The Surveillance Society: Information Technology and Bureaucratic Social Control

by Oscar H. Gandy, Jr.

Advanced electronic technologies "dramatically increase the bureaucratic advantage" in the workplace, marketplace, and government by enabling—and encouraging—increasingly automatic methods of surveillance of the individual that the U.S. legal system cannot control.

Information has become an essential resource for the bureaucratic management of the global political economy. Perceptive analysts (2, 22, 38) recognize that the real source of growth in both the information work force and the development of information technologies is not to be found in any transformed consumer demand, but in the continually expanding surveillance requirements of multinational corporate enterprise. Indeed, for some observers, "information society" is a misnomer that hides the extent to which industrial societies have in fact become surveillance societies (11).

Surveillance, like propaganda, is a term that has taken on an unfortunate negative connotation. The idea of surveillance brings to mind images of the undercover police agent or counterspy rather than more acceptable images of the journalist, researcher, or communication specialist performing, in Harold Lasswell's term, "the surveillance of the environment." Charles Wright (55) has asked,

what are the consequences of conducting surveillance through the process of mass communications instead of through some alternative system, such as a private intelligence network? That is, what are the results of treating information about events in the environment as items of news to be distributed indiscriminately, simultaneously and publicly to a large, heterogeneous, anonymous population? (p. 17).

In this article we ask, similarly: What are the consequences of conducting surveillance through the system and logic of corporate and state bureaucracies?

Oscar H. Gandy, Jr., is Associate Professor at the Annenberg School of Communications, University of Pennsylvania. The author's work on the project reported in this article was supported in part by a grant from A.T.&T. through the Center for Communications and Information Science and Policy at the University of Pennsylvania. This support made it possible for the author to enjoy the able assistance of Cathy Preston, Csilla Voros, Eleanor Novek, and Jerry Baber.

These bureaucracies treat information about a large heterogeneous population as data to be jealously guarded—shared with other bureaucracies when there is the promise of mutual gain and shared with individuals only under the threat of penalties established by law.

One consequence is an increasing inequality between those who provide and those who gather personal information. By confining their analyses to the structure and performance of markets and regulatory environments, the usual assignments of information inequality—to the "haves" and the "have-nots," the technological elites and the technopeasants, the pedestrians and the wizards—largely miss the point. The inequality that best describes the information age is not the rift between castes or classes but the widening chasm of power between individuals and bureaucratic organizations (33).

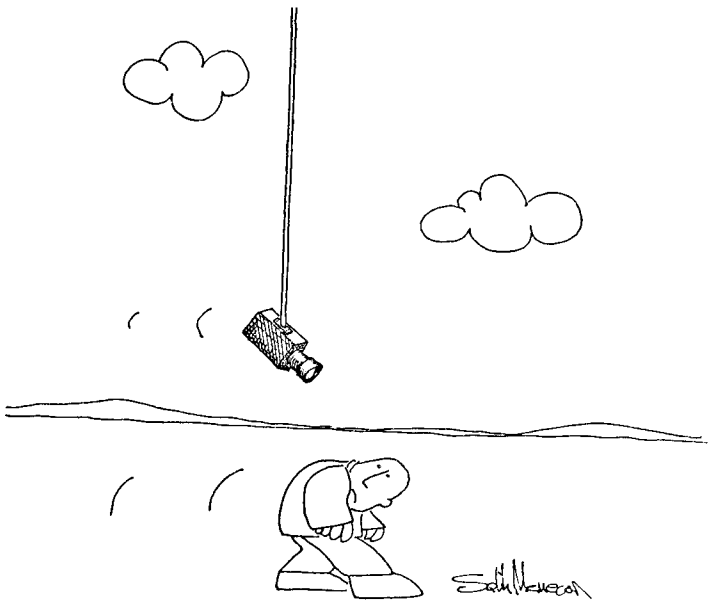
Here we attempt to describe how communications and information technologies are being used to increase the reach and influence of bureaucratic surveillance. Computerization and the speed of telecommunications networks have been combined in ways that dramatically increase the bureaucratic advantage. The current legal system is hopelessly inadequate to the challenge of controlling the "technologies of control" (54).

Modern surveillance technology is an integrated system of hardware and software that includes devices for sensing, measuring, storing, processing, and exchanging information and intelligence about the environment. For the most part the "new" technologies make the pursuit of information through surveillance more extensive, more efficient, and less obtrusive than former methods, because advanced electronics allows innovations not originally designed for surveillance to be integrated into the pool of surveillance resources.

These devices serve a variety of purposes, from noting the presence or absence of persons or objects to determining their identity or status, including their state of mind. Cameras now require little or no light, and microminiaturized versions can be easily hidden from sight; listening devices can hear conversations in rooms many hundreds of yards away; and scientific instruments can examine bodily fluids and genetic material at the molecular level. We include here the scanners that read the Universal Products Code (UPC) on commercial products in the supermarket as well as the infrared detectors that count the number of patrons for museum exhibits. The common quality is that these devices are more sensitive than ever before and overcome previous limits of time, space, and distance in gathering information about individuals (25). Associated technologies also allow for the storage, retrieval, and processing of these data gained through surveillance of the environment.

