IMPACT
ASSESSMENT
BULLETIN

VOLUME 7, NO. 1, 1989

PRIVACY AND THE HOME: THE KING DOESN'T HAVE TO ENTER YOUR COTTAGE TO INVADE YOUR PRIVACY

Gary T. Marx*

"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 must be most aware of change in the air – however slight – lest we become unwitting victims of darkness" – Justice William O. Douglas.

In the auspicious year of 1776, William Pitt wrote: "The poorest man may, in his cottage, bid defiance to all the forces of the crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his force bares not to cross the threshold of that ruined tenement" (Flaherty, 1972).

Pitt's oft-quoted words have become a rallying cry for defenders of personal liberty. But what would Pitt write today if he were to look in on the United States? Were he to restrict himself to the kinds of blunt intrusions that could occur in his day – a door broken down or an agent of the King searching a desk, he would have to conclude that the home has become an even greater bulwark of liberty. But if he were to focus on other kinds of searches, I think his assessment would be very different.

What might surprise Pitt and later observers such as George Orwell is that one could have a society where significant inroads were made on privacy, liberty, and autonomy, even in a relatively nonviolent environment

*The author is professor of Sociology, Massachusetts Institute of Technology. Work on this paper was done as a Fellow at the Center for Advanced Study in the Behavioral Sciences. Support provided by National Science Foundation grant No. BNS-8700864. Delivered at Rose-Hulman Institute of Technology as part of GTE Lecture Series on Technology on the Home Front.

with democratic forms and presumed bulwarks against totalitarianism in place. It is important to ask to what extent traditional democratic societies are vulnerable to the destruction of liberty through ostensibly non-violent technical means and voluntary changes in cultural and social practices.

The role of the home as a preserve for the protection of privacy is being eroded. With modern technology the King and his agents no longer need enter our tenements to collect or deliver information. Ghost-like, the King may enter without physical force or human presence. Unseen, his real (or imagined) influence may be great. As befits a ghost, new forms of information theft are possible without the taking of anything tangible.

Some of the technical, economic, social and cultural barriers that traditionally prevented information from leaving or coming into the home are weakening. Electronic umbilical cords and invisible leashes send ever more information out of the home, even as more electronic information comes in. The home is more integrated into the broader society and more interdependent with it. The weakening of the boundaries between the home and the broader society involves changes which tend to be of low visibility, voluntary, incremental and benignly offered, as such they are easy to miss. Judgment may be further distorted because new intrusions occur alongside of enhanced protections against the traditional kinds of searches the Fourth Amendment was intended to control.

It is also correct that over the last centuries there has been a broad increase in the amount of "private" physical space individuals have within the home. Judged strictly in spatial terms domestic privacy has increased. There is more space both absolutely and relative to the number of inhabitants in the home; there are more separate rooms with doors, and hallways separate rooms. More substantial barriers between rooms, and floors without cracks, mean enhanced privacy within a room (Flaherty, 1972). There are fewer people living in the average dwelling and the percentage of people living alone has increased in recent decades. With the development of the suburbs, the detached family home gained importance relative to apartments and townhouses (though in the last decade this trend has weakened).

Such factors must be balanced against the lessened potential for solitude outside the home that has accompanied the decline of the frontier and the reduction of agriculture and rural communities. Ironically the

city may offer less solitude, but greater anonymity. But regardless of how one assesses this in overall terms, the traditional spatial and physical measures by which privacy has been approached are largely irrelevant to the new forms of privacy invasion.

In other work I have asked if we are on the road to becoming a "maximum security society"(Marx, 1987). In such a society the line between public and private disappears; everything goes on a permanent record, we are under constant observation, much of what we say, do and even feel may be known and recorded by those we do not know – whether we will this or not, even whether we know about it or not. Data from widely separated places easily can be merged and analyzed. Predictive formulaic actuarial models rather than individualized assessments determine how persons are treated.

Information gathering technology becomes ever more penetrating, intrusive and precise. If we make an analogy between the information gathering net and a fishing net, then the mesh has been finer and more pliable, and the net has become more widely spread (Cohen, 1985; Foucault, 1977). Information can be gathered with the pin point specificity of the laser or the absorbent capacity of the sponge.

