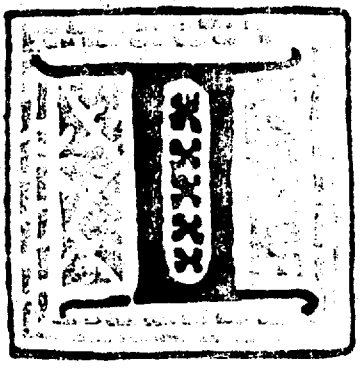
Privacy & Technology



BY GARY T. MARX

IN THE UNITED STATES we recently celebrated the two-hundredth anniversary of the Constitution, a document that extended liberty. Unfortunately, the bicentenary of another important document that restricted liberty has gone virtually unnoticed — the 1791 publication of Jeremy Bentham's *Panopticon; or, the Inspection House.*

Bentham offered a plan for the perfect prison, in which there would be constant inspection of both prisoners and keepers. His ideas helped give rise to the maximum-security prison. Recent developments in telecommunications, along with other new means of collecting personal information, give Bentham's image of the panopticon great contemporary significance.

The stark situation of the maximum-security prison can help us understand societal developments. Many of the kinds of controls and information-gathering techniques found in prison specifically and the criminal justice system more broadly are diffusing into our culture. We may well be on the road to becoming a "maximum-security society." Such a society is transparent and porous. Information leakage has become rampant; indeed, it is hemorrhaging. Barriers and boundaries — be they distance, darkness, time, walls, windows, or even skin — that have been fundamental to our conceptions of privacy, liberty, and individuality are giving way.

In such a society, actions, feelings, thoughts, pasts, and even futures are made visible — often without the individual's will or knowledge. The line between the public and the private is being obliterated; we are under constant observation, everything goes on permanent record, and much of what we say, do, and even feel may be known and recorded by others whom we do not know — whether we will this or not and even whether we know about it or not. Data in many different forms and coming from widely separated geographical areas, organizations, and time periods can be merged and analyzed easily.

As the technology becomes ever more penetrating and intrusive, it becomes possible to gather information with laserlike specificity and spongelike absorbency. If we visualize the information-gathering process as a kind of fishing net, then the net's mesh has become finer and the net wider.

Just as free association led to discovery of the unconscious, new techniques reveal bits of reality that were previously hidden or contained no informational clues. When their privacy is invaded, people are in a sense turned inside out, and what was previously invisible and meaningless is made tangible and significant.

It is easy to get carried away with science-fiction fantasies about things that might happen. But we need not wait for the widespread use of videophones, paperless electronic safety-deposit boxes, wafer-thin portable personal communications devices, satellite monitoring of individuals via implanted transmitters, or DNA fingerprinting and other forms of biometric monitoring to note profound changes in the ease of gathering personal information. Consider the following:

A college student secretly videotaped sexual encounters with a girlfriend. After breaking up with her, he played the tape for members of his fraternity. She learned of this and was victorious in a civil lawsuit, although no criminal statute had been violated.

Teachers in a school lounge were complaining about their principal,

Gary T. Marx is a professor of sociology at M.I.T. His latest book is* Undercover: Police Surveillance in America *(University of California Press, 1988). This piece is excerpted from a longer article published in* The World and I, *September 1990.
—Howard Rheingold

when one jokingly said, "Be careful, the room might be bugged." Just then they spotted a transmitter in the ceiling, which in fact had been hidden there by the principal.

During a toy manufacturer's television ad, a clown asked children to place their telephone receivers in front of the TV. The studio then broadcast dialing tones that called an 800 number, which resulted in kids dialing the number. The 800 number called had automatic number identification service and recorded the children's phone numbers. The purpose was to create marketing lists.

A friend went on vacation. On returning he had only one message on his answering machine. Shortly after his departure, a synthesized voice "interviewer" had called to ask if he would consent to being interviewed. Since he did not hang up, the system assumed he had agreed to be interviewed and proceeded to ask him a series of questions, pausing after each to let him answer. The interview consumed the full length of the answering machine's tape. In several cases citizens have won lawsuits because during an emergency, an automated dialer had captured their line and could not be disconnected, making it impossible to dial 911.

The line between the public and the private is being obliterated; we are under constant observation, everything goes on permanent record, and much of what we say, do, and even feel may be known and recorded by others whom we do not know — whether we will this or not and even whether we know about it or not.

