Culture Unbound
Journal of Current Cultural Research

Surveillance: The "Digital Trail of Breadcrumbs"

By Toby Miller

Surveillance is an ordinary part of daily life. It's commonplace, routine. If you talk to state security agents, they'll tell you there are perhaps ten million spies in the world (approximately half of whom are Chinese). The United States alone boasts well over three million surveillance and enforcement workers (http://www.bls.gov/oes/current/oes330000.htm), and we all know how pervasive closed-circuit television has become in major cities (there are said to be 4.2 million such cameras in Britain and thirty million in the US) not to mention radio-frequency identification chips, website cookies, store-loyalty cards, and global-positioning trackers (Butler 2009). Law-enforcement services are thrilled with YouTube's surveillance possibilities as a means of directly observing "crimes". They even urge YouTubers to become amateur sleuths. One in five employers in the US screen candidates for jobs by searching social-networking sites such as Facebook for incriminating evidence about them (Miller 2009; Havenstein 2008). Even as most countries in the Global North see decreases in violent crime and terrorism (down 4.4% in the US in the first six months of 2009, http://www.fbi.gov/ucr/2009prelimsem/index.html), there are massively-increased investments in the surveillance sector, whose public-relations machines trot out panics galore (La Vigne *et al*. 2008). The computing-security firm McAfee publishes a *Virtual Criminology Report* each year that is dedicated to alarming readers about information systems' porosity—and exciting them at the ease with which these can be turned to surveillance purposes.

This should surprise no-one. For surveillance has been a central strut of modernity since it began, supposedly making populations secure and productive. Foucault explains:

> an important problem for [French] towns in the eighteenth century was allowing for surveillance, since the suppression of city walls made necessary by economic development meant that one could no longer close towns in the evening or closely supervise daily comings and goings, so that the insecurity of the towns was increased by the influx of the floating population of beggars, vagrants, delinquents, criminals, thieves, murderers, and so on, who might come, as everyone knows, from the country. ... In other words, it was a matter of organizing circulation, eliminating its dangerous elements, making a division between good and bad circulation, and maximizing the good circulation by diminishing the bad (1978/2007: 54; also see 1976)

With the expansion of state authority into the everyday, into all corners of life, the *quid pro quo* for the security afforded by governments has become that our lives be knowable. The equivalent expansion of corporations into the everyday, into all

corners of life, has as *its quid pro quo* for the provision of goods and services by companies that they, too, know more and more about us. The supposedly neoliberal paradise of the monadic, ratiocinative, citizen-consumer is nothing of the sort. It represents the onward march of governmental and corporate knowledge of the population, spectacularly exemplified by the genre of securitainment that Mark Andrejevic engages in this thematic section. As Jessica Behm's essay shows, even military clothing is now a technological surveillance device, while however poorly it may do the job, biometrics' ongoing popularity as a method of "identifying" miscreants is notably examined by Kelly Gates here.

It's touching, isn't it, to see both left and right tie themselves in knots over surveillance? The right shouts about too much state power, even as it calls for authoritarian policing and religious and racial profiling of potential evildoers. The left shouts about too few civil liberties, even as it calls for legislation to secure freedom from corporate oversight. The right seems not to care a jot about corporate invigilation of everyday life; the left not a whit about the need to protect societies through espionage. Hence bodies like the American Civil Liberties Union referring to contradictory yet bipartisan anxieties over the birth of a "surveillance monster" inside a "surveillance society" (Stanley and Steinhardt 2003). Both sides get caught up in dilemmas over how to understand the act of looking, as if it were unholy. In related papers for this section, Henry Krips troubles psychoanalytic film theory and Ruhi Khan queries "native" ethnography.

There is an interesting history to the complex blend of private and public surveillance that underpins what these contributors offer us. A poll of over a thousand US business executives in the mid-1970s followed up a *Harvard Business Review* study of 1959 (Wall 1974; Furash 1959). The corporate hacks who were surveyed believed that espionage had increased over the previous decade and a half, because of declining ethics, increasing competition, macroeconomic concerns, and shareholding by executives. The bigger the company, the more intelligence it gathered, and the more security measures it took. Secondly, younger executives were more in favor of espionage than their older counterparts, regardless of legality. The US government estimated a loss to corporate business of US$3 billion in 1965 because of (mostly domestic) spying, and US$4 billion five years later. By 1973, almost three hundred thousand security guards were employed by US corporations, and overall expenditure on the sector was US$4.4 billion. The Federal Bureau of Investigation investigated four hundred cases of industrial espionage in 1994 and eight hundred in 1996, while the American Society for Industrial Security estimated annual losses to US companies from such assaults at US$100 billion in 1997, up five-fold in two decades (Miller 2003). As the FBI puts it, explaining its operations under the Economic Espionage Act of 1996, "The Cold War is not over, it has merely moved into a new arena: the global marketplace" (http://www.fbi.gov/hq/ci/economic.htm). In 2004, theft of trade secrets

and critical technologies was said to be worth US$250 billion a year (Gebhardt 2004).