We are becoming a porous or transparent society in which once shielded actions, even feelings and thoughts, can be made visible.[1] Barriers and boundaries – distance, darkness, time, walls, windows and even the skin – fundamental to our conceptions of privacy, liberty and individuality give way. I have written on this for the workplace and for citizenship in general; here, I focus on the home.

TELEPHONE AND COMPUTER COMMUNICATIONS

How secure are our phone and computer communications? On balance it appears that as our means of communication become more versatile, inexpensive and easier to use, they become less secure. New forms of communication are relatively easy to intercept without special, expensive precautions. The transmission of phone communications in digital form via microwave relays and satellites, cellular automobile and cordless telephones using radio waves, and communications between computers offer new possibilities for eavesdropping.

[1]The "transparent society" is one of six interrelated subsocieties characterizing the maximum security society. The others are a dossier society, an actuarial or predictive society, an engineered society, a self-monitored society and a suspicious society.

As telephone companies have shifted to computer controlled switches for routing calls, telephones now can be programmed so that whenever a given extension dials a number, the line of a secret listener also can be dialed. This makes legal wiretapping much simpler. Automatic telephone switching technology also can record when, where, to whom, and for how long a call is made, regardless of whether it is long distance or to another extension within the same organization.

In 1984 there were 801 legal domestic taps and 600 national security taps. The National Security Agency monitors electronic communication to and from the United States (Bamford, 1983). The extent of illegal wiretapping and bugging is unknown. But to judge from the number of surveillance and counter-surveillance devices sold, it is likely not insignificant. With the right access codes an intruder using a personal computer can connect into the phone network and remotely program it. Beyond eavesdropping, bills can be altered, facsimile transmissions stolen and lines kept permanently busy (*New York Times*, July 22, 1988).

Traditional transmission and recording of face-to-face conversations also have become simpler. With the democratization of surveillance, eavesdropping equipment is now marketed to the public. Tiny radio transmitters hidden in clocks, books, picture frames, table legs, cuff links and umbrellas, are commercially available. There is a subminiature tape recorder the size of a matchbox, not to mention a voice-activated refrigerator sized machine that can simultaneously record up to 40 phone conversations.

Through advertisements in major national periodicals (not simply esoteric security publications) and catalogues, a vast array of control and counter control devices has been brought to mass markets. One company offers a "secret connection briefcase" which includes a "miniature voice stress analyzer which lets you know if someone is lying" and an "incredible 6 hour tape recorder so small it fits in a cigarette pack." A voice-activated tape recorder is described under the bold heading "Eavesdrop for under $80!" With the "spy camera hiding in a lighter" it is possible to "... unobtrusively snap a photo while appearing to light a cigarette." Another company offers "the brief case that sees everything" – "when you carry this ordinary looking briefcase, you're really videotaping everything that occurs." Still another company advertises an undetectable "super-ear" that permits you to hear "not just a baby's cries, but quiet breathing, through a concrete wall a foot thick." Its "Dyna-Mike Transmitter," smaller than a quarter, "will transmit every sound in a room to an FM

radio tuned to the proper unused frequency" up to 2 miles away. Users can "let the tiny microphone sit unobtrusively on the table or concealed on a shelf." Another company sells an electronic listening device, the "Safe-T-Guard Baby Minder" which allows you to hear your baby, and anyone else, when you are not in the room. Even if used only for children, there are interesting issues regarding when parents should stop listening to a child (at age 5, 14?).

Many of these devices also are available as toys. Eavesdropping is presented as a game and spying on your friends is portrayed as fun. In one popular catalog under "Toys to Grow On" ($19.95) "Super Ears" will "help you detect even the slightest sounds! Even if your target is far away, you'll hear every rustle, every footstep, every breath, every word!" "Super Ears" is recommended for children from 5-12 years old.

