THE CHRONICLE OF HIGHER EDUCATION

Watching the Watchers

By Peter Monaghan | March 17, 2006

In the burgeoning field of surveillance studies, researchers scrutinize the many ways in which human activity is monitored by government and industry

Walk anywhere in Manhattan's business districts, and almost every step you take will be recorded by surveillance cameras.

But you don't need a camera or a big city for surveillance. Anyone on a computer — from a farm outside Orem, Utah, to a resort on the Fijian island of Viti Levu — is most likely being monitored by electronic forms of surveillance that track consumer habits or calculate probable voting behavior.

As a fast-growing group of scholars sees it, the recent revelations of warrantless domestic spying and "data mining" by federal agencies should come as no surprise at all. They say a public-private merger of government and commercial interests has created an expanding and ever-more-encompassing net of surveillance.

Proponents promise that, post-9/11, increased surveillance will bring security, which is why legislation like the Patriot Act is essential to clearing a path for it. Critics decry the transformation of the information age into an era of pervasive spying. The conflict means that academic research and publishing on the subject are flourishing.

"Several decades ago, you could probably fit all the surveillance researchers into a phone booth; now you would need an auditorium," says Gary T. Marx, a professor emeritus of sociology at the Massachusetts Institute of Technology who is the doyen of such studies in the United States.

The embrace of surveillance technology by the United States and other economically developed countries is driving the growth of an interdisciplinary subfield known as surveillance studies, says David Lyon, director of the international Surveillance Project at Queen's University, in Ontario, and the author of many books on the subject.

The raw material for the field is everywhere (see "What Do Surveillance-Studies Scholars Watch?"). The legal, political, and philosophical questions are proliferating as

well. Researchers in the field are asking whether surveillance measures really do reduce crime and increase security, and how they alter the nature of modern citizenship. What does the explosion of surveillance mean for long-cherished notions and hard-won rights of privacy, expression, association, movement, and assembly? And does the demographic sorting of citizens include them in some realms of citizenship — for example, providing them with certain government services — and exclude them from others — if, say, they are identified as security risks?

Because such questions are broader than one discipline can answer, collaborations are springing up across academe. Anthropologists, communications technologists, criminologists, cultural and literary theorists, geographers, historians, legal analysts, philosophers, political scientists, social economists, sociologists — all have angles on surveillance.

What they discover may have far-reaching consequences in an increasingly watchful — and watched — civilization.

THE PRIVACY BUGABOO

A key consideration for these scholars, as for the general public, is privacy. But many researchers caution against fixating on it. Such a focus, says Mr. Marx, ignores the fact that "for some, the real issue isn't too little privacy, but too much." That is, too much secrecy. Encryption and privacy laws, for instance, have so restricted what employers and employees can say and ask, that "some persons and organizations clearly feel we have gone much too far in the other direction."

Many researchers also believe that an emphasis on individual privacy steals the spotlight from larger issues. More useful, Mr. Marx suggests in an e-mail message, is "to empirically and logically and ethically understand the different forms, contexts, and conditions of [surveillance], and to show how things connect and disconnect. … Questions about distribution and impacts require systematic empirical research, not horror stories and talk-show fodder."

Whether it is the government trying to close off opportunities for people to commit crime or a corporation trying to open up opportunities to make sales, surveillance is always "a sort of social engineering," says Mr. Lyon, who is North American editor of the online journal Surveillance & Society (http://www.surveillance-and-society.org), which he and some colleagues inaugurated in 2002.

———

Though the attacks on New York and Washington on September 11, 2001, catalyzed scholarly interest, Mr. Lyon notes that he and his colleagues began studying the growing pervasiveness of surveillance before those events.

Much of that interest has focused on government surveillance. The goal of intelligence agencies is to achieve "the ultimate in coverage: constant, real-time surveillance of the planet," says James Bamford, an investigative journalist and independent scholar who has written several books on intelligence and surveillance.

Civil-liberties advocates agree. In a 2003 report, the American Civil Liberties Union warned of the approach of an era of cheap, ubiquitous cameras "tied via wireless technology into a centralized police facility where the life of the city can be monitored" — and also stored digitally, forever, in giant databases, constantly augmented by feeds from unmanned surveillance aircraft such as those used by the military.

