information on every file on a user's hard drive and send it to advertisers, and the application does little to assuage security and privacy concerns" (Hoover, 2007). Users will still be separated from their data not by physical space but by the software they use to access it, which will stipulate monitoring as one of the terms of access. Even this model depends on the extension of the reach of a physical interactive enclosure: for it to work, just as in the case of the DVD that would not play in Australia, the computer has to be networked.

The process of digital enclosure differs from land enclosure, at least for the moment, to the extent that it does not take place under the threat of force. It does, of course, presuppose the property rights regime of the

contemporary market economy—that is to say, it builds upon, extends, and reproduces the social relations secured by so-called primitive accumulation (land enclosure): "Once the separation is given, the production process can only produce it anew, reproduce it, and reproduce it on an expanded scale (Marx, 1973, p. 462). In other words, it is testimony to the naturalization process that the notion of a nonprivatized enclosure sounds vaguely outlandish—who would provide us with e-mail and Wi-Fi if not Google, EarthLink, et alia? Thanks to the legacy of private control over productive resources, it seems to pass without any serious challenge that the content we provide to companies like Google becomes their property. We think of our e-mail, for example, as our own creation—personal missives that we compose for our own use and that of selected correspondents. But by virtue of composing our letters online, these become the property of the entities that own and control the data enclosure in which our correspondence is stored. A close read of Gmail's privacy policy, for example, reveals that even when users delete messages from their Gmail accounts, Google reserves the right to retain copies indefinitely: "Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers and may remain in our offline backup systems" (Google, 2005). Given that Google's business model is based on accumulating as much information as possible, and the company is engaged in an ongoing expansion of its database resources to do so, we should not count on the company purging its back-up systems anytime soon.

This is not to deny that attempts to reinforce and secure relations of separation remain part of the ongoing process of struggle identified by Schiller (2007). There are still some municipalities in the U.S. working on public or nonprofit schemes for universal Wi-Fi access, but the telecommunications companies have been lobbying hard to restrict and even, in some quarters, to ban such initiatives. The lobbying efforts have resulted in restrictive state legislation and in the proposal of federal legislation to limit municipal Wi-Fi programs, including, for example, the "Preserving Innovation in Telecom Act" and the "Broadband Investment and Consumer Choice Act," both proposed by conservative, business-friendly congressional Republicans (Gnatek, 2006). Louisiana's state ban on free municipal Wi-Fi gained national notoriety when Bell South invoked the law in an attempt to shut down a Wi-Fi service that New Orleans residents relied upon during the devastation caused by Hurricane Katrina. Such efforts indicate that telecommunication companies understand much is at stake in preserving the privatized character of digital information enclosures. When it comes to other information services, such as e-mail and data storage, there is little in the way of proposed alternatives to a privatized commercial model—except, perhaps in the educational and

government research sectors associated with the preprivatized version of the internet.

In the face of the current commercialization of the Web, it is easy to forget that the original digital enclosure of information—its migration into digital storage and its transmission via digital networks—was a publicly subsidized one, a noncommercial, publicly funded network designed to facilitate access to and sharing of information. This historical fact should serve as a much-needed reminder that the convenience associated with digitized forms of data storage, sorting, and transmission is not inherently linked to commercialization or privatization, and that alternative information architectures are possible. Ownership matters, space matters, and materiality, as it were, still matter.

It is in this regard that enclosure is to be understood not simply as a metaphor but as a geographic process involving the reconfiguration of physical space in ways that structure relations of control over access to information of all kinds. As Henri Lefebvre observed, the production of space goes hand-in-hand with that of social relations: "Space is at once result and cause, product and producer; it is also a stake, the locus of projects and actions deployed as part of specific strategies, and hence also the object of wagers on the future" (1991, p. 143). Viewed through this lens, the land enclosure movement, for example, served as a palpably spatial strategy for shaping relations of production in an emerging capitalist economy. Separating workers from the land they cultivated was a necessary precondition for restructuring the terms of their access to productive resources. Against the background of restructured property relations, workers had little choice but to enter "freely" into exploitative wage labor agreements.