Increasingly, telecommunications networks allow data to be shared among systems and across distances (32) and among government agencies, contractors, and clients (48, pp. 58–60). The reach and efficiency of such systems allow a virtually unified data base to be created, even though the actual files may reside in the memories of quite distant machines.

Sophisticated analytical software also makes possible the dynamic processing



and display of intelligence based on correlating thousands of discrete bits of information about the targets of surveillance. "Expert systems"—computer software applications that incorporate the expertise of an analyst—are able to process available data, issue diagnoses, and direct the actions of other devices or persons. By reducing the time and cost associated with moving from data gathering to decision making and by centralizing control (36), they make surveillance more efficient. Thus, analysis can estimate the probability that an individual will pursue a particular course of action that either serves the interests of the controller or represents an unacceptable level of risk; the analysis can even suggest where additional data would be necessary (47). The marriage of computers and telecommunications (37) is the major material force in the new technology of surveillance.

The new technologies have transformed the nature of surveillance in important ways. Contemporary surveillance derives from Bentham's early nineteenth-century Panopticon, an architectural design for a prison where inmates were (or would believe that they were) being watched by unseen eyes. The Panopticon was also to be a laboratory for testing approaches to modifying behavior. Through "its preventative character, its continuous functioning, and its automatic mechanisms," the device would ensure desirable conduct (12, p. 206).

Similarly, the new surveillance can be thought of as a form of "remote sensing" where the observer is never seen. Information is processed by unknown, faceless technicians and specialists who have no direct, personal knowledge of or concern for their data subjects. The superior technology available to the sur-

veillance agency enables it to generate intelligence about an individual that even the individual does not possess. For example, remote laboratories that perform blood tests on job applicants may discover the presence of life-threatening diseases about which the individual has had not the slightest warning sign. If the tests have been performed without the subject's consent—such as tests for AIDS in those jurisdictions that bar requirements for HIV testing as a condition of employment—the results may never even be revealed to the individual.

The new surveillance is increasingly automatic and is triggered by the data subject. Thus, a person who enters a parking garage, office, or secure floor using a magnetically striped card initiates the creation of a record noting the date and time of entry and exit. The act of logging on to a computer system begins the documentation of files entered, keystrokes and errors made, and messages sent and received. "Station message detail recorders" on office telephone systems can record the number, time, and duration of all calls placed from any instrument. Advanced audience assessment devices record which television programs are being viewed—or at least, on the basis of their scanned images, who is present in the room. If the system is uncertain, its on-screen display can inquire about who entered or left the room. Individuals participate voluntarily in much of contemporary surveillance, even if not with fully informed consent.

The analysis of surveillance data, too, has become more automatic (26). Cross-matching computer files has become routine in the government provision of services. Eligibility, or "front-end" verification, is used to compare an applicant's file with the files of banks, employers, insurance companies, or others who might provide evidence of unreported resources. Cross-matching might also reveal the absence of matches where they are expected, as in the case of claims for dependent children who do not appear on any school registration lists. Such matches need not be initiated by any particular application but may be the result of a bureaucrat's "hunch" about where evidence of illegality might be found. Illegality is assumed, and all individuals in a particular file are subjected to this "search" without their knowledge or consent. And, as soon as the existence of a new data base becomes known, its potential for providing additional information about a data subject is assessed, and the demand for more matches grows.

Contemporary surveillance is directed toward preventing or avoiding loss or injury, rather than detecting crime that has already occurred. Individuals are no longer brought under surveillance merely to determine whether they have committed a crime; bureaucratic surveillance is initiated more frequently to determine if an individual has even the *potential* to commit a criminal act. And, as we have seen, the definition of criminal behavior may expand as telematics improves the capacity of the system to survey and discipline (47).

For example, Credit Bureau Incorporated, with files on 142 million consumers, offers a service called Delinquency Alert System (DAS). DAS provides a

rating that the creditor can use in deciding whether to extend or limit credit to persons who, though not currently delinquent, might be at risk given the nature of their expenditures and accounts (5). The same kind of predictive models are used to assess the riskiness of assigning bail to persons charged with crimes and the punitive orientation of prospective jurors.

These analytical models generate "types" or classes of persons, rather than specific individuals, and anyone falling within those groups comes under suspicion and hence surveillance. Thus, males of a certain age, skin color, and point of origin have an increased likelihood of being searched, or at least questioned, by customs and security agents at international airports. In the southeastern part of the United States, certain models of automobile have a greater probability of being stopped by police if their drivers are black or Latino. These narcotics interdiction and antiterrorist profiles have their equals in the Internal Revenue Service scans of tax returns and in the routine processing of applications for credit cards. The ostensible purpose is the same—to predict and prevent.