Phone systems designed as intercoms or paging devices allow managers to listen to conversations in other offices without being detected. Even most conventional telephones are potentially "hot on the hook," that is, easily wired to send voice signals to a terminal, even when the phone is not in use. Or a more exotic "harmonica bug" can be installed so that a predetermined harmonic sound is sent to prevent the victim's phone from ringing. At the same time the telephone microphone is connected into a line to permit the eavesdropper hearing any conversations within earshot.

There are more exotic ways to overhear conversations than a microphone inside a room. Lasers and parabolic microphones aimed at a window permit eavesdropping without the need to enter the premises. Internal sounds also can be heard if one has the foresight and means to aim microwaves from outside at small cone-shaped metal cavities or steel reinforcing rods planted in walls (as the Russians appear to have done in the new U.S. Embassy in Moscow).

Phone privacy is also affected by new phone systems that flash the telephone number of an incoming call. We may welcome this feature since it gives forewarning and we can program phones to block calls from particular extensions. It is also beneficial to emergency services such as police and fire departments since they instantly know where a call is from. On the other hand, this feature destroys the anonymity of the caller. The system may also mean the involuntary disclosure of unlisted phone numbers.

A bit of social maneuvering space also is lost by the widespread use of phone-answering machines which permit their owners to know if a call was returned and allow the caller to leave a recorded message as proof of intention.[2] Electronic and voice mail communication have similar properties, as does the paging beeper. One simply cannot evade these. Such devices encroach upon the white lie, tactful evasion, quiet investigation and solitude (and if one pushes the wrong button, a personal message may be unwittingly transmitted over the entire network). The links between fabrication and privacy are rich and, beyond the pioneering efforts of Erving Goffman, have received surprisingly little scholarly attention.

Phone and computer monitoring are conditions of work in an increasing number of telecommunications, word processing, programming, and customer service occupations (Marx and Sherizen, 1986). Software developments permit monitoring the activities of anyone using a company's computer system – without the user's knowledge. With a program called CNTRL, managers can observe all input entered by the employee and all output from the computer to the user's terminal as it occurs. "Telecomputing" which allows employees to work at home using a computer telephone modem blurs the division between the home and work. Forms of monitoring found in the office or factory by default can enter the home (the reverse is true as well as work places come to offer child care and recreational facilities).

Even home computers not connected to a network are vulnerable. Relatively inexpensive technology can allow the image on most unprotected computer screens to be reproduced up to a mile away without access to the premises where the computer is located. Even electronic typewriters can be bugged! The unique signal each letter gives off when typed can be transmitted and reproduced elsewhere.

Apart from snooping, new techniques such as videotex and teletext that bring on-line information services into the home permit the creation of very detailed profiles of users. Jerome Aumente observes that it is possible to build

> ...an incremental portrait of what news requests an individual selects, how deeply into them they read, requests for other information, messages placed on open bulletin boards

[2]On the other hand these may insulate as well, permitting an individual to deliver a message to those who wish to reach him, without the necessity of a direct response.

> or closed electronic mailboxes, banking, shopping and reservations. In the hands of a marketer, the data can lead to annoying privacy invasions; in the hands of a totalitarian government or unscrupulous employer, it could mean a person's career or personal freedom (Aumente, 1987).

BIG SISTER, BROTHER, MOTHER, FATHER

Norms about family members reporting on each other may be changing. A variety of commercial devices make surveillance of family members easy. From tiny voice-activated tape recorders that can be hidden under the bed of a suspected spouse, to tiny video cameras, to "U-Care," a home drug monitoring kit that permits parents to test children, to hot line reporting, family members find it increasingly easy to check on each other.

The spread of telephone hotlines for reporting almost everything has implications for privacy in the home. A Texas police sergeant, coordinator of a successful crime-reporting program, notes "we get husbands turning in wives, wives turning in husbands – we've even had mothers turn in their sons."

In 1986 the presidential-led war on drugs not only saw parents turn in children, but children turn in parents. The youngest informer was a 6-year-old in New Jersey. The father of a 13-year-old girl who reported her drug using parents says he is proud of his daughter. Similar sentiment is found in Orwell's 1984: "Who denounced you?" ... "It was my little daughter... she listened at the keyhole. Heard what I was saying, and nipped off to the patrols the very next day... I'm proud of her. It shows I brought her up in the right spirit, anyway."