While civil-liberties advocates deplore such developments, academic researchers are examining their continuity with long-established practices like workplace monitoring. One can, in fact, detect a continuum of surveillance in the United States that began with the 18th- and 19th-century slave pass, and continues today in the monitoring of e-mail and telephone conversations, for example, or the use of infrared badges to track employees, writes Christian Parenti in The Soft Cage: Surveillance in America From Slavery to the War on Terror (Basic Books, 2003).

Mr. Parenti, a journalist and former fellow at the Center for Place, Culture, and Politics at the Graduate Center of the City University of New York, contends that the growth of such monitoring bureaucracies has progressively curtailed American liberties, shifting power from the judiciary, the press, and other democratic institutions.

BUYING INTO SURVEILLANCE

The public generally has been ambivalent about surveillance, despite its invasiveness, researchers suggest.

"People want surveillance on some level, and it can be used on a positive level," says Dean Wilson, a lecturer in criminology and criminal justice at Monash University, in Australia. "Surveillance can always run a spectrum between care and control. But it has to be said that post-9/11 surveillance has tended to be more about control than about care."

———

Mr. Wilson and Clive Norris, a professor of sociology at the University of Sheffield, are preparing a volume of essays called Surveillance, Crime and Social Control (Ashgate).

Mr. Lyon agrees that the public's take on surveillance, which promises to improve safety and to help people shop, is ambivalent. Surveillance's "plausible rationales" include convenience, safety, comfort, efficiency, productivity, and security, he notes. So, it is no surprise to him that people fairly readily provide the triggers that all surveillance systems need.

Even the most dizzying, high-technology tools, such as complex algorithms that predict the likely behaviors of multiple cross-sections of a society, rely on people using bank cards, Web sites, highways, and other conveniences of modern life.

Mr. Marx of MIT is troubled by the emergence of a range of "soft surveillance" techniques in which personal information is elicited through an appeal to the needs of the community.

Consider, he says in one essay, a Justice Department "Watch Your Car" program in which owners place decals on their cars that invite police anywhere to stop the car if it is driven late at night. Or, he adds, "the ubiquitous building signs, 'In entering here you have agreed to be searched.'"

Many such methods solicit "good citizenship or patriotism," he says. Combined with the data gathered from people as they drive, shop, and surf the Web, it adds up to what Mr. Marx calls "surveillance creep," the displacement of brutally invasive methods by a series of new and expanding demands for personal information.

"There is a chilling and endless-regress quality in our drift into a society where you have to provide ever more personal information in order to prove that you are the kind of person who does not merit even more intensive scrutiny," he writes in an e-mail message.

Mr. Lyon argues that at work, shopping, or traveling, people provide information — usually unwittingly — to governments and businesses that allows them to treat different categories of people differently. The result is new forms of social control developed "without democratic participation," he writes in Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination (Routledge, 2002). The most obvious category of such treatment, he says, remains race, most dramatically in the racial profiling of purportedly dangerous groups such as young black men or of people who share the nationalities of foreign foes.

———

But a broader, "rampant process" is under way, he believes, to "advance the work of customer-relationship marketing, which of course has zero to do with relationships and everything to do with building connections with potential customers, and trying to lure them into consuming more, and of course to cut off others from the whole process.

"These days," he continues, "it's not only workers but also consumers who get fired, from whatever — telephone companies, banks — because they are not thought to be worth anything to the corporation concerned."

A GANG OF 'LITTLE BROTHERS'

Civil-liberties advocates complain that privacy laws mean little when government agencies can simply buy purchasing information from private-sector data banks.

Groups such as the American Civil Liberties Union, the Electronic Privacy Information Center, the Electronic Frontier Foundation, and the Free Congress Foundation are pressing for improved, comprehensive privacy laws because, as the ACLU has put it, "the technologies of surveillance are developing at the speed of light, but the body of law that protects us is stuck back in the Stone Age."

The privacy advocates say that the Fourth Amendment, which asserts the right of people to be free from unreasonable searches unless authorities have probable cause to suspect criminal activity, is under siege.

That sentiment is reflected in much of the academic analysis of the moral and legal implications of surveillance, with an emphasis on concepts such as informed consent.

