Move over, Big Brother

Commercialized surveillance is what we should be concerned about. By Mark Williams

Technology and Privacy: The New Landscape
Edited by Philip E. Agre and Marc Rotenberg
325 pages, $25
Massachusetts Institute of Technology Press

Jeremy Bentham (1748–1832), the English philosopher and reformer, is best known for his theory of utilitarianism, with its "hedonic calculus" and argument that "the greatest happiness of the greatest number" should be society's ultimate objective. But Bentham wrote about prison reform as well, and his curious proposal in that arena—the Panopticon—has received renewed attention in recent times.

Prisoners in Bentham's Panopticon were to be isolated in rings of cells, all within sight of a central tower. Unable to see their observers, the prisoners would have to assume they were being watched at all times. This architectural system of social regulation could be applied not only to prisons but to asylums, factories, and apartment complexes as well. In the '70s the French philosopher Michel Foucault revived the Panopticon as a metaphor for the way in which people under ceaseless surveillance internalize social discipline. Lately, some cypherpunks have taken it as a model of how the world would look if there were no electronic privacy from the powers that be.

Technology and Privacy, a collection of essays edited by Philip E. Agre and Marc Rotenberg, has a promising introduction and a first chapter called "Beyond the Mirror World," both written by Mr. Agre. Mr. Agre begins by tracing the evolution of distributed computers able to collect personal information into centralized databases. The present network infrastructure can track particulars of the real world in real time; for clues to what this will eventually mean, Mr. Agre points to separate efforts by California's Air Resources Board and Transportation Department to develop systems for tracking fleets of vehicles with radio transponders.

Mirror, mirror on the wall

The best expression of this database-centered view of computing, Mr. Agre thinks, is the 1991 book *Mirror Worlds* by the computer scientist David Gelernter. "Mirror worlds" are software structures representing entire companies, hospitals, universities, cities, or anything else, and Mr. Gelernter predicts that soon a vast, distributed computer system will contain *a working model of reality*. Mr. Gelernter, a likable fellow, is at pains to explain how his mirror world "isn't snoopware" but is rather a collective enterprise to liberate and empower a democracy of individuals. Yet his book's epilogue enthusiastically speculates that this technological revolution, unlike any previous, may finally force those lazy masses to acquire scientific mental habits or else become disenfranchised information have-nots. One man's technological utopia is another's Panopticon (ironically enough, in 1993 Mr. Gelernter was maimed by a package from the Unabomber).

Mr. Agre, after analyzing what he believes are Mr. Gelernter's questionable assumptions, closes by endorsing privacy-enhancing technologies (PETs). Good enough.

Alas, most of *Technology and Privacy* is not as inspiring as its initial pages. The next contributor reports merely how her team fed audio and video monitoring of the Apple Computer canteen to a Web page; employees were informed that they were being observed. Though a chapter analyzing the broader implications of how people's behavior changes for the mirror world would be valuable, this chapter isn't it. The author rehearses her team's jargon-ridden theories about the experiment—and finishes with the punch line that although privacy is certainly important, it's hard to predict what people will want in 2020.

Next, a Canadian academic gives a history of data-protection laws and says there'll probably be an international standard eventually. A German academic theorizes about PETs. A Washington, D.C., activist warns that privacy rights have become commodities yet expends his strongest criticism on police and government. Likewise, the privacy commissioner in British Columbia advocates limiting government data collection, only to admit at the chapter's end that "what remains problematic is data protection in the private sector."

Such—despite the subtitle *The New Landscape*—are the imaginative limits of *Technology and Privacy*. Contributors offer brief lip service to the fact that Orwellian scenarios of centralized government surveillance are unlikely. Then, because their intellectual toolkits provide little with which to confront the emerging actuality of *private* surveillance, they retreat to the familiar ground of government-citizen relations.

Life in a glass house

Only the last writer, Rohan Samarajiva, in the chapter "Interactivity As Though Privacy Mattered," tries to engage reality. We are entering an era, he observes, in which every time a credit card passes through a supermarket scanner, market researchers' databases will link the cardholder's identity with the bar codes on each purchase of chocolates, contraceptives, or hemorrhoid ointments, correlating it with the buyer's

age, weight, address, marital status, family history, religious affiliations, and whatever else shows up in the electronic deposits of personal data that everybody emits in the network economy. America is becoming a landscape where public spaces and traffic flows are monitored, with license plate numbers retrieved and drivers' addresses and census information analyzed for deeper demographic trends: a continent digitally mapped so that satellite cameras can be trained on almost any tract house or building in any city and the results matched with details about each parcel, down to the location of every gas meter.

The global transition from a predominantly mass production economy to one oriented toward mass customization, Mr. Samarajiva recognizes, creates enormous demand for networks to collect detailed data—mostly from transaction-generated information (TGI)—about customer behavior. Yet, he writes, "the firm knows about the customer, but the customer does not have equivalent information about the firm. . . . The firm extracts information more or less involuntarily in the form of TGI, while the customer has to rely on advertising disseminated by the firm." This is not necessarily the way things have to be.

'The firm knows about the customer, but the customer does not have equivalent information about the firm.'

While mass customization makes more precise customer-marketer interactivity inevitable, Mr. Samarajiva believes that it could be based on either consensual or coercive surveillance. From the perspective of privacy advocates, the underlying economic process and channel proliferation hold potential for good outcomes—if corporations see the benefits of consensual surveillance. Alternately, if customers don't defend their privacy, coercive surveillance will grow entrenched. The prospects for privacy will become dim.

A decade ago, Congress denied the FBI clearance to enter national databases. These days technology makes such privacy legislation irrelevant for the commercial sector. *Everything* is for sale: public records are sold to corporations for hundreds of millions of dollars annually to maintain budget-strapped bureaucracies (Rhode Island makes $9.7 million every year by selling its DMV records). Huge loopholes let corporations ignore the lines between legal and illicit data. If consumers don't act now, this standard will be locked into place.

Something like Mr. Gelernter's mirror world—the aim, perhaps, of all science—is inevitable: what's at stake are citizens' rights in that context.

Mark Williams is a science writer living in Oakland. Write to him at markred@aol.com.