Our legal system, unlike that of many European countries, has no parent-child testimonial privilege. Until recently this didn't matter since prosecutors almost never compelled parents or children to testify against each other. But in the last decade this has changed (Rubin, 1987).

VISUAL IMAGES

Video images mixed with audio transmission offer a much more comprehensive view than sound or the written word alone. They also are harder to avoid – a person can remain silent or talk in code, but physical movement can not be as easily shielded. The collection of visual data

from the home and its environs is much less common than the collection of audio data. Yet this is likely to change as a variety of powerful visual display devices (e.g. video cameras, satellite photography, night vision and heat imaging devices) become available.

The 1968 law which regulates police wiretapping makes no mention of closed circuit television, perhaps because the bulk of cameras then available made them hard to conceal. If police wish to record your phone conversations or to hide a bug in your room, they must get a warrant. It is illegal for citizens to covertly do this, but no warrant is required for authorities to videotape your actions with a hidden camera, nor are citizens prohibited from doing this to each other. This is significant since a video record may be more invasive than simply capturing sound.

It has been jokingly said that chips and microprocessors are so small that TV sets can be made which can't be seen. The sensing chip for a video camera requires an opening no bigger than a pinhole and can easily be hidden. Video cameras can be concealed inside picture frames, books, mannequins, attache cases, radios, paper towel dispensers and fire extinguishers. There is a tiny, hand-held video camera the size of a deck of cards. "Mini-awacs" can spot a person from 30,000 feet up and satellites take pictures from 180 miles. Computer-enhanced satellite photography can identify vehicles moving in the dark, detect camouflage and "see" through clouds. The heat a person radiates permits thermal imaging devices to determine if a house is occupied. The "starlight" light amplifier can be used with a variety of film and video cameras or binoculars. It needs only starlight, a partial moon, or a street lamp 500 yards away to practically turn night into day.

Phone and video technology can be merged. A video-phone box to which a TV and a video camera attach can be purchased for about $400. Every 5-10 seconds updated still images are sent by phone line to the person on the other end. Some estimates suggest that by the year 2000 videophones with continuous transmission will be common in the home. One need not be a civil liberties lawyer to imagine the privacy invading potential of this, without adequate protections. It is easy to imagine unwanted communication from persons exposing themselves ("crank images"?), as well as remote interception by voyeurs and opponents. This system is voluntary and can be turned off, or not purchased. But we may reach a time when remote monitoring systems intended to protect health, safety and security are involuntary. Already some forms are involuntary.

One type of house arrest requires frequent visual identification using video transmitters. More than a decade ago in an Arizona retirement community new homes were wired for 2-way TV systems, fire-detectors, and emergency call and burglar alarms. Police and fire personnel receive immediate notification of possible emergencies and can activate the video cable to see inside the residence – whether or not the resident is at home – without the resident's knowledge (Senate Subcommittee Staff Report, 1976).

LOCATION MONITORING

There are new means of location monitoring that penetrate the walls of the home. As part of an expanding system of house arrest, there is increased use of electronic anklets, bracelets and necklaces that signal a central computer if the device is removed, or the wearer goes more than a short distance (Ball, 1987; McCarthy, 1987). For some, rather than the proverbial castle, the home is now a prison. To paraphrase Robert Frost, rather than a refuge and place where you have to be taken in, the home becomes a prison, a place that won't let you out.[3]

These location monitoring devices are used in conjunction with computerized voice validation, telemetric breathalyzer readings, even wide-angle lens video room scanning. It is but a step to continuous audio and visual room-by-room monitoring. As with wiretapping, such monitoring has implications for the privacy of others in the home not of formal surveillance interest.

Locational devices also are available for the elderly, children and animals. For children a tiny transmitter can be attached to the leg or arm. A monitor sounds an alarm if the child goes beyond a given distance. Another device can be placed in a child's shoe to send signals that can be read several miles away. Equivalent devices help locate lost hikers. There are dog collars that emit a shock if the animal goes beyond a given area; one can imagine a variant for humans.[4] With one device marketed for the elderly or ill living alone, inactivity for too long a period triggers an

[3] In "Hired Hand," Frost writes, "Home is the place that when you have to go there, they have to take you in."