The euphemism ”competitive intelligence” has been coined to describe both legal and more dubious sides to surveillance. Some of this work involves studying political activities, laws, economic reports, country and client information, production figures, and research and development. The dubious part comes when marketing or technological developments have their costs cut by stealing information developed and paid for by others. Classic cases include car designs, drug prototypes, anti-parasite chemicals, toothpaste market reports, and disk drives (Miller 2003).

During the late 1980s, the Central Intelligence Agency kept its budget up despite *perestroika* by claiming that national security risks were being displaced by commercial ones, with industrial surveillance the latest Soviet threat. In addition, it was stated that even allies were penetrating US firms in search of secrets that would produce business advantages. And throughout its life, Britain’s Official Secrets Act has been subject to debates over the status of commercial forms of knowledge and whether their theft can be construed as a threat to security on purely economic grounds. This is the point where safety and national interest meet in the capitalist world system. US intelligence claims that dozens of countries are involved in economic espionage against it, and must be countered through ever-greater levels of surveillance. Government policy shifts were announced in the 1990s, tying the spy agencies of Australia, Britain, the US, Russia, and South Africa to economic work separate from, and equal to, their alibi of national security (Miller 2003).

And the private sector itself? In addition to spying on competitors, corporations also engage in surveillance of their employees. The newer technologies offer crucial forms of Taylorism, measuring keystrokes and delivering anti-theft tactics. No computer, email account, or phone is secure from corporations’ predations and obsessions (Bupp 2001; Mosco and Kiss 2006; Hayes 2008; Derene 2007). My principal concern here, however, is their surveillance of customers, particularly via the media.

The prevailing euphemism for this surveillance is “accountability”. That term *should* refer to corporations and governments being accountable to popular democracy; but in the culture industries, it signifies the information about audiences that commercial web sites and TV networks hand to advertisers. These data cover identity, wealth, and taste: who people are, what they watch, when and where they do so, and what that then urges them to purchase. Hence the advent of firms such as Phorm and FrontPorch (“Watching” 2008), and corporate consultant Openwave’s useful *Privacy Primer*, which says it is offering consumer protection from an *Era of Behavioral Marketing*, but gleefully avows that ”On the internet, customer feedback isn't requested so much as it’s collected, like a digital trail of

breadcrumbs. Mobile technology only sharpens the focus on user behavior by bringing location and contextual information into play" (2009).

New on-line corporate sites that replay US television and movies, such as Hulu, use "geo-filtered access logs" to disclose viewer information, alongside confessional testimonies by potential audiences—if you tell us about your life and your practices of consumption, we'll tell you about programs that may interest you (Miller 2010). Disney's global sports TV network ESPN exploits interactive *fora* such as "My Vote" and "My Bottom Line" to uncover more and more data about audience drives, in the name of enabling participation and pleasure in watching. Visitors to Time Warner's HBO web site on boxing encounter a section entitled "COMMUNITY" that invites them to vote in polls, subscribe to a newsletter, and express their views on bulletin boards. This "COMMUNITY" is a system of surveillance that allows the network to monitor viewers for ideas without paying for intellectual property—which they must sign over in order to participate (Miller 2010; Miller and Kim 2008).

And consider the impact of YouTube's Video Identification. The software was developed with Disney and Time Warner. It is a surveillance device for tracking copyrighted materials on the site that follows the history of each uploaded frame, spying on users to disclose their internet protocols, aliases, and practices to corporations. That permits these companies to block or allow reuse of texts, depending on their marketing and surveillance needs of the moment. YouTube has become Hollywood's valued ally, tracking intellectual property, and realizing the culture industries' dream of engaging in product placement each time copyright is infringed on line, while learning more and more about their audiences (Miller 2009).

There is, of course, a certain amount of resistance to these tendencies, from unions (Mosco and Kiss 2006) and social movements (Privacy International publishes a yearly review of "Surveillance Societies" [2008] while Liberty (http://www.liberty-human-rights.org.uk) and the Electronic Privacy Information Center, http://www.epic.org, do pathbreaking work) plus scrutiny through privacy commissions (such as Canada's, http://www.priv.gc.ca/index_e.cfm) and academia (the Surveillance Studies Network, http://www.surveillance-studies.net, runs the journal *Surveillance and Society*, while, more ambiguously, the Information War Monitor consults with "industry", http://www.infowar-monitor.net/; also see Maxwell 1996, 1998, 1999; 2005; Lyon 2007; Cohen 2008).