As in the case of land enclosure, digital enclosure facilitates control over resources so as to structure the terms of access. Private property is a precondition for the economic logic of digital enclosure which, in its commercial form, provides physical space with an interactive overlay (or multiple overlays) which facilitate the capture and control of data that can be resold in the form of cybernetic commodities. We might think of the expansion of such enclosures as a way of completing the process of spatial dediffferentiation inaugurated by broadcasting. If TV and radio signals were able to overcome the boundaries between sites of leisure and domesticity alike, bringing the messages of advertisers into spaces of recreation, domesticity and consumption, internet connections, cellular phone networks, and digital cable complete the circle by allowing marketers to extract information back from these same sites.

The physical process of enclosure—the creation of ubiquitous, always on networked spaces—becomes a precondition for the rapid expansion of information enclosure. Collecting increasingly fine-grained information

about consumers, viewers, and citizens requires building interactive networks that make the collection process automatic and cost-efficient. When, for example, a supermarket "smart cart" tracks both the items placed in it (via radio frequency identification tags) and the location of the user in the shop, it can gather information that would have been prohibitively costly to collect accurately by either customer surveys or direct human monitoring. Searching out items in a large supermarket, an activity that once took effort but remained economically unproductive, can become value-generating labor when folded into the monitoring embrace of a digital enclosure.

The same might be said of a growing range of activities, transactions, and communication activities that are being encompassed by digital networks. When we make the move from snail mail to Gmail, for example, we make it possible for Google to store, search, and sort the contents of every message, noting when it was sent, received, and responded to. When we switch from analog to digital cable TV, we enable a quantum leap in the ability to track viewer behavior, thanks in part to DVRs that monitor not just which shows are stored and when they are viewed, but which segments are paused, rewound, or fast-forwarded. When we switch from terrestrial to cellular phone communications, we enable service providers to monitor not just our calling activity, but its relation to our time-space path throughout the course of the day. Already some municipalities, including the city of Baltimore, are using cellphone data as a traffic management tool, monitoring the movement of cellphones from one cell to the next to keep track of traffic flow and congestion (Dresser, 2005). As long as the phone is turned on, it serves as a passport into a monitored electromagnetic enclosure.

There is a self-stimulating character to the data-capture capability of digital enclosures—the more ubiquitous they are, the more likely they are to be used in a variety of locations for an increasing range of applications that generate an ever-more fine-grained portrait of users. The more ubiquitous such enclosures are, the more willing users will be to store an increasing range and quantity of personal data on them, from personal correspondence, to online journals and multi-media files. At the same time, the more information users store on commercial servers, the more detailed the user data such sites will be able to collect—not just about what users search for online, or what they write about in their e-mails, but, for example, when, where, and how often they listen to their music, view their pictures, and modify their online files, whom they contact for voice, text, and video communications, when, and where. The list has the potential to expand indefinitely, up to the point of what Bill Gates (1996) has described as a totally documented life—one in which every detail of quotidian existence is redoubled in storable, searchable, digital form.

Gates, however, imagined this data would be captured and controlled by the user rather than by overlapping layers of increasingly coordinated private data collection systems whose activities remain, for the most part, invisible to users. The frenetically productive information and communication environment envisioned by the engineers of such enclosures traces the productive spiral outlined by Lefebvre (1991) as a "sequence of operations" that, "implies a productive consumption: the consumption of a space . . . that is doubly productive . . . What actually happens is that a vicious circle is set in train which for all its circularity is an invasive force serving dominant economic interests" (p. 374). The more ubiquitous such applications become, the more likely users are to use them and thus to generate an expanding range of information commodities.