The capacity to predict also provides the opportunity to control. In James Beniger's perspective (4), information technologies are control technologies, which reduce the costs of uncertainty by establishing routines that efficiently "preprocess" and classify, and thereby help to rationalize various activities in the environments of complex, interconnected systems. But his naturalistic model largely ignores the political and economic impact of these modes of control. As state and private bureaucracies seek to control the social environment in which they function, they must also, as John Kenneth Galbraith suggests, plan the behavior of the people within them (15, pp. 39–40). As the power of the corporate bureaucracy grows in relation to individuals and to smaller competitors, it also grows relative to the power of the state (1).

Thus, surveillance that ostensibly predicts and prevents also makes the individual citizen, worker, or consumer the target of bureaucratic control. If, as Frank Webster and Kevin Robins suggest (51, pp. 49–73), information technology is a complex social relation, then its development and spread reflect the design and interests of bureaucracies and, increasingly, the consent and assistance of a "disciplinary state" that contains dissent and opposition from those least well served by the information revolution.

The spread of computerization throughout the bureaucratic infrastructure changes the bureaucracy while it increases the bureaucracy's power relative to other organizations and to the individuals who are its employees, clients, or suppliers. Telecommunications networks extend the advantages of economies of scale and scope that computerization confers on an organization. Under the guise of decentralization and independence, this coordination function reinforces the power and influence of centralized authority (6). The massive scale of transnational operations requires private global networks; meanwhile, the organization can use its oligopsony power to extract discounts and special favors from service providers (37, 39).

Once a network and computerized data base have been established, the marginal cost of adding additional bits of information declines, so large organiza-

tions gather more information and discard less (23). The organization need not have an immediate need or application for any particular item of information its network collects, because storage and access are cheap relative to collection. The nature of multivariate analytical and predictive models is such that information already in storage becomes more valuable as new information is added to the data base.

Because of the monopoly power of corporate bureaucracies and the authority and autonomy of state bureaucracies, the theoretical restraints of the market have little effect on their surveillance activities. Similarly, the peculiar qualities of information (3), including the substantial externalities associated with its collection and use, lead organizations in general (and monopoly firms in particular) to collect more information than is socially optimal. By the same token, because each isolated bit of information on the citizen/consumer has such a seemingly small "privacy cost" and because monitoring the bureaucracy's use of that information has a high cost, individuals are incapable of acting in their own interests. Indeed, because individuals are "contract term takers" (23), and because they are usually required to provide personal information as a condition of service, resistance is perhaps even irrational. Examining information technology as a social relation in three environments—the workplace, the marketplace, and government—shows how the concerns of the individual are increasingly subjected to the unobtrusive powers of bureaucratic surveillance.

Although pre-employment background searches have become routine, it is on the job that surveillance becomes total and continuous. A study by the Office of Technology Assessment (45) notes that "electronic monitoring is only one of a range of technologies used in today's workplace to gather information about the work process or to predict work quality based on personal characteristics of the workers" (p. 12; see also 27). The surveillance of workers in the information age begins well before they enter the office or factory. The growth in pre-employment drug tests (43), psychological screening batteries (18), and searches of credit bureau files and arrest records reflects not only the advances of computer-aided analyses but also the declining costs of collecting, storing, and processing data thought to be relevant to employment decisions.

On the job, in pursuit of greater efficiency in production and management, both large and small employers use computer-based systems to record and compare workers' output against standards or goals and to link their individual responses to changes in the work environment. It is ironic, perhaps, that the sector of the work force under the most complete and continuous surveillance is that which contains the largest contingent of information workers—workers whose very purpose is the collection and processing of data.

The growing importance of telemarketing and the inbound processing of orders and claims for banking, insurance, and investment organizations has increased management's claims that surveillance of the telephone worker is necessary to maintain standards and efficiency. The Communications Workers of America estimates that nearly 15 million telephone workers are being

secretly "bugged," either automatically by an electronic supervisor or by anonymous quality-assessment personnel. These remote supervisors, often located in phone centers hundreds of miles from the workers being observed, listen in on conversations to evaluate how well employees are following the predetermined scripts and how well they are maintaining the appropriate tone and quality of voice (7).

Setting aside concerns about gains in productivity, Andrew Clement's (6) examination of the progress of office automation focuses instead on the exercise of control over the labor process. More than 80 percent of white-collar workers are expected to have computerized work stations by the end of the century, and such systems facilitate the collection and analysis of a variety of work and nonwork activities in the modern office. As higher and higher levels of the organization become connected to the electronic umbilical, it becomes possible "for technical forms of workplace control to be extended to occupational ranks that previously had not been exposed to such techniques" (6, p. 233). The spread of personal computers throughout the office represented something of a temporary loss of this surveillance potential. However, local area networks capable of integrating PCs that use different communications protocols will restore their preferred managerial status as "intelligent terminals."

Surveillance technology in the realm of consumer behavior has the potential to exceed the effects identified for the workplace, because while not everyone is gainfully employed, nearly everyone is an actual or potential consumer. The control of mass consumption involves using information about consumers, including data about the extent to which they have been exposed to persuasive messages, as well as indices of their responsiveness to such appeals. "People meters" represent a shift from measuring households to measuring individuals; some versions, reflecting the primary purpose of assessment, provide ratings of commercials as well as news and entertainment programs. The importance of comprehensive, continuous audience surveillance is reflected in the steady pressure to develop overnight ratings in all television markets and to include estimates of cable and VCR usage in those packages.