[4] The film "Running Man" features a device worn around a prisoner's neck which explodes if the wearer goes beyond a perimeter. A more benign version has been suggested in which an electrode could be implanted in the body of the offender with an "automatic shock schedule (that) could be triggered if the offender moved away from the approved probation/parole areas." (Stephens and Tafoya, 1985)

alarm. For example, if the person fails to open their refrigerator for 24 hours an alarm is sent and an emergency medical team responds.

Personal location also can be tracked through card-security systems. In some hotels you are given a personalized computer key, a card which controls access to facilities – operates the elevator, opens the room door and activates all electrical appliances. In one system, when the room refrigerator is opened, a bright amber light flashes and a recorded voice says "please do not remove any beverage unless you will use it. Removed beverages cannot be replaced and will automatically appear on your bill. Enjoy your refreshments."

Other forms of access control and record keeping based on biometric identification (hand or finger geometry, signal access, retinal patterns) are possible. For example, while a photo can be faked, hand geometry is relatively constant. At some colleges when students purchase food service contracts, their hand geometry is encoded onto magnetic stripes and placed on plastic cards. At college dining halls, students place their card in the monitor and their hand on the machine. The information is then compared and if it matches, access is granted.

Such devices may find their way into the home to control access to a room or to particular machines. One can imagine such systems for rooms with particular temptations – the kitchen, TV or game room, liquor cabinet, or garage.

What and how much we eat might someday be controlled by biometric access and monitoring. Consider the human possibilities of a system developed by a Hogansville, Georgia farmer who hooked his dairy cows to transmitters. When a cow sticks its head into a feeding station, the computer identifies it, calculates its grain ration and triggers a feed-dispenser. One can as well imagine a machine programmed to release the right amount and kind of food for a person's scientifically determined characteristics and needs. The advent of handheld transmitters used by waiters to send orders to the cook offers another example. One can imagine an electronically processed order first being matched to the person's health records to be sure that the food requested is consistent with needs (e.g. known allergies, religious prohibitions, etc.).

Other devices will soon make the home more transparent. Much more than location can be electronically monitored. A "non-intrusive appliance load monitor" has been developed that can generate an "exact usage history" of all home appliances (Hart, 1985). Each electronic appliance has

a distinctive electronic signature which can be easily measured when the device is turned on and off. This monitor can be legally and inexpensively installed on a utility pole, far from the site being monitored without the consumer's knowledge or consent. As with electronic bank and telephone transactions, such records belong not to the consumer but to the company involved in the transaction, in this case the utility company. The device is offered as a means to better understand energy use and to improve planning.

In repressive societies it is easy to imagine how opening the home to those (literally) with the power is undesirable. Analysis could reveal a forbidden printing press, home computer, copying machine, electric typewriter or VCR. Even in our society, one can imagine controversial uses for the data: checking if welfare recipients possess electronic items to which they were not entitled or claim not to have (e.g. a color TV), tax agents might compare electric power profiles to assure that taxes had been paid on luxury items, persons with unusual energy consumption patterns (either in the type of devices or the time they were used) might become subjects for more intensive investigation, persons found to be using energy inefficiently or high energy consuming devices might be subjected to higher rates or special taxes, and private health problems could be revealed by noting the use of machines associated with particular diseases (Cornish, 1988). Such devices can reveal information that an individual has a right to keep confidential in other contexts.

Utility companies could sell the data to market researchers who might then identify homes without TVs, electric can openers and the like for targeted appeals. Do we really want outsiders to know exactly when we use our toaster, hairdryer, TV or hot tub, not to mention a variety of other machines? While not as intrusive as a video camera in every room, there is still something unsettling about opening up our electrical behavior to distant monitors, however benign the ostensible purpose.