Harlan J. Onsrud, a professor of spatial information at the University of Maine at Orono, has argued that the operators of surveillance systems seem unconcerned with that notion. Cartographers like himself, he has written, are perturbed that data sets about citizens are being integrated without their informed consents. Their concern is heightened by the many kinds of records that are being kept: maps of emergency-vehicle calls, crime patterns, roads and utilities, tax payments, land usage, health and medical services, business location, waste disposal, traffic flows, and much else.

Historical conceptions of privacy rights were formulated to resolve conflicts among "singularly identified individuals," he says, and are prone to being abused when applied to profiling of large groups.

———

Tracking people via their cellphone calls, the selling of post-office change-of-address cards, analyses of small-area census and tax data are less an Orwellian Big Brother scenario than a case of many Little Brothers ganging up, agrees Mark S. Monmonier, a distinguished professor of geography at Syracuse University and author of Spying With Maps: Surveillance Technologies and the Future of Privacy (University of Chicago Press, 2002).

But Mr. Monmonier also sees possible benefits. He imagines a system of speed limits that varies to suit changed road conditions. It would control the flow of traffic, and could have policing aspects. And, he says, "I can envisage linking that to a governor on car engines that would not let them go faster than the limit. Is that highly invasive? Only if you consider that people have a right to speed."

Jerome E. Dobson, a research professor of geography at the University of Kansas, is far less sanguine about the prospects for ethical use of such data. An expert in using Global Positioning Systems to identify and assess environmental and terrorist risk factors, he has made dire predictions about an era of "geoslavery," which he has called "the greatest threat to freedom we've ever experienced in human history."

Mr. Dobson, a former researcher at the federal government's Oak Ridge National Laboratory who is now the president of the American Geographical Society, fears that the kinds of GPS tracking now used to keep tabs on criminals, parolees, and most commonly sex offenders, will expand to take in more classes of people. He imagines that such systems might restrict people's access to sensitive sites (or any kind of site) by warning them when they approached too closely.

Perhaps, he says, the systems might even be linked to physically disabling technology — say, a shock whenever an individual was acting improperly or was at odds with whomever controlled the switch.

FORMS OF RESISTANCE

When any such technologies emerge, attempts to deploy them will be vigorous, researchers expect.

Indeed, says Mr. Lyon, people do retain some power to negotiate their involvement with surveillance technologies. At a simple level, for example, they can modify their actions and behaviors or falsify information to confound others' record keeping — which teenagers seeking free e-mail accounts were long ago quick to discover.

———

In his The Digital Person: Technology and Privacy in the Information Age (New York University Press, 2004), Daniel J. Solove, an associate professor of law at George Washington University, laments the indifference of Americans to their loss of privacy as they become mere "digital dossiers." He advocates not isolated lawsuits against prying agents, but a concerted, national regulatory system akin to those that keep food, environment, and financial institutions in check.

Artists have also spoken out against pervasive surveillance. The notion that the body is becoming a virtual data set has figured in such productions as Super Vision (http://www.superv.org), a collaboration between the performance group the Builders Association and the visual-arts studio dbox. The project uses digital animation, video, electronic music, live performance, and computerized set design to suggest some of the dimensions of life in a "post-private society" in which citizens become "data bodies" that circulate, stained by bad credit and other digital traces.

Steve Mann, a professor of electrical and computer engineering at the University of Toronto who directs the EyeTap Personal Imaging Lab, has helped to improve small-camera design with his research, but his performance pieces attack deployment of such cameras as frequently unquestioning and abusive. He has taken a wearable camera into shops to film himself being filmed and then recording his responses to store managers who confront him that he did not give them permission to film him either. (For some of the results, see Shooting Back, a Web documentary, http://www.wearcam.org/shootingback.html).

Such table-turning acts underpin the performances of the Surveillance Camera Players, in New York, who perform in front of surveillance cameras in, for example, Times Square, and have given rise to World Sousveillance/Subjectrights Day, December 24 (http://www.wearcam.org/wsd.htm).

FAILURE AND FAIL-SAFE

Predictably, where there is resistance to unchecked surveillance, there is also resistance to the resistance.

As federal and state governments contemplate stronger privacy laws, some major industry groups have decried such efforts as bad for business — and as contrary to federal government agencies' own common practices of information sharing.