In its abstract form of ubiquitous computing, a digital enclosure describes a space of universalized recognition and communication in which the places through which we move and the objects they contain recognize individuals and communicate with them (via portable devices). It is a space within which cars know their location and can rapidly access information about their surroundings, one in which supermarket shelves know when they need to be stocked and when they are being approached by someone likely to buy a particular product. In more concrete terms, the infrastructure of the digital enclosure is rapidly becoming a privatized, commercial one—fueled by large investments in wireless technology and ubiquitous computing. As in the case of some of the most ambitious physical enclosures of the 20th century, including the giant shopping malls, the digital enclosures will be commercial ones. In this respect, the digitization of the enclosures—their ability to span sites of labor, leisure, and domesticity—does not merely dedifferentiate the public from the private; in so doing it, privileges commercial information gathering over personal control of information. It allows, in other words, for the privatization of public space to broaden its reach even as such enclosures reprivatize personal information as commercial property. The result is not the end of privacy but its repurposing in commercial form.

The privatization process relies not just on the construction of electromagnetic enclosures, but also on facilities to store the tremendous amounts of data captured by interactive networks. On the one hand, we are confronted by the overlay of physical space with interactive capabilities—space as interface: the grafting of the interactivity associated with the virtual enclosure of the Internet onto the physical spaces of daily life. On the other, we are witnesses to the unprecedented construction of giant data centers around the globe. Rather than a "cloud," the spatial formations associated with digital enclosure are vast data repositories—so-called "server farms"—sprouting up in locations where land and electricity are relatively inexpensive: along the Columbia River Basin in Washington

State and Oregon, in Texas, North Carolina, and elsewhere. Google has reportedly budgeted some $1.5 billion in 2006 as part of a project to build "a worldwide string of data centers" nicknamed "Googleplex" (Markoff & Hansell, 2006) and its rivals Microsoft and Yahoo have embarked on similar data warehouse construction projects.

For a business that seems to have no tangible products, Google relies heavily on very real "bricks-and-mortar" facilities. As one analyst put it, "Google is as much about infrastructure as it is about the search engine . . . They are building an enormous computing resource on a scale that is almost unimaginable" (Markoff & Hansell 2006, p. 1). The physical corollary of computing as pervasive and invisible as air is the concrete condensation of information represented by the construction of such data enclosures on a giant scale—acres of "air-conditioned warehouses filled with thousands upon thousands of computer servers" (Harden, 2006). These loom on the landscape like depopulated afterimages of industrial-era factories, inhabited not by workers, inmates, or patients, but by the combined data doubles of all of them: enclosures not of people, but of information *about* people assembled for the purposes of both assisting them and managing them more effectively. As the interactive enclosures expand and thereby facilitate the convergence of spheres of social practice (we can, thanks to the network, labor from home or the corner coffee shop, stream video at work, and so on), they also gather their resources into the tightly guarded and privately controlled server farms where rapidly growing databases can be mined for profit—in the billions of dollars, based on the earnings of internet giants like Google, Yahoo, and Microsoft, and of database companies like Acxiom and ChoicePoint that are cashing in on post-9/11 Homeland Security contracts and the demand for both security screening and marketing data.

IMPLICATIONS

The emerging information economy that I have described is predicated not on the loss of privacy, but on its galloping expansion in the form of the private control not just of the means of information storage, communication, and retrieval—a long-standing trend, in many respects—but also of the interactively generated information associated with the proliferation of digital enclosures. For years, media ranging from telephony to broadcasting (in the U.S.) have been under private control—but these technologies generated a relatively minimal amount of information about how they were used (as evidenced by the ongoing attempts by broadcasters to monitor viewers and listeners). As they entered the digital realm and were supplemented by networked information and communication technologies, these media technologies helped constitute the means for a

quantum leap in information gathering—a leap that included, in many cases, information that could not be captured previously.

The resurgent server-client model envisioned by the proponents of ubiquitous computing further extends the reach of this capture process: activities that used to take place beyond the reach of interactive monitoring are migrating into the rapidly growing databanks of Googleplex and similar information warehouses. As they do so, they enter private domains that come with new terms of entry. We can access the data we have turned over to them, but only in exchange for willing submission to, among other conditions, the forms of monitoring and control facilitated by the interactive infrastructure.