Advances in digital communications technologies, especially in terms of their addressability and verifiability (17), allows market research to apply the sophisticated techniques of social science to the surveillance of consumers in order to predict and control their behavior. The preprocessing or classification component of control identified by Beniger (4) finds its contemporary reflection in the sophisticated segmentation of consumer markets on the basis of data gathered from surveys, experiments, and continuous monitoring of the marketplace (10, 14, 29).

Television audiences are classified on the basis of individual interests, needs, and orientations (13) through a technique called geodemographic clustering. The PRIZM target marketing system, developed by the Claritas Corporation, utilizes data collected by the U.S. Census Bureau and numerous other sources of

public and private consumer surveillance to classify each of the nation's 250,000 neighborhoods (52). This preprocessing of a vast, heterogeneous population into one of 40 consumption-related categories or types helps those who plan targeted commercial and political appeals.

The computer facilitates the use of older communications channels to support market research. Just as UPC codes pinpoint the identity of products as they are passed over the laser scanners in the supermarket, similar bar codes identify the consumer who has submitted a coupon received in the mail or pulled out of a magazine. When matched with store price and where it was redeemed, the coupon also helps estimate the price and income elasticity of demand for such goods. The storage capacity of these computers allows lists of such coupon responders to be inexpensively reproduced and sold to others in the business community. Each week, the *Friday Report,* a newsletter of the direct marketing industry, reports on dozens of available lists at prices ranging from $45 to $100 per thousand names.

Kevin Wilson (54) focuses our attention on the home as a site for many computer-based information systems, or "technologies of control." Interactive home networking systems are subject to, if not a direct product of, efforts to "transform human activities into marketable commodities" (p. 9). Their "impact on techniques of public surveillance will be felt most strongly as these systems increase points of contact between client and agency, because there is no practical limit to the types of information which will circulate through interactive systems" (p. 95).

Spiros Simitis, a law professor and Data Protection Commissioner for the West German state of Hesse, takes a similar view of interactive systems (41). Many modern cable systems are already capable of providing a variety of services, from catalogue shopping and data retrieval to the monitoring of fire and burglar alarms. Because use of these services is quickly and efficiently recorded in the system's computer, Simitis concludes that where "anonymity was once the rule, complete transparency now dominates. . . . Videotex is, therefore, further proof of the steady, but often imperceptible, transition in social control from physical coercion to observation and surveillance" (41, p. 729).

The U.S. government is both the single largest user and the greatest supporter of the development of computer and telecommunications systems' surveillance capacities. The federal government operated an estimated 27,000 large mainframe computers in 1985, serving some 173,000 terminals (46). A survey of 12 cabinet-level departments and 13 independent agencies by the U.S. Office of Technology Assessment found 539 records systems, with 3.5 billion records subject to the guidelines of the Federal Privacy Act of 1974.[1] More than half of these systems had been fully or partially computerized by 1985 (44, p. 40).

[1] The Privacy Act, passed in 1974, sought to restrict the collection and sharing of personal information by the federal government to the purposes for which it had been gathered; it was supposed to require the informed consent of the citizen for such use. The Act was passed before computerization of

This massive collection of data does not begin to describe the surveillance activity of the federal bureaucracy, which is also the primary gatherer of social and behavioral statistics. The $3.2 billion estimate of federal government expenditures for information dissemination in fiscal year 1987 provides a sense of the size of the data pool that the government collects or causes to be collected on its behalf (48). Many of these data do not qualify as records under the Privacy Act, as they do not identify individual data persons, but they are no less part of the government's surveillance function.

The Department of Defense is the largest collector and distributor of information within the government. Its surveillance requirements are global, and from time to time it has been actively involved in domestic political surveillance of civilians (9). It is joined by the Central Intelligence Agency, the National Security Agency, and the Federal Bureau of Investigation as major collectors of information used for surveillance. In 1988, for example, the FBI successfully avoided facing restrictions on its "Library Awareness Program," which sought the assistance of librarian-informers in keeping track of foreigners and others who might gain access to information that threatens national security (21).

The Internal Revenue Service is the major civilian collector of personal data within the government. To extend its reach and to improve the ability of its analytical models to identify nonreporters or underreporters, the IRS has sought—occasionally with the consequence of adverse publicity (49)—to use private data bases that contain considerable detail about citizens' expenditures and income.

In response to recommendations of the President's Private Sector Survey on Cost Control (the Grace Commission), politicians suggested establishing federal mandates for performing extensive matching of public and private files to detect fraud, waste, and abuse at the state level. This requirement, which became part of the Deficit Reduction Act of 1984 (PL 98-369), serves as yet another economic spur to adopt practices that have their own economic incentives.