But scholars are also questioning whether the justification for increased government surveillance — greater security — is a false promise. Many surveillance technologies

have been promoted as capable of far more than they are, researchers and civil-liberties advocates contend.

The Electronic Privacy Information Center, for instance, estimates that Londoners are filmed or photographed more than 300 times a day; yet none of the more than 1.5 million cameras installed in the city in response to terrorist bombings has ever prevented an attack or caught a suicide bomber before the act.

Surveillance researchers are not surprised by the lack of results, because experiments have shown that few individuals can concentrate on video monitors for more than 20 minutes.

How, in any case, could the success of techniques like closed-circuit television cameras ever be measured, asks Mr. Wilson of Monash. "It's a very complicated question, with a lot of money poured into it," he says. In open-street environments, introducing cameras and then attributing a decline in crime to them is "extremely simplistic," he says, "because they're always introduced in combination with other things, such as more policing."

Yet, cameras "still have a great appeal to the bureaucratic mindset," he says. "There's a great desire to have reports that produce statistics, and a graph with a line that points down."

CREATING A FRAMEWORK

Mr. Lyon notes that the tug of war between privacy and security can be complicated.

"The question, from my point of view as a sociologist, is to say, 'Well, at what point do people comply willingly?' And of course lots of people do comply willingly," he says. "They actually ask, for example, whether their number has been taken if they're going through the airport with their frequent-flier card."

Mr. Marx agrees. He writes in an e-mail message that dealing with "the norms around concealing and revealing information" calls for a field that could be dubbed the sociology of information. "We need," he writes, "a broad conceptual net that captures privacy, secrecy, confidentiality, anonymity-identifiability, freedom-of-information, diplomacy, confessions, etc."

The collection of data about citizens is inevitable — it is how business and much else is now run — so what is needed, contends Simson L. Garfinkel, a postdoctoral fellow

at the Center for Research on Computation and Society at Harvard University, is insistence on responsible management of that activity.

"In the U.S., data privacy has traditionally been assured by trying to have limits on collection," he says. "As a result, now, if people can collect data, they can pretty much do what they want with it."

Mr. Garfinkel would like to see a "national data protection office, like every other country in the industrial world." Information about people could be compartmentalized so that it was not available for the wrong reasons, and laws could require that people be told when their records had been accessed.

And, he says, more "cultural awareness" of privacy issues would lead even critics of surveillance to see that privacy and surveillance must protect each other's interests.

After all, he says: "You may need surveillance to ensure privacy, since an important part of privacy is freedom from intrusion, and being blown up by terrorists represents a considerable intrusion into people's lives."

WHAT DO SURVEILLANCE-STUDIES SCHOLARS WATCH?

When people think about surveillance, they usually think of the metal detectors at airports or the ubiquitous, unblinking eyes of surveillance cameras. But surveillance-studies scholars interviewed by The Chronicle say that a number of other, less visible means of monitoring are increasingly being used. Those methods, they add, may be made more dangerous by the refusal of the United States to adopt a comprehensive privacy law, relying instead upon a patchwork of protections. Among the methods are:

- Complex algorithmic systems that purport to differentiate people at a distance through facial features and even to spot anomalies from norms of behavior. Such systems are replacing or augmenting direct observation, which suffers from limits of human attention and patience.

- DNA testing and other forms of genetic monitoring as a key sorting device for the next generations of health care and employment. Civil-liberties groups lament that current medical-privacy laws do not prevent the amassing and sharing of records by insurance companies and trade organizations. The industries are lobbying Congress to prevent the passage of laws that would impose more-stringent limits on such practices.

- Biometric systems that use fingerprints, irises, retinas, voice patterns, hand geometry, facial features, and other aspects of the human body. Such systems are being used in passports and visas, workplace-entrance systems, banking, e-commerce, and many other settings, including college-campus buildings.

- Devices and systems that can locate and track people, including cellphones, navigation systems, traffic-control systems, and ankle tags. In radio-frequency identification, or "smart shelf" technology, tiny chips are placed in packaging so that retailers can monitor their shipment and their movement once purchased, or stolen. The systems solve the problem of items running low on shelves, greatly increasing their sales.