The goal of this essay is not to downplay the conveniences attendant upon mobile computing and associated forms of networked interactivity. Even forms of target marketing—such as those practiced by Amazon.com—can be useful. It would be wonderfully convenient to be able to access all the music one has ever purchased wherever one happens to be and to be able to share information, data files, and photos effortlessly with distant friends, family, and co-workers, or to retrieve the various documents one is working on without having to back them up incessantly on a proliferating array of storage devices. Indeed, the economic model I have been describing would be untenable if there were not real advantages to the ubiquitous interactivity and communicative capability of what I have been calling digital enclosures. It is, however, critically important to consider precisely what the cost of these conveniences might end up being, not just in economic terms, but in terms of control over information. These costs, and the social relations that underwrite them, are masked by the metaphors of unfettered digital freedom so frequently invoked in discussions of next generation interactive technologies. They are further obscured by the taken-for-granted character of the privatization of networks and databases. "Of course," we reason, "we have to give up some measure of control in exchange for free Wi-Fi access or, for two gigabytes of e-mail storage—if we are only giving up control of information about ourselves that is not of any use to us, why not?"

But perhaps we are giving up more than we realize—not least of which might be the possibility of alternative conceptions of how digital, interactive infrastructures could be developed and implemented. The private, market-driven model of the digital enclosure imposes some significant limits on the promise of the Internet, as the conservative blogger Andrew Sullivan (2002) put it (in a free-market parody of Marx), to allow those with internet access to "seize the means of production." Consider, for example, the case of the Chinese political blogger Zhao Jing who, when the government used its control over Internet routers to block his Web site, switched to the Microsoft Corporation's blogging tool, MSN Spaces.

After he criticized the firing of an editor from one of China's more independent newspapers and called for a boycott of the paper, his blog was shut down again, this time by Microsoft at the Chinese government's behest. As one press account put it, "What was most remarkable about this was that Microsoft's blogging service has no servers located in China; the company effectively allowed China's censors to reach across the ocean and erase data stored on American territory" (Thompson, 2006). Microsoft, with an eye to the lucrative potential of the Chinese market, helped take the activism out of interactivity, with the explanation that in order to do business in China it had to follow the laws that "require companies to make the internet safe for local users" (Spencer, 2006).

Suggestively, the company has also reportedly taken the democracy out of its blog service: "In China, Microsoft does not allow the word 'democracy' to be used in a subject heading for its MSN Spaces blog service" (*War of the Words*, 2006) The company is not alone in making concessions with an eye to the bottom line: "Google . . . restricted search results for the Tiananmen Square massacre; and Yahoo handed over private e-mail information to the conviction of two internet dissidents" (*War of the Words*, 2006). United States politicians have been critical of the actions of these companies abroad, even while some of them defended the Bush administration's Justice Department's request for information about millions of searches made on popular search engines including Google, AOL, MSN, and Yahoo. It is not hard to imagine why large Internet companies with an eye to government regulators might be all-too-willing to comply (although Google did put up some token resistance). These forms of recentralized control over information are facilitated by the processes of privatization and separation associated with digital enclosure. To the extent the resources for communication, expression, and interaction are encompassed by a privatized digital enclosure, access to these resources is subject to enhanced forms of monitoring and control.

Such developments suggest the potential costs associated with a reliance on private companies for an increasing array of communication and information functions that entail surrendering an expanding range of information to their control. On the one hand, the Internet might represent a very powerful tool for free expression even—or perhaps especially—under authoritarian regimes. On the other hand, to the extent that expression becomes increasingly reliant upon private corporations more committed to the realities of the bottom line than to abstract principles of civil liberties, the technology that facilitates the ability to challenge entrenched power could evolve into a breathtakingly efficient tool for monitoring, tracking, and filtering dissident expression. The anarchic version of online communication associated with the Internet may well be an artifact of an early stage in its development represented by the years of

government subsidy and limited control. As the informational slack is eliminated from privatized digital enclosures, every message will become traceable, every interaction, monitorable and recordable. Moreover, as the recent attempts by the U.S. Justice Department to peruse private databases suggest, the digital enclosure facilitates function creep. Data that can be almost effortlessly collected and inexpensively stored and sorted becomes a tempting data mine for state officials, as privacy scruples give way to the political mobilization of the "war" on terror.