In Iowa, a woman overheard a neighbor's cordless-phone conversation on her FM radio. She was suspicious of the call and informed police. They instructed her to continue to listen and to record his conversations, all without a warrant, which she did for more than a year. The Supreme Court has ruled that such eavesdropping is permissible.

A variety of personal communication devices, such as cordless and cellular phones and room monitors for infants, can be intercepted easily (and often legally) by scanners, FM radios, and older TV sets with UHF channels. Cordless phones using the same frequency may also pick up wireless communication. Speakerphones may amplify communication. A conversant can never be sure who is listening. In a recent example President Bush was unaware that his off-the-cuff remarks were overheard by a large audience listening in via a speakerphone.

Work monitoring has been taken to new heights, or depths, depending on your point of view. Quantity of keystroke activity, number of errors and corrections, speed of work, and time away from the computer can be measured. Programs such as CTRL and SPY permit remote secret monitoring of a target's personal computer use when his terminal is attached to a larger system. A permanent record of the intercepted terminal's input and output can be made. There is also the possibility of "initial screen repaint," which permits the watcher to see what was on the target's screen before the SPY program was activated. The headsets used by telephone reservationists can be converted to microphones to permit remote monitoring of all office conversation by a supervisor many floors, or even miles, away.

Home phones can be made "hot on the hook": An "infinity transmitter," whether attached to a telephone or part of an answering machine, converts the phone into a microphone. The individual who dials in (the phone does not ring) is able to listen to what is being said in the room.

The US commissioner of immigration has proposed a nationwide computer system to verify the identities of all job applicants. An FBI advisory board recently recommended putting the names of those suspected of (but not arrested for) crimes into a nationally accessible database, as well as the names of the friends and associates of known criminals. The director of the FBI rejected the proposal. Yet pressures to create such national databases are strong.

Marketing researchers are gathering ever more detailed data and carrying out increasingly fine-grained analysis. For example, supermarkets use the itemized bills made possible by bar coding to collect unprecedented information about consumers. Such information (when combined with the personal data consumers provide for checkcashing privileges) is easy to analyze and sell. There is often more to mailed promotional coupons than meets the eye — "invisible" personal data (name, address and other demographic information) may be in the bar code or elsewhere. The behavior of customers who agree to use "frequent shopper cards" is monitored closely, and it will be possible to market directly to households, using

coupons to steer them toward products with higher profit margins. Consumer behavior also can be linked to exposure to specific ads seen on cable television. Persons on the same block watching the same channel may receive different versions of the ad being tested.

Lotus Corporation proposed a new product called "Marketplace," to be available at retail software stores. Its database contained information such as name, address, age, gender, marital status, and estimates of income, lifestyle, and buying habits of 80 million households. The 120 million consumers contained in the database were not asked if they wished to have their personal transactional information treated as a commodity; they would not have been compensated for its sale, nor could corrections easily have been made. The product was withdrawn after massive public protest.

It is easy to imagine how marketing lists might be misused. Purchasers of pregnancy-testing kits may receive solicitations from pro- and anti-abortion groups, or from sellers of birth-control products and diaper services. Purchasers of weight-loss products or participants in diet programs may be targeted for promotional offers from sellers of candy, cookies and ice cream, or, conversely, those whose purchases of the latter exceed the average may receive offers for weight-loss products and services. Subscribers to gay and lesbian publications may be targeted by religious and therapeutic organizations, or face employment denials, harassment, and even blackmail. Frequent travelers and those with multiple residences may receive solicitations from sellers of home-security products, and such lists would be a boon to sophisticated burglars. A list of tobacco users might be of interest to potential employers and insurance companies. A list of those with credit troubles and excessive indebtedness would certainly be of interest to promoters of scams that promise to help people obtain credit cards or get out of debt. A cynic might even hypothesize that such a list would be used by promoters of alcoholic beverages, sweepstakes advertising, and gambling junkets.

THE PREVIOUS EXAMPLES raise a variety of troubling issues: injustice, intrusion, denial of due process, absence of informed consent, deception, manipulation, errors, harassment, misuse of property, and lessened autonomy. But running through most of the examples is the central issue of privacy, as it relates to the control of personal information.

Given these examples and potential problems, it is not surprising that in 1989 half the population thought new laws were needed to protect personal privacy. Yet in a country fascinated by technology, committed to free enterprise and freedom of speech, and concerned over declining productivity, AIDS, crime, drugs, and terror, there are also contrary voices.