The house of the future will make it even easier for data to flow out to unknown places and users. The National Association of Home Builders, a consortium of the major appliance manufacturers, and providers of services are working on the "Smart House." All wiring will be coordinated so that telephones, burglar alarms, stereo speakers and TVs can be plugged into the same wall outlet. Appliance manufacturers have begun equipping new products with microchips which fit into the closed-loop system of new houses and tell the system controller what's plugged in and what type of service is required.

In addition to leakage from electronic transmissions, the home emits an enormous amount of garbage. Not surprisingly archaeologists have made careers of studying American garbage (Rathje, 1984). But there is also work here for journalists and police. Recently, the Supreme Court ruled that police could legally go through people's garbage in search of evidence.[5] Police are entitled to inspect materials in an individual's trash container, even if it is covered. One can imagine that paper shredders will become common features of the home. But even these may not help, as the Iranians' painstaking reconstruction of shredded CIA documents indicates.

Body wastes are another source of information. Since these are voluntarily given up, control is lost once they leave the body. There are extreme forms of toilet tapping such as at Camp David when the CIA reportedly discovered that Kruschev had diabetes as a result of intercepting the remnants of a flushed toilet. In satirical fashion I wrote an imaginary company's Restroom Trip Policy that had a capability for automatic urine analysis after the toilet was flushed. I was shocked to discover that commercial variants of this may soon be available (Marx, 1987; Hoffman and Silvers, 1987).

Genetic information in DNA molecules in skin cells, hair and blood can reveal identity, family background and current or future health. Such materials may be collected as residue from routine tests or from surgical discards headed for the incinerator. Sometimes, these materials can be converted into profitable biomedical products. For example, a man with leukemia had his spleen removed. His doctor grew cells from the spleen in the laboratory and discovered that they had unique properties that might be promising in fighting diseases, including AIDS. The doctor was able to transform the material into a cell line that he patented in 1984. The original owner of the spleen brought suit but the case was dismissed, several related cases have been settled out of court. The issue of whether patients have property and other rights to their unique genetic make up and discarded cells is unclear (*Boston Globe*, May 18, 1987).

SCREENING SERVICES

Computer technology even may be used to determine whether one obtains housing (whatever the subsequent potential for privacy invasion). In the past a renter was simply interviewed by the landlord. But, as the

[5] *Calif. v. Greenwood*, U.S. (May 16, 1988).

housing market tightens, landlords increasingly turn to tenant screening services. Today renters in major metropolitan areas may be subject to a computer data search, without their consent or knowledge.

These services may investigate finances, rent and employment histories and backgrounds of prospective tenants. They may be linked directly to credit bureaus and other data sources. One pioneering company, Unlawful Detainer Registry, had over 2 million records in 1985 and annually answered nearly a quarter of a million information requests. According to one estimate 40% of Los Angeles' homeless are in its data base. The problem for the homeless is not only, or necessarily, a shortage of housing but also being blackballed for the housing that is available.[6]

In most states there is no requirement that you be informed that you are being checked or are in the data base.[7] There are no standards for accuracy. You cannot see or correct your file. Your name can be entered not only because you failed to pay the rent, but if you signed a rent control petition, sued a landlord, were served with an eviction notice (regardless of the outcome) or have a questionable lifestyle – as reported by a previous landlord. There is no limit to how long a name remains in the file.

The use of predictive profiles is not restricted to rentals but may also affect your chances for a mortgage, home insurance, consumer credit, employment, medical treatment, and college admission. A new, largely unregulated data-scavenging industry sells information gleaned from such sources as drivers' licenses, vehicle and voter registration lists, birth, marriage and death certificates, land deeds, telephone and organizational directories and census-tract records. Computer matching and profiling are increasingly important determinants of life chances (Marx and Reichman 1984).

Nor is the information restricted to quantitative or narrative forms. Video images of homes and offices also are marketed to public safety agencies and delivery personnel, among others. The insides of many important buildings reportedly have been videotaped by the FBI for use in emergencies. There are of course more mundane uses. After placing an order for a pizza delivery, a sociologist observes: "I was astonished to hear the person

[6] "You are in the Computer," WGBH, Boston, MA, May 14, 1985

[7] California is one of the few states with limited legislation. Your name must be removed after data in the file is seven years old. A company has an obligation to tell you what is in their files about you and you can add your version to the record. Landlords are supposed to tell rejected clients they have the right to see their record, although implementation of that standard is another matter.

license numbers, employer, address). This easily could be used to analyze consumption habits. This information might help the store to better meet consumer needs and to anticipate changes in customer behavior, but one can imagine other uses.