In somewhat more abstract terms, to the extent that markets in personal data have proven lucrative, we might also consider the value captured by the digital enclosure as a form of exploitation. Those who submit to increasingly pervasive and productive forms of data-gathering do so as part of an exchange that is structured by private control over the means of interaction. If publicly funded municipal or cooperative Wi-Fi networks or e-mail services were readily available, we might not be so quick to surrender control over our personal information or to submit to detailed forms of information-gathering. Additionally, the regulation of monitoring practices might more readily be seen as a legitimate public issue—rather than an abrogation of the property rights of private corporations. If the city of San Francisco controlled its own Wi-Fi service, residents would approach the decision of whether or not to track and record their own time-space paths as a public issue subject to citizen oversight and accountability.

Finally, enclosure raises the issue of asymmetrical control over personal information, and the ways in which this can be exercised as a strategy for managing or manipulating consumers. It is one thing to imagine marketers targeting ads to users based on general categories of information in which they have demonstrated an interest, but quite another to envision the possibility of marketers targeting specific individuals based on details about their online browsing habits, combined with the content of their e-mail messages, the shape of their time-space path throughout the course of the day, and any other details of their personal and professional lives that can be gleaned from an increasing array of overlapping digital enclosures. Even if details of users' private lives are not publicly disclosed, the very fact that they are aggregated to create personalized advertisements shatters the anonymity that buffered the onslaught of advertising in mass society. The implications for the marketing of certain types of products—from medical remedies to self-help books, and so on—are at best unsettling. As increasingly detailed databases merge and recombine, we may find ourselves facing much more sophisticated and personalized forms of customization—products and services targeted not only on the basis of past preferences, but on increasingly high-resolution data portraits that combine details about our personal lives with

demographic, psychographic, and biometric information. Will those who currently adopt a sanguine attitude toward proliferating consumer surveillance find cause for concern when they learn that details of their love lives, combined with their Web surfing habits, the size of the clothes they buy, the search terms they have entered in search engines, the places they have traveled to, and their daily commuting habits are used in combination not just to inform them about products, but to manipulate them based on their anxieties and insecurities as well as their hopes and fantasies? At what point does the amount of information available to advertisers come to constitute a form of control over consumers—especially in a context wherein consumers have very little knowledge about what information marketers have collected and how they are using it? This might be considered an empirical question (if it were not for the pervasive framing of self-disclosure as a form of empowerment and self-expression): will consumers start to perceive marketing as both a form of intrusion and unfair leverage when ads are priced according to information about past purchasing patterns and individual wealth? What about when advertisers start to use biometric information to determine when consumers might be most inclined to respond to advertising appeals?

As issue is more than a highly variable, legally contested, and double-edged right to privacy: such examples raise the issues of asymmetrical access to information resources, databases, and processing power. At issue is also the question of control over the benefits that accrue to the use of information consumers generate about themselves. As in the case of the land enclosure movement, within the digital enclosure those who control the resources—in this case, information-gathering technologies and databases—can lay claim to the value generated by those who enter "freely" into the enclosure. When submission to monitoring becomes a condition of access not just to work, but to goods and services (from food to telephony), relations of unequal access to and control over resources structure the terms of entry. When all retail outlets implement forms of electronic surveillance and payment, the "freedom" to avoid monitoring becomes, in practice, a theoretical one. Consumers will be free not to divulge information about themselves as long as they do not consume.

For the time being, this submission to monitoring is being portrayed by those who own and operate digital enclosures as a form of participation. Those of us within the reach of the conveniences of the digital enclosure have become habituated to multiplying possibilities for such participation—in designing our shoes, customizing our news, voting on our TV shows, and so on. One of the unifying themes of this seeming multiplicity of practices is that to the extent that they contribute to the production of products for the database industry, they serve as participatory forms of economically productive *labor*. This labor is productive not least because

it is a form of active participation in the processes of marketing to and policing oneself: a version of "self-expression" as an active form of submission that preserves and consolidates relations of power and property.