Surveillance systems and techniques are also used to manufacture political consent by manipulating public opinion (28). The skillful provision of information subsidies through a variety of information channels has been shown to influence public policy (16).

The same segmentation and targeting approaches that help to market commercial goods and services are regularly used to market political candidates and positions on policy referenda. A special licensing agreement with Claritas Corporation allows Targeting Systems Incorporated to apply the geodemographic clustering method to political issues (52). PRIZM cluster analysis helps political consultants decide where more data are needed or where it makes

records had become widespread within the government bureaucracy, and it also included a number of exceptions, including a blanket exclusion for what an agency might declare to be a "routine use." These exceptions have become the rule, necessitating the passage of more specific legislation controlling the use of government data bases for matching.

sense to simply ignore the resident population. Concern that the cluster method would be used to win elections appears to have been unfounded, as politicians find the data gathering too expensive for most local campaigns. Instead, "cluster targeting has found a more receptive target among corporate clients attempting to influence public policy and arouse the citizenry" (52, p. 221). With each election and referendum vote, fresh data about the similarity of political behavior within clusters improve the precision of the PRIZM data base.

The bureaucracies of the state and the private corporations have amassed an almost unimaginable technological advantage when compared with the resources of the average individual. Within the sphere of bureaucratic organizations, too, inequality is the rule rather than the exception. The largest firms have the most powerful, sophisticated, and fully integrated systems of surveillance that money can afford. The presence of personal computers in the homes of a few million consumers is no more of a threat to TRW than the presence of even greater number of VCRs and cameras is to CBS. Indeed, as Wilson and others have argued, the spread of such systems increases the potential of surveillance.

It is difficult to gauge the extent to which the U.S. population accepts such disparity in technological systems as the natural, evolutionary, and inevitable consequence of economic growth. Some individual concerns about privacy have surfaced in a variety of national opinion surveys over the years.

A rather narrow search of the Roper Center data base for the years 1975–1986 produced some useful indicators of concern (34). According to Walker Research's Marketing Research Industry Image studies, for example, an increasing share of respondents—between 25 and 28 percent in 1978–1984—agreed that "polls or research surveys are an invasion of privacy."[2] However, an overwhelming majority of respondents (81 percent) in a 1986 study (40) still agreed that "the research industry serves a useful purpose," although this figure represented a slight decline. Indeed, a slightly increased proportion (82 percent) of Americans apparently believed that "polls and research surveys are used to help manufacturers produce better products," while only 44 percent believed that polls and surveys help "manufacturers sell consumers products they don't want or need."

In 1983, under the sponsorship of the Southern New England Telephone Company, the Harris organization surveyed nearly 1,300 telephone households to explore knowledge and opinions about technology and privacy (20). As in previous surveys, the extent of concern about privacy was quite high. Forty-eight percent of respondents were very concerned and 29 percent were some-

[2] This finding is consistent with evidence of the growing number of people who refuse to participate in opinion surveys. The differential rates of survey nonresponse between the United States, Canada, and Britain have been attributed in part to differences in national response to the census from 1930 to 1980 (19).

what concerned about "threats to your personal privacy in America today." While 68 percent agreed that they begin surrendering their privacy when they enter the credit system, nearly the same proportion (67 percent) believed that personal information was being kept in files for purposes unknown to them.

Respondents seemed to have a fairly well developed understanding of how information about their past behavior could be gathered and included in a master file, and 78 percent of those polled indicated that such files would represent an invasion of their privacy. Eighty percent of the respondents also agreed that computers have made it "much easier for someone to obtain confidential personal information about persons improperly." Seventy-seven percent agreed that selling information about a person's credit standing would be a serious invasion of privacy—yet the sale of access to such information is precisely what credit bureaus do. The inconsistency in these responses is also evident in the fact that 80 percent of the respondents claim never to have been the victim of an improper invasion of privacy.

A more theoretically sophisticated study by Eugene Stone et al. (42) found quite distinct differences in attitudes associated with different kinds of organizations likely to threaten individual privacy. Respondents were asked about the extent to which they believed that they themselves, rather than bureaucratic organizations, had control over how information about them would be gathered and used. The data suggest that the more people seem to "value informational privacy the less control they believe they actually have over personal information" (42, p. 464). This is consistent with data reported by Alan Westin (53) that linked concerns about privacy with feelings of alienation and distrust of government and other powerful forces in society. Respondents were more confident about their ability to personally control information relative to employers than to the IRS, insurance companies, credit grantors, law enforcement agencies, or lending institutions.

Privacy legislation has done little to preserve or to extend the rights and freedoms that were envisioned when the laws were initially passed. Bureaucratic practice and the incentives of managers to extend the reach and influence of their agencies have led to the eventual normalization of "exceptions," which soon become the bureaucratic paths around the legislative barriers (11). When a data protection or privacy commission is established, complacent citizens and politicians presume that the problem has gone away. Yet the limited resources and hostile environment such efforts will encounter guarantee that they will lose their edge over time.