- "Data aggregator" companies. While the Supreme Court of the United States has affirmed that the home is, as Justice Antonin Scalia has put it, "safe from prying government eyes," data surveillance, or "dataveillance," knows no concrete or fiberboard boundaries. Data-aggregator companies pull together details and patterns of consumption into databases that private or public organizations may freely purchase. In a 2003 report, the American Civil Liberties Union complained, it "will soon be possible to combine information from different sources to re-create an individual's activities with such detail that it becomes no different from being followed around all day by a detective with a video camera."

SURVEYING SURVEILLANCE

With scholarly articles on surveillance multiplying as fast as closed-circuit cameras, keeping track of it all requires a keen and nimble eye. One place to start is Surveillance & Society, a free, online quarterly journal started in 2002 by researchers in a number of countries and based at the University of Newcastle Upon Tyne. A glance at some of the work in recent issues provides a sense both of the range of investigation under way and the international scope of the inquiry:

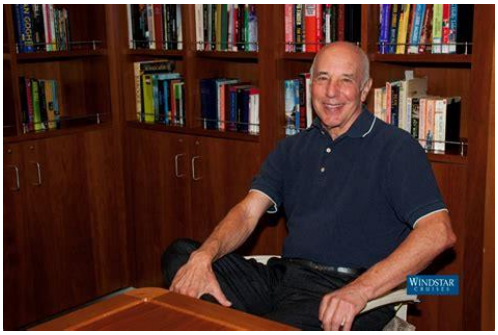
- Lynsey Dubbeld, Centre for Studies of Science, Technology, and Society, University of Twente, the Netherlands: In "Protecting Personal Data in Camera Surveillance Practices" (Vol. 2, Issue 4; December 2004), Ms. Dubbeld argues that data-protection practices in the operation of video-surveillance systems include few procedures to protect subjects' rights.

- Jonathan Finn, department of communication studies, Wilfrid Laurier University, Canada: In "Photographing Fingerprints: Data Collection and State Surveillance" (Vol. 3, Issue 1; March 2005), Mr. Finn examines the way that fingerprint identification acted historically as an avenue for the introduction of other techniques of state surveillance.

- Steve Wright, Praxis Centre for the Study of Information & Technology for Peace, Conflict Resolution & Human Rights, Leeds Metropolitan University, England: In "The Echelon Trail: an Illegal Vision"(Vol. 3, Issue 2/3; August 2004), Mr. Wright examines the history of public revelations about the system of global telecommunications interceptions, Echelon, that the United States operated in England in the 1970s. Academic researchers who first discovered the system were silenced, and their findings did not become common knowledge until the late 1990s.

- Haim Yacobi, department of politics and government, Ben-Gurion University of the Negev, Israel: Mr. Yacobi's "In-Between Surveillance and Spatial Protest: The Production of Space of the 'Mixed City' of Lod" (Vol. 2, Issue 1; March 2004) analyzes the role of surveillance and other forces of state control of Palestinians protesting or otherwise struggling for space they have lost within supposedly ethnically mixed cities in Israel.

- Nils Zurawski, Institute for Criminological Research, University of Hamburg, Germany: In "'I Know Where You Live!'--Aspects of Watching, Surveillance and Social Control in a Conflict Zone (Northern Ireland)" (Vol. 2, Issue 4; December 2004), Mr. Zurawski analyzes how everyday, nontechnological surveillance of citizens by other citizens in conflict-torn Northern Ireland affects views of other forms of surveillance, as well as such abstract phenomena of everyday life as trust.



Gary T. Marx, a professor emeritus of sociology at the Massachusetts Institute of Technology, is the doyen of surveillance studies in the United States.

Video surveillance managed to catch images of Mohammed Atta and Abdulaziz Alomari, two of the 9/11 hijackers at an ATM in Portland, Me., on September 10, 2001 (left), and the four men who set off bombs on London transit on the day of the bombing, July 7, 2005. Some scholars who study surveillance observe that while such videos allow law enforcement to reconstruct events, they do not prevent such attacks.

David Lyon, director of the Surveillance Project at Queen's University, in Ontario, argues that surveillance has opened up new forms of social control "without democratic participation."

— PETER MONAGHAN

TAKE MY PRIVACY, PLEASE

Some forms of surveillance make us feel secure against crime and harm. The intrusiveness of other forms of monitoring make us feel somehow diminished. But what about reality television — the sort of surveillance to which many people willingly submit for notoriety and prizes?