Labor of this kind has been described as "immaterial," to differentiate the production of information commodities and other forms of communicative capital from that of, say, refrigerators and cars. Immaterial labor, as Hardt and Negri note, can "be dispersed across the unbounded social terrain" and it can expand "to fill the entire time of life" (2000, p. 53). Within the digital enclosure, activities such as playing video games, wending one's way through the streets of San Francisco, and driving on the freeway with one's cellphone can be economically productive, insofar as they generate information commodities with a market value. However, the "immaterial" descriptor can be misleading to the extent that it suggests the valorization of this labor takes place independently of capital resources that make interaction, communication, and information-gathering possible. Digital enclosures are to these forms of immaterial labor what land enclosure was to agricultural and, eventually, industrial labor. The digital enclosure movement—the construction of a privatized architecture for rendering physical space interactive—serves to separate those who generate value from the tools that have rendered immaterial labor so powerful and efficient in the digital era—communication networks, information databases, and so on—and in doing so to structure the terms for accessing these resources. Absent an engagement with questions of ownership of and control over such resources, the process of digital enclosure promises little more than the reproduction of the social relations it purports to overcome. It is no longer enough to call for the cultivation of participation and the deployment of ubiquitous interactivity as an antidote to the undemocratic character of mass consumer culture. We have to consider the actual costs of the convenience on offer and start thinking—and communicating—outside the digital enclosure.

NOTE

1. As of this writing, Earthlink has pulled out of the plan to equip San Francisco with free Wi-Fi access, leaving Google to look for another partner.

REFERENCES

Andrejevic, M. (2004). *Reality TV: The work of being watched*. Lanham, MD: Rowman and Littlefield.

Bantick, M. (2007). Lookout: Google watches your gaming activity. *iWire*, 15 May. http://www.itwire.com.au/content/view/12152/1092/. Last accessed August 20, 2007.

Bard, A., & Söderqvist, J. (2002). *Netocracy: The new power elite and life after capitalism*. London: Pearson Education.

Benkler, Y. (2006). *The wealth of networks*. New Haven: Yale University Press.

Bond, P. (2003). ID tags make products talk. *The Atlanta Journal Constitution*, 29 July, p. A1.

Borges, J. L. (1999). Funes, his memory. In *Collected fictions* (pp. 128–132). New York: Penguin.

Boyle, J. (2003). The second enclosure movement and the construction of the public domain. *Law and Contemporary Problems, 66*, 147–178.

De Angelis, M. (1998). Marx and primitive accumulation: The continuous character of capital's enclosures. *The Commoner Web Journal*, No. 2. http://www.commoner.org.uk. Last accessed August 20, 2007.

Dresser, M. (2005). Cell phone data tracing traffic in Md; System "watches" vehicles, raises fears about privacy. *The Baltimore Sun*, 18 November, p. A1.

Dyson, E., Gilder, G., Keyworth G., & Toffler, A. (1996). Cyberspace and the American dream: A magna carta for the knowledge age. *The Information Society, 12*, 295–308.

Gates, B. (1996). *The road ahead*. New York: Penguin.

Gilder, G. (2006). The information factories. *Wired*, 14.10, October. http://www.wired.com/wired/archive/14.10/cloudware.html. Last accessed August 18, 2007.

Gnatek, T. (2006). Services. *The New York Times*, May 3, p. G1.

Google (2005). Gmail privacy notice. *Google*, October 14. http://mail.google.com/mail/help/privacy.html. Last accessed June 6, 2007.

Harden, B. (2006). Tech companies lured by cheap energy; Microsoft, Yahoo have plans to build servers fueled by Washington dams. *The Houston Chronicle*, July 9, p. A3.

Hardt, M., & Negri, A. (2000). *Empire*. Cambridge, MA: The Harvard University Press.

Holliday, J., & Wieners, B. (1999). The internet cloud. *The Industry Standard*, July 9. http://www.thestandard.com/article/0,1902,5466,00.html. Last accessed August 20, 2007.