Those unconcerned about privacy remind us that we live in an open society that believes that visibility in government brings accountability. With respect to individuals, a valued legacy of the 1960s is personal openness and honesty. The only people who worry about privacy are those who have something to hide. Right?

A response to privacy concerns, expressed by some industry spokespersons, columnists, and citizens, is simply, "So what? Why worry?" In their view, these technologies fill deeply felt needs. A host of arguments is offered to bolster their position: We increasingly live in a world of strangers, rather than in homogeneous rural communities where all residents know each other. The Supreme Court in the *Katz* decision has said that privacy was protected only when it could be reasonably expected. Technology changes and social expectations can't remain static. With more powerful technologies we can reasonably expect less and less, and hence privacy must become more restricted. After all, they say, most so-called privacy invasions are not illegal, and given the free market, one can buy technologies to prevent privacy invasion. For that matter, personal information is just a commodity, to be sold like any other. Companies have an obligation to stockholders to make money. Protecting privacy is expensive and can deter innovation.

Consumers, too, are demanding personalized and customized services. Mass marketing is inefficient, and economic viability requires the "pinpoint" or "segmented" marketing that computer analysis now makes

possible by using "point-of-sale" information. It is up to government to use whatever means it can to be more efficient and to find the guilty and protect the innocent.

Those unconcerned about privacy remind us that we live in an open society that believes that visibility in government brings accountability. With respect to individuals, a valued legacy of the 1960s is personal openness and honesty. The only people who worry about privacy are those who have something to hide. Right?

IT HAS BEEN SAID that a civilization's nature can be seen in how it treats its prisoners; it might also be seen in how it treats personal privacy.

Noting the social functions of privacy certainly is not to deny that privacy taken to an extreme can be harmful. Nor should the right to privacy infringe on other important values, such as the public's right to know and the First Amendment guarantees.

Unlimited privacy is hardly an unlimited good. It can shield irresponsible behavior — protecting child- and spouse-abusers, unsafe drivers, and money-launderers. Taken too far, it destroys community. Without appropriate limitations it can trigger backlash, as citizens engage in unregulated self-help and direct action. The private subversion of public life carries dangers, as does the public intrusion into private life.

Contemporary information-extractive technologies can, of course, protect liberty, privacy, and security. Without the incriminating tapes secretly recorded by President Nixon, Watergate would have remained a case of breaking and entering; without the Xerox machine, the Pentagon Papers might never have reached the public; and without the backup computer records kept in NSC files that Oliver North thought he had erased, we would know far less about the Iran-Contra affair. Aerial surveillance can monitor compliance with pollution standards and help verify arms-control treaties. Tiny transmitters can help locate lost children or hikers caught in an avalanche. Devices that permit firefighters to see through smoke may save lives, and remote health monitors can protect the elderly living alone (in one type, an alarm is sent if a day goes by without the refrigerator being opened).

But elements of Greek tragedy are present: the technology's unique power is also its tragic flaw. What serves can also destroy, absent increased public awareness and new public policies.

An important example of the kind of principles and policies needed is the Code of Fair Information developed in 1973 for the U.S. Department of Health, Education, and Welfare. The code involves five principles:

- There must be no personal-data record keeping whose very existence is secret.
- There must be a way for a person to find out what information about him is in a record and how it is being used.
- There must be a way for a person to prevent information about himself that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for a person to correct or amend a record of identifiable information about himself.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

These ideas might be built upon. Ways to do so include establishing a principle of *minimization*, such that only information directly relevant to the task at hand is gathered; a principle of *restoration*, such that in a communications-monopoly context, those altering the privacy status quo should bear the cost of restoring it; a *safety net* or *equity* principle, such that a minimum threshold of privacy is available to all; a principle of *timeliness*, such that data are expected to be current and information that is no longer timely should be destroyed; a principle of *joint ownership of transactional data*, such that both parties to a data-creating transaction must agree to any subsequent use of the data and must share in any gains from its sale; a principle of *consistency*, such that broad ideals rather than specific characteristics of a technology determine privacy protection; and a principle of *redress*, such that those subject to privacy invasions have adequate mechanisms for discovering and being compensated for violations.