In addition, the bulk of legislative action at the federal level has been directed toward government actions, all but ignoring the activities of corporate bureaucracies, which have a far more extensive reach.[3] As the movement

[3] Legislative attempts to preserve privacy in the consumer realm in the United States include efforts to restrict government access to data held in private files. These include the Right to Financial Privacy Act and the Electronic Funds Transfer Act of 1978. Specific acts, concerned primarily with ensuring the accuracy of banking, credit, and employment data held in private records, have emerged (cont'd.)

toward commoditization and privatization spreads and deepens, the need for legislative attention to corporate practices will grow, although "attempts to restore privacy and individual autonomy by dismantling bureaucracies as such are doomed to failure" (30, p. 288).

Even if it weren't for the continued pressure of bureaucratic expansion, much recent legislation that on its face promises to protect the rights of privacy is seriously flawed and serves primarily to legitimate the very assaults the laws were designed to prevent. For example, the Electronic Communications Privacy Act (ECPA) of 1986 (HR 4952) has been heralded as a tremendous success, the result of historic cooperation between government and often-competing industry groups. But while Congress was extending the reach of outdated prohibitions against unwarranted wiretapping to include the emerging digital communications systems, the legislation also considered the disclosure of record content and transactions. The legislative analysis interprets the Act's nondisclosure section (section 2702) as formally establishing the right of those data managers to treat the fact of transaction as information that can then be divulged to third parties. Thus, it further legitimates the use of such transaction information in creating mailing lists, complete with electronic addresses of "persons fitting broad demographic criteria."

James Katz's evaluation of the ECPA (24) finds that the tightening of some restrictions, such as those on unauthorized access, has been accompanied by some weakening of the safety net with regard to government access. This weakening is accomplished by increasing the range of activities that qualify for state surveillance, easing the requirements for gaining court orders, and improving the state's ability to gain access to usage data. Katz also sees the ECPA legislation as explicitly recognizing the economic rationale behind the legitimization of surveillance: "If it could be shown that a technology gives birth to new industries, improves the trade balance, increases industrial efficiency, and creates meaningful jobs, the privacy costs would be more willingly accepted by the polity" (24, p. 362).

Along similar lines, the so-called "Bork Bill," rushed through Congress following an uproar over a newspaper's publication of Supreme Court nominee Robert Bork's video rental records, legitimizes industry practice. The Video Privacy Protection Act (S 2361) is read by some as limiting video stores' ability to rent lists of their customers (21); but the list industry saw the bill as a historic reversal of threatening trends in the struggle for rights in consumer transaction records. In its initial form, the proposed legislation would have required video stores to obtain a customer's expressed consent before renting his or her name to a direct marketer. In its final form, the legislation places the responsibility on customers to indicate that they do not want their names used; otherwise, the rental firms (and, by implication, any other transaction records keepers)

(cont'd.) since the passage of the Privacy Act. Compilations of state and federal privacy laws are published regularly by the *Privacy Journal*. The protection offered by these laws pales in comparison with those recommended by the Council of Europe for its members. For discussion of the Data Protection Convention and the need for its revision, see (8).

may sell or transfer lists of customers who regularly view particular kinds of videotapes. The prohibition from releasing information about which particular titles are viewed is of no significant consequence. In the view of one industry analyst, with the passage of this legislation, "we have built a Congressional endorsement and trade-off which should carry us into the next century" (50).

The legislative burden is placed squarely on the shoulders of citizen-consumers, who generally have only limited awareness of the nature of the list industry and of the opportunities that might be available for them to have their names withdrawn from the lists. National surveys and industry reports suggest that, even though there is growing resentment of "junk mail" and unsolicited telephone calls (31), individuals tend not to request or even to indicate that they would like to have their names removed from lists.

Kevin Wilson (54), extending the analysis of James Rule (35), sees public demand for protection against surveillance weakening at a time when the need for coordination and compliance spurs on its growth. From this perspective, surveillance works through its ability to maintain the internalization of the rules. Legislation that protects against the occasional "abuses" of the surveillance merely provides a social justification for its extension in this "improved" form.

Other legislation that specifically addresses the problems of data sharing fails to take into account the changing nature of U.S. industry. While there may continue to be some restrictions on sharing customer lists between organizations, it would be unimaginable to think that such restrictions would apply *within* firms. Vertical integration and horizontal conglomeration are creating a structure in which quite diverse organizations under the same corporate umbrella can be expected to collect, process, and share internally quite comprehensive information about individuals gleaned from their transaction records. Thus, a model conglomerate of the future will have banking and financial services, credit cards, travel and insurance, and the traditional automotive and consumer retail service records. In addition, it will support an expanding line of entertainment and information businesses, from cable television and videocassette rental (from automatic kiosks) to videotex, electronic mail, and data base gateway services. The possibilities for cross-marketing on the basis of information available to such a firm stagger the imagination—and would be absolutely invisible to the majority of consumers.