Hoover, N. J. (2007). Microsoft patents may hint at the future of Windows. *Information Week*, July 16. http://www.informationweek.com/story/showArticle.jhtml?articleID=201001485&cid=RSSfeed_IWK_News. Last accessed August 3, 2007.

Intel (2005). Research proactive computing. *Intel.* www.intel.com/research/exploratory/. Last accessed 2 August 2005.

Kazanjian, D. (2002). Mercantile exchanges, mercantilist enclosures: Racial capitalism in the black mariner narratives of Venture Smith and John Jea. *The New Centennial Review, 3*, 147–178.

Kopytoff, V. (2006). Wi-Fi plan stirs big brother concerns; log-on rule would allow Google to track users' whereabouts in S. F. *The San Francisco Chronicle*, April 8, p. C1.

Lefebvre, H. (1991). *The production of space*. Oxford: Blackwell Publishers.

Lessig, L. (2004). *Free culture*. New York: The Penguin Press.

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

Markoff, J., & Hansell, S. (2006). Hiding in plain sight. Google seeks an expansion of power. *The New York Times*, June 14, p. A1.

Marx, K. (1992). *Capital volume 1: A critical analysis of capitalist production*. New York: International Publishers.

Marx, K. (1973). *Grundrisse*. New York: Penguin Classics.

Midnight Notes Collective (2001). The new enclosures. *The Commoner Web Journal*, No. 2., September. www.commoner.org.uk/02midnight.pdf. Last accessed August 2, 2007.

MIT Project Oxygen (2004). Project overview. *Project Oxygen*. http://www.oxygen.lcs.mit.edu/Overview.html. Last accessed May 20, 2007.

Mosco, V. (2004). *The digital sublime: Myth, power, and cyberspace*. Cambridge, MA: MIT Press.

Mosco, V. (1989). *The pay-per society*. Toronto: Ablex.

O'Connell, P. L. (2005). Korea's high tech utopia, where everything is observed. *The New York Times*, October 5, 2005, p. A1.

Pearce, C. (1997). *The interactive book*. New York: Penguin.

Reiss, S. (2006). His space: Twilight of the media moguls? Not for this guy. *Wired*, 14.07, July. http://www.wired.com/wired/archive/14.07/murdoch.html. Last accessed August 7, 2007.

Schiller, D. (2007). *How to think about information*. Chicago: University of Illinois Press.

Schiller, D. (1999). *Digital capitalism: Networking the global market system*. Cambridge, MA: MIT Press.

Spencer, R. (2006). Microsoft pulls plug on China protest blog. *The Telegraph*, January 7. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/01/06/wmicro06.hml&sSheet=/news/2006/01/06/ixworld.html. Last accessed June 2, 2007.

Sullivan, A. (2002). The blogging revolution: Weblogs are to words what Napster was to music," *Wired* 10.5, May. http://www.wired.com/wired/ archive/10.05/mustread.html?pg=2. Last accessed January 12, 2006.

Tanz, J. (2007). Desktop, R.I.P. *Wired*, 15.04, March. http://www.wired.com/wired/archive/15.04/wired40_rip.html. Last accessed April 10, 2007.

Telecommunications Industry News (2006). Google seeking patent on location-based Wi-Fi advertising. March 26. http://www.teleclick.ca/2006/03/google-seeking-patent-on-location-based-wi-fi-advertising/. Last accessed August 20, 2007.

Terranova, T. (2000). Free labor: Producing culture for the digital economy. *Social Text 63*, 33–57.

Thompson, C. (2006). The great firewall of China. *The Advertiser* (Australia), April 29, p. W9.

Trippi, J. (2004). *The revolution will not be televised*. New York: Regan Books.

Virilio, P. (2005). *The original accident*. Cambridge: Polity Press.

"War of the words" (2006). *The Guardian* (London), February 20. Retrieved November 6, 2007 from http://www.guardian.co.uk/china/story/0,1713317,00.html.