IT IS NOT a foregone conclusion that developing technology will reduce the power of the individual relative to large organizations and the state, although the forces favoring this outcome tend to be stronger than those opposing it. Schools and religious organizations should deal more directly with the individual's rights with respect to means such as third-party records, computer dossiers, drug testing, and the polygraph. It is important that citizens react to invasions of privacy by questioning organizations, rejecting assertions such as "the computer says" or "that is the policy." Why is it the policy? What moral and legal assumptions underlie it? What alternatives are there? How were the data gathered? How are they protected and used?

It is also important that the technology be demystified and that citizens not attribute to it nonexistent powers. There is a chilling danger in the myth of surveillance, and when tech-

nologies are revealed to be less powerful than authorities claim, legitimacy declines. There should be truth in communications policies, just as we have truth in advertising and loan policies. The potentials and limits of the technology must be understood.

There are a number of steps that individuals can take to protect privacy:

• Don't give out any more information than is necessary. You are legally required to give out your social-security number in only a few instances. Don't answer questions that seem irrelevant to the issue at hand. (For example, you may refuse to give your phone number when making a credit-card purchase, or family and income information when filling out a warranty card.)

There should be truth in communications policies, just as we have truth in advertising and loan policies. The potentials and limits of the technology must be understood.

• Don't say things over a cellular or cordless phone or baby monitor that you would mind having overheard by strangers.

• Ask your bank to sign an agreement that it will not release information about your accounts to anyone lacking legal authorization. It should state that in the event of legal authorization, the bank will notify you within two days.

• Obtain copies of your credit, health, and other records and check for accuracy and currency. You are entitled to know what is in many records and, if you dispute the information, to add your version. Credit records can be obtained from TRW, Equifax, and Trans Union. Medical records can be obtained from the Medical Information Bureau (a databank maintained by 800 insurance companies), Box 105, Essex Station, Boston, MA 02112.

• If you are refused credit, a job, a loan, or an apartment, ask why. There may be a file with inaccurate, incomplete, or irrelevant information.

• If you think you are being investigated by a federal agency or believe the agency has a file on you, submit a Freedom of Information Act request asking to see the file.

• If you think your telephone is tapped or a bug is being used and you find evidence of eavesdropping equipment, contact the police and an attorney. Make use of technologies that can protect your privacy, such as an answering machine.

• Realize that when you respond to telephone or door-to-door surveys, the information will go into a databank. The only federal survey that most persons are legally obliged to answer is the U.S. Census.

• When you purchase a product or service and file a warranty card or participate in rebate or inventive programs, your name may well be sold to a mailing-list company. Ask that it not be circulated.

The Privacy Protection Act of 1974 refers primarily to actions at the federal level and tends to exclude state, local, and private-sector activities. A major failing of the Privacy Act is weak-to-nonexistent discovery and enforcement mechanisms. It is unrealistic to expect most individuals to discover violations, given the hidden and complex nature of much data collection and exchange. The means of locating violations and enforcing standards needs to be strengthened. However, the Office of Management and Budget has given this task a low priority.

The Fair Credit Reporting Act offers no recovery if a consumer is hurt by a technically accurate but misleading report. It is important that there be provision for injunctive relief for damages for persons who suffer intangible harm as a result of privacy invasion and that incentives be created that will increase compliance with the legislation we do have.

Unlike many European countries, the United States does not attempt to regulate data collection. Most protections pertain to how data are treated once they are collected. The First Amendment and concern over creating another regulatory bureaucracy partly explain this situation, but as a consequence, citizens are on their own in discovering and bringing action when their rights are violated and data collectors are given a free hand in gathering information. Given the low visibility of many violations and citizens' lack of knowledge of their rights, laws here are underenforced.

A variety of new federal, state, and local initiatives are needed. Among the promising federal legislation introduced, though not passed, as of 1990 are a bill to extend the protections of the Fair Credit Reporting Act to tenant-screening services; a bill to require a periodic audible beep on phones being monitored; a bill to extend the warrant protection of aural surveillance to video; and a bill to eliminate single-party-consent eavesdropping (a major loophole) so that all parties to a recorded conversation would have to agree.

While the Constitution has implications for privacy in a number of places (in the First, Third, Fourth, Fifth, and Fourteenth Amendments, among others), there is no explicit amendment guaranteeing privacy. States such as California

and Pennsylvania have such protections. The United States might emulate countries such as Switzerland, Sweden, Italy, and Portugal by drafting a constitutional amendment protecting privacy. The challenge is to draft it in a general enough way to protect what needs to be protected, without creating a statute whose vagueness shelters things the public interest requires to be revealed. That such a law might be largely symbolic would not detract from its significance.