Finally, existing legislation uniformly limits the reach of data protection to "individually identifiable information." Such restrictions provide no limits on the collection, distribution, and use of information about "groups" of any size or definition beyond those that have won some degree of protection through political action (e.g., blacks, women, the elderly). Thus, the characteristics of communities or neighborhoods, defined in terms of five-digit zip codes, have no limits in privacy claims. On the basis of indices developed through "anonymous" data aggregation, geodemographic targeting (52) can proceed unabated to "redline" particular communities as being ineligible for investment, unwise for travel, and unlikely as prospects for political mobilization. Economic, social, and political discrimination simply take on new forms as they grow and spread.

What hope is there for resistance to the spread of surveillance? Priscilla Regan (33) suggests that, ironically, "liberal democracies, whose *raison d'être* is the protection of the individual, are rendered virtually impotent in the face of bureaucratic power" because their institutions were designed at a time when bureaucratic power did not exist (p. 360). But to the extent that reports of public sentiment reflect a genuine understanding of and resentment toward the growing disparity in power that is facilitated and extended by surveillance, there is always the potential for resistance. Resistance may be mobilized in response to well-publicized cases of abuse, or it may come in response to the reemergence of a "literature of alarm" (33, p. 24) like that which accompanied the dramatic spread of computerization throughout the government bureaucracy in the 1960s and 1970s. The potential for resistance is always present, and the rather high level of awareness and concern suggests that it rests just beneath the surface, waiting to be released.

References

1. Adams, Walter and James W. Brock. *The Bigness Complex: Industry, Labor, and Government in the American Economy.* New York: Pantheon Books, 1986.
2. Arriaga, Patricia. "Towards a Critique of the Information Economy." *Media, Culture & Society* 7, 1985, pp. 271–296.
3. Babe, Robert E. "Information Industries and Economic Analysis: Policymakers Beware." In Oscar Gandy, Jr., Paul Espinosa, and Janus Ordover (Eds.), *Proceedings from the Tenth Annual Telecommunications Policy Research Conference.* Norwood, N.J.: Ablex, 1983, pp. 123–136.
4. Beniger, James R. *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge, Mass.: Harvard University Press, 1986.
5. "Changes Affecting Credit Bureaus." *Privacy Journal* 14(7), May 1988, p. 11.
6. Clement, Andrew. "Office Automation and the Technical Control of Information Workers." In Vincent Mosco and Janet Wasko (Eds.), *The Political Economy of Information.* Madison: University of Wisconsin Press, 1988, pp. 217–246.
7. Communications Workers of America. *Fact Sheet: Secret Monitoring in the Workplace.* Washington, D.C.: CWA, 1987.
8. Council of Europe. *New Technologies: A Challenge to Privacy Protection?* Strasbourg: Council of Europe, 1989.
9. Donner, Frank J. *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System.* New York: Knopf, 1980.
10. Engel, James F., Henry Fiorillo, and Murray A. Cayley (Eds.). *Market Segmentation: Concepts and Applications.* New York: Holt, Rinehart & Winston, 1972.
11. Flaherty, David H. "The Emergence of Surveillance Societies in the Western World: Toward the Year 2000." *Government Information Quarterly* 5(4), 1988, pp. 377–387.
12. Foucault, Michel. *Discipline and Punish: The Birth of the Prison.* New York: Random House, 1977.
13. Frank, Ronald E. and Marshall G. Greenberg. *The Public's Use of Television: Who Watches and Why.* Beverly Hills, Cal.: Sage, 1980.

14. Frank, Ronald, William Massey, and Yoram Wind. *Market Segmentation.* Englewood Cliffs, N.J.: Prentice-Hall, 1972.

15. Galbraith, John Kenneth. *Economics and the Public Purpose.* Boston: Houghton Mifflin, 1973.

16. Gandy, Oscar H., Jr. *Beyond Agenda Setting: Information Subsidies and Public Policy.* Norwood, N.J.: Ablex, 1982.

17. Gandy, Oscar H., Jr., and Charles E. Simmons. "Technology, Privacy and the Democratic Process." *Critical Studies in Mass Communication* 3(2), June 1986, pp. 155–168.

18. Gardner, Susan. "Wiretapping the Mind: A Call to Regulate Truth Verification in Employment." *San Diego Law Review* 21(2), March 1984, pp. 295–323.

19. Goyder, John and Jean Leiper. "The Decline in Survey Response: A Social Values Interpretation." *Sociology* 19(1), February 1985, pp. 55–71.

20. Louis Harris and Associates. "The Road After 1984: The Impact of Technology on Society." Study conducted for Southern New England Telephone for presentation at the Eighth Annual Smithsonian Symposium, December 1983.

21. "In Congress." *Privacy Journal* 14(11), October 1988, p. 7.

22. Jonscher, Charles. "Information Resources and Economic Productivity." *Information Economics and Policy* 1, 1983, pp. 13–35.

23. Jussawalla, Meheroo and Chee-Wah Cheah. *The Calculus of International Communications.* Littleton, Colo.: Libraries Unlimited, 1987.

24. Katz, James E. "US Telecommunications Privacy Policy: Socio-Political Responses to Technological Advances." *Telecommunications Policy,* December 1988, pp. 353–368.