I began this introduction by insisting on the ubiquity and inevitability of surveillance. That certainly doesn't mean we should accept the way that states track residents' every move, or that corporations observe employees' and customers' every shimmy, selling the results without their knowledge or approval. Foucault is right to twin surveillance to modernity as a longstanding form of control as the predicate to growth. But it has always had a paradoxical other side. The right to anonymity, to being a stranger, is just as much part of modernity as is the trade-

off with security (Simmel 1976). Specifically, the internet is a multiply-edged sword, and we must be aware of all its capacities in order to control it democratically, thereby securing the right to individual and cultural mystery as much as security.

Toby Miller is Professor Media & Cultural Studies at the University of California, Riverside, and the author of over twenty books, the latest of which is *Television Studies: The Basics*. E-mail: tobym@ucr.edu.

The editor and the authors would like to thank the anonymous reviewer whose thoughtful and initiated response has contributed greatly to this thematic section of *Culture Unbound*.

References

Bupp, Nancy (2001, Fall): "Big Brother and Big Boss Are Watching You", *WorkingUSA,* 69-81.
Butler, Don (2009, June 18): "You Are Being Watched", *Ottawa Citizen*.
Cohen, Nicole (2008): "The Valorization of Surveillance: Towards a Political Economy of Facebook", *Democratic Communiqué* 22, no. 1, 5-22.
Derene, Glenn (2007, September 20): "Is Your Boss Spying On You? Inside Workplace Surveillance", *Popular Mechanics*.
Foucault, Michel (1976): *Histoire de la sexualité, I: La Volonté de savoir*, Paris: Gallimard.
—— (1978/2007): "Spaces of Security: The Example of the Town, Lecture of 11th January 1978" Trans. Graham Burchell, *Political Geography* 26, no. 1, 48-56.
Furash, Edward E (1959): "Problems in Review: Industrial Espionage", *Harvard Business Review* 37: 6.
Gebhardt, Bruce (2004, January 12): Speech to the International Security Management Association, Scottsdale, Arizona.
Havenstein, Heather (2008, September 12): "One in Five Employers Uses Social Networks in Hiring Process", *Computerworld*.
Hayes, Read (2008): *Strategies to Detect and Prevent Workplace Dishonesty: An ASIS International Foundation Research Council CRISP Report*, Alexandria, Va.: ASIS International Foundation.
La Vigne, Nancy G., Samantha S. Hetrick & Tobi Palmer (2008): *Planning for Change: Security Managers' Perspectives on Future Demographic, Crime, and Technology Trends*, Washington: Urban Institute/ASIS Foundation.
Lyon, David (2007): *Surveillance Studies: An Overview*, Cambridge: Polity Press.
McAfee (various years): *Virtual Criminology Report*, Santa Clara: McAfee.
Maxwell, Richard (1996): "Ethics and Identity in Global Market Research", *Cultural Studies* 10, no. 2, 218-236.
—— (1998): "What is a Spy to Do?", *Social Text* 56, 125-141.
—— (1999): "The Marketplace Citizen and the Political Economy of Data Trade in the European Union", *Journal of International Communication* 6, no. 1, 41-56.
—— (2005): "Surveillance: Work, Myth, and Policy", *Social Text* 23, no. 2, 1-20.
Miller, Toby & Linda J. Kim (2008): "Overview: It Isn't TV, It's the 'Real King of the Ring'", *The Essential HBO Reader*, (ed.) Gary R. Edgerton & Jeffrey P. Jones, Lexington: University of Kentucky Press, 217-236.

Miller, Toby (2003): *SpyScreen: Espionage on Film and TV from the 1930s to the 1960s*, Oxford: Oxford University Press.
—— (2009): "Cybertarians of the World Unite: You Have Nothing to Lose But Your Tubes!", *The YouTube Reader*, (ed.) Pelle Snickars & Patrick Vondereau, Stockholm: National Library of Sweden, 424-440.
—— (2010): *Television Studies: The Basics*, London: Routledge.
Mosco, Vincent & Simon Kiss (2006): "What are Workers Doing About Electronic Surveillance in the Workplace? An Examination of Trade Union Agreements in Canada", *The Information Society: Emerging Landscapes*, (ed.) International Federation for Information Processing, Berlin: Springer, 193-209.
Openwave (2009): *Privacy Primer: Protecting the Consumer in an Era of Behavioral Marketing*, Redwood City: Openwave.
Privacy International (2008): *Annual Report*, London: Privacy International.
Simmel, Georg (1976): "The Metropolis and Mental Life", Trans. Kurt H. Wolff, *Sociological Perspectives: Selected Readings*, (ed.) Kenneth Thompson & Jeremy Tunstall, Harmondsworth: Penguin, 82-93.
Stanley, Jay & Barry Steinhardt (2003): *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, New York: American Civil Liberties Union.
Wall, Jerry L. (1974): *Industrial Espionage in American Firms,* Dissertation Presented to the Faculty of the Graduate School, University of Missouri.
"Watching While You Surf" (2008, June 7): *Economist*, 3-4.