With respect to information-gathering technology, we are now in the twilight zone that Justice William O. Douglas wrote about in arguing that the protection of our basic values is not self-executing:

"As nightfall does not come at once, neither does oppression. In both instances, there is a twilight when everything remains seemingly unchanged. And it is in such twilight that we all must be most aware of change in the air — however slight — lest we become unwitting victims of the darkness. One could as well argue that we are in a sunrise zone, and that we must be aware of change in the air in order to insure that we all profit from the sunshine. But for this to happen the technology must be bounded by increased public awareness, responsible corporate and government behavior, and new laws and policies." ❦

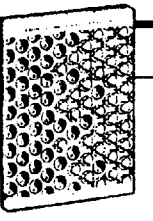
From Satori to Silicon Valley

Theodore Roszak, the man who coined the word and the idea "counterculture," has come out with an eloquently written, tightly argued little book that brings together the counterculture of the sixties with the cyberculture of the seventies and eighties. Originally delivered as the 1985 Fine Lecture at San Francisco State University, ***From Satori to Silicon Valley*** *has all the advantages of an oral presentation: not too long, not freighted with dozens of footnotes, yet offering a clear vision of what ties together the psychedelic and visionary impulses of the Haight-Ashbury and the high-tech thrust of computer culture. Anyone interested in the genesis of Bay Area visionary culture and/or computers should read this book. If you're an uncritical flagwaver for the digital revolution, be forewarned: though not as devastating as Roszak's* ***Cult of Information****, this book paints a somber picture of what became of hippie and hacker ideals as the world of international business absorbed them into its vastly older and more powerful domains. In the struggle between what Roszak calls the "reversionaries" — back to nature and the organic way, down with the military-industrial complex! — and the "technophiles" — better living through chemistry and the digital solution to world problems! — one side won and the other lost. We are living with the consequences of these victories and defeats right now, and will be for years to come.*

—Arthur Chandler

•

It was an attractive hope that the high technology of our society might be wrested from the grip of benighted forces and used to restore us to an idyllic natural state. And for a brief moment — while the music swelled, and the lights flashed, and the dope cast its spell — it looked like the road forward to many bright spirits. But ultimately — and really in very short order — the synthesis crumbled, and the technophiliac values of the counterculture won out. They are, after all, the values of the mainstream and the commanding heights, forces that have proved far more tenacious than most members of the counterculture guessed.



From Satori to Silicon Valley
Theodore Roszak, 1986; 60 pp.
$3.95 ($5 postpaid) from Lexikos Publishing, P. O. Box 296, Lagunitas, CA 94938; 415/488-0401
(or Whole Earth Access)

Tough Questions • Student Pugwash USA

In 1957, Albert Einstein and Bertrand Russell called upon the world's scientists and citizens to "learn to think in a new way." To that end, a conference was held in Pugwash, Nova Scotia, bringing together academics and policy advisers to propose ways to curb the nuclear arms race. Student Pugwash USA (SPUSA) draws its inspiration from the Pugwash Conferences. Where the original Pugwash Conferences concentrated on nuclear weapons, SPUSA takes a broader view, providing high-school and university students and recent graduates with educational programs organized around understanding the social and ethical implications of technology. ***Tough Questions*** *is SPUSA's quarterly publication.*

—Howard Rheingold

•

Student Pugwash USA programs address the fact that science and technology are shaping the world in increasingly profound ways. We recognize that if society is to avoid thoughtless applications of technology in the future, it is first critical to train young people to consider the implications of their decisions. Scientists and engineers should be educated about the effects their work will have on society, while policy makers should be prepared to analyze and shape the course of technology policy. Perhaps most importantly, citizens — both young and old — must feel that they have a right and a responsibility to join with experts in addressing the world's most pressing problems.

Tough Questions
Free from Student Pugwash USA, 1638 R Street NW/Suite 32, Washington, DC 20009-6446; 202/328-6555

SPECIAL INAUGURAL REPRINT ISSUE: INFORMATION ENVIRONMENT TOOLS AND IDEAS Whole Earth Review Dedicated to the Incoming Administration 20 January 1996 - Link Page

Previous	Reclaiming Our Technological Future (Winter 1991)
Next	Genes, Genius, and Genocide (Winter 1991)

Return to Electronic Index Page