25. Marx, Gary T. *Under Cover: Police Surveillance in America.* Berkeley: University of California Press, 1988.

26. Marx, Gary T. and Nancy Reichman. "Routinizing the Discovery of Secrets: Computers as Informants." *Software Law Journal* 1(1), Fall 1985, pp. 95–121.

27. Marx, Gary T. and Sanford Sherizen. "Monitoring on the Job: How to Protect Privacy as Well as Property." *Technology Review,* November/December 1986, pp. 63–72.

28. Meadow, Robert G. (Ed.). *New Communication Technologies in Politics.* Washington, D.C.: Washington Program of the Annenberg School of Communications, 1985.

29. Meyers, James H. and Edward M. Tauber. *Market Structure Analysis.* Chicago: American Marketing Association, 1977.

30. Moore, Barrington, Jr. *Privacy: Studies in Social and Cultural History.* Armonk, N.Y.: M. E. Sharpe, 1984.

31. Nadel, Mark S. "Rings of Privacy: Unsolicited Telephone Calls and the Right of Privacy." *Yale Journal on Regulation* 4, 1986, pp. 99–128.

32. Pacific Bell. *Pacific Bell's Response to the Intelligent Network Taskforce Report.* Sacramento, Cal.: Pacific Bell, 1988.

33. Regan, Priscilla. "Public Use of Private Information: A Comparison of Personal Information Policies in the United States and Britain." Unpublished doctoral dissertation, Cornell University, Ithaca, New York, 1981.

34. Roper Center for Public Opinion Research. University of Connecticut, Storrs. Search completed for the author on November 2, 1987.

35. Rule, James B. *Private Lives and Public Surveillance: Social Control in the Computer Age.* London: Allen Lane, 1973.

36. Rule, James, Douglas McAdam, Linda Stearns, and David Uglow. "Documentary Identification and Mass Surveillance in the United States." *Social Problems* 31(2), December 1983, pp. 222–234.

37. Schiller, Dan. *Telematics and Government.* Norwood, N.J.: Ablex, 1982.

38. Schiller, Dan. "How to Think About Information." In Vincent Mosco and Janet Wasko (Eds.), *The Political Economy of Information.* Madison: University of Wisconsin Press, 1988, pp. 27–43.

39. Schiller, Herbert I. *Information and the Crisis Economy.* Norwood, N.J.: Ablex, 1984.

40. Schleifer, Stephen. "Trends in Attitudes Toward and Participation in Survey Research." *Public Opinion Quarterly* 50, 1986, pp. 17–26.

41. Simitis, Spiros. "Reviewing Privacy in an Information Society." *University of Pennsylvania Law Review* 135, 1987, pp. 707–746.

42. Stone, Eugene, H. Gueutal, D. Gardner, and S. McClure. "A Field Experiment Comparing Information-Privacy Values, Beliefs and Attitudes Across Several Types of Organizations." *Journal of Applied Psychology* 68(3), 1983, pp. 459–468.

43. "Testing for Drug Use in the American Workplace: A Symposium." *Nova Law Review* 11(2), Winter 1987.

44. U.S. Congress. Office of Technology Assessment. *Electronic Records Systems and Individual Privacy. OTA-CIT-296.* Washington, D.C.: U.S. Government Printing Office, June 1986.

45. U.S. Congress. Office of Technology Assessment. *The Electronic Supervisor: New Technologies, New Tensions. OTA-CIT-333.* Washington, D.C.: U.S. Government Printing Office, September 1987.

46. U.S. Congress. Office of Technology Assessment. *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information. OTA-CIT-310.* Washington, D.C.: U.S. Government Printing Office, October 1987.

47. U.S. Congress. Office of Technology Assessment. *Criminal Justice. New Technologies and the Constitution. OTA-CIT-366.* Washington, D.C.: U.S. Government Printing Office, 1988.

48. U.S. Congress. Office of Technology Assessment. *Informing the Nation: Federal Information Dissemination in an Electronic Age. OTA-CIT-396.* Washington, D.C.: U.S. Government Printing Office, October 1988.

49. U.S. Congress. Senate. Committee on Governmental Affairs. Hearing, June 6, 1984. *Computer Matching: Taxpayer Records.* Washington, D.C.: U.S. Government Printing Office, 1984.

50. "Video Privacy Protection Act of 1988." *Friday Report,* November 11, 1988, p. 1.

51. Webster, Frank and Kevin Robins. *Information Technology: A Luddite Analysis.* Norwood, N.J.: Ablex, 1986.

52. Weiss, Michael J. *The Clustering of America.* New York: Harper & Row, 1988.

53. Westin, Alan, Louis Harris and Associates, and Sentry Insurance. *A National Opinion Research Survey of Attitudes Toward Privacy.* Stevens Point, Wisc.: Sentry Insurance, 1979.

54. Wilson, Kevin G. *Technologies of Control: The New Interactive Media for the Home.* Madison: University of Wisconsin Press, 1988.

55. Wright, Charles R. *Mass Communication: A Sociological Perspective.* New York: Random House, 1959.