On a recent Wednesday night, Mark Andrejevic, an assistant professor of communication studies at the University of Iowa, has agreed to share his insights about reality TV with a reporter. He is watching an episode of Beauty and the Geek, a show on the WB network that matches eight comely women (the "beauties") with eight "geniuses" (the "geeks") for laughs, life lessons, and a $250,000 grand prize to be shared by the winning couple.

On tonight's episode, each geek gets $1,500 to spend at Bed, Bath & Beyond (product placement, anyone?) to design and decorate a bedroom. (Later in the show, the beauties will be plunged into the world of computers.)

"There are some pretty sad efforts at interior design," observes Mr. Andrejevic. Indeed, one of the geeks has stapled a teddy bear to a wall.

The exercise seems far removed from the world of surveillance studies. (Although someone might want to keep an eye on the guy with the nail gun.) But the professor suggests that the link to surveillance is not at all distant.

"One of the promised results of willing submission to being watched all the time is the ways in which one learns about oneself, grows, and changes, and finds ways to express oneself," he says. "There's a reflexive element of seeing oneself through the eyes of others."

Cast members of reality shows are not the only ones who willingly submit themselves to surveillance, Mr. Andrejevic points out. We all do it, every day, when we participate in "the interactive information economy" — the world of traceable online and credit-card shopping, cellphones, and cars fitted with GPS devices that can locate you at a moment's notice. "And the way that you're able to express yourself more fully is to allow those commercial entities that are interested in finding out about you to learn more and more about you, to provide you with customized products and services."

In short, he says (as he watches beauties and geeks take turns watching one another via closed-circuit television), the citizen gets to participate in the new, purportedly interactive community and to enjoy its allure.

———

Chronicle of Higher Education, 00095982, 3/17/2006, Vol. 52, Issue 28
Page 13

"Regular consumers and citizens," he says, "are gaining access to all kinds of strategies and techniques for monitoring one another. In some ways, then, they're adopting the model of interactivity that is advanced by commercial and state entities, which is that you interact by submitting information about yourself, in a one-way, nontransparent fashion."

'RIVETING AND DISTURBING'

Among the primary motifs of reality shows is the elimination element, in which contestants are judged by fellow contestants or appointed arbiters or the public itself — all of whom in some way monitor the proceedings. Mr. Andrejevic notes the "standard set of claims that people make when they get kicked off shows like this: 'I didn't make it, but I learned a whole lot about myself. The experience was great. …' We'll get an exit debriefing and see if my prediction is correct."

Eventually one of the contestant couples falters. The denouement unfolds much as Mr. Andrejevic predicted: Tonight's losers are Thais — an affable model who cannot identify the meaning of a "cc" in an e-mail address line — and Tyson, an expert at Rubik's Cube.

In the exit interview, Thais says Tyson has changed and become more sociable. Tyson hopes "that the confidence I've learned here will carry through." Thais, he adds, is "a really smart cookie."

"Watching these shows, it always has that strange feeling of watching an accident — somehow riveting and disturbing at the same time," says Mr. Andrejevic. Such programs cast life as a competition in a way that resonates with the country's prevailing political philosophy, he argues. They hint at a dystopian future, "where a larger proportion of the population is going to go without benefits associated with the social safety net, and instead they can participate in all kinds of competitions to gain some of those forms of support back."

The shows resonate, too, he says, with the political philosophy that says that citizens should look to private industry, and their own resourcefulness, for their survival.

These meditations on Beauty and the Geek bring Mr. Andrejevic back to the idea of surveillance as an invitation to participate. "If you want goods and services delivered to you based on who and where you happen to be, you have to surrender more and more information about yourself," he says. "Taken to the limit, you have to be willing to live in an always-on and always-monitored relationship with the entities that provide those goods and services."

———

After all, he says, "commerce is your friend, and the way you are able to perform it provides you with opportunities. Clinging to privacy is a barrier to unfolding your subjectivity."

Mark Andrejevic, an assistant professor of communication studies at the U. of Iowa: "If you want goods and services delivered to you based on who you are and where you happen to be, you have to surrender more and more information about yourself."

— PETER MONAGHAN

Chronicle of Higher Education, 00095982, 3/17/2006, Vol. 52, Issue 28
Page 15