Over time, our supermarket purchases might be compared to an ideal USDA diet. If we purchased too much fat, sugar, or salt or not enough vegetables, a warning message could be printed. There might be monthly quotas for junk food. Beyond a notice (e.g., "too many Twinkies this month"), the price for subsequent purchases could be greatly increased, there could be special taxes, or the store might simply refuse to sell more to the customer. Purchases of liquor could be tracked over a several year period and patterns of consumption compared to those of known alcoholics. Persons who show a pattern of increased consumption might receive warnings such as "your pattern of increased purchase of alcohol and decreased purchase of food is consistent with that shown by persons who become alcoholics. Help is available call 1-800 ...."

One traditional way to avoid record linkages and consumer tracking is to pay cash, but the protection this offers may disappear. The U.S. Treasury Department is considering a plan to supplement the serial numbers on paper currency with bar codes to facilitate the tracking of cash. But even apart from bar codes and merged data, enterprising data gatherers may track our purchases in invasive ways. Consider the actions of a reporter who obtained a computerized list of Judge Bork's video rentals and used this as the basis of a story.

UNWANTED AND/OR INVOLUNTARY ENTRANTS

Thus far we have considered communications that can be taken from the home via sound, visual or behavioral indicators. The element of privacy involved is the right to control information about yourself. Let us now focus on the related issue of communications that may involuntarily enter the home without our knowledge and which have the potential to manipulate behavior. The privacy concern involved here is the right to be left alone.

SUBLIMINALS

The use of subliminal forms of communication (auditory or visual) is rapidly expanding. We have come a long way since 1956 when a New Jersey movie theater flashed an invisible message across its screen every 32 seconds saying "Eat popcorn. Drink Coke" and saw concession sales

increase. Today's computer technology permits sending messages in new ways.

Subliminals are found in some workplaces and commercial settings. One program called the "messenger" can be called up by the VDT operator which displays images of mountains and streams along with subliminal messages, such as "my world is calm." More ominous are subliminal messages that the recipient may have no knowledge or control over. Music piped into factories can contain benign subliminals "safety pays," "take pride in your work." But other messages could say "work faster" or even "don't join the union."

Similarly music in department stores may contain buried messages such as "don't steal" or "honesty pays" along with the clanging of a jail door and wailing sirens. But, they might also say "if you love them, buy an expensive gift," or "vote yes." Other settings where subliminals have been used are supermarkets, auto dealerships, real estate agencies and gambling casinos. Subliminal pep talks have been used on professional sports teams.

In 1979 the inventor of one system observed "I see no reason why someday there won't be audio-conditioning the same way we now have air conditioning" (*Time*, Sept. 10, 1979). A decade later a thriving self-help subliminal communications industry has emerged. Hundreds of audio cassette tapes are available for everything from weight loss to "housekeeping with love." One company markets an audible learning tape that parents play when the child is asleep and a subliminal tape with music that is to be used in the background when the child plays. Individuals presumably know what they are doing when they buy such tapes.

But what of subliminal communications received that we have not chosen? Recent developments require us to ask questions such as that raised by a marketer of subliminals for computers: "What is to prevent the manufacturer of a television or a computer from including a chip in the machine that flashes a subliminal message encouraging you to like the machine and buy another?"(*New York Times*, Sept. 20, 1988).

The rental or purchased videos we bring into our home may offer visible advertisements for other videos or products. They may also use subliminals as part of the entertainment (as the film the "Exorcist" is said to have done by flashing a death mask) (Schiller, 1982). But subliminal ads could also be present.

ger – "... public intrusion in private life or private subversion of public life?"(Griffin, 1984).

The prospect of retrieving much of the world's information on a home computer, the ability to shop and bank from home, the chance to choose personal television viewing, the security and protection from electronic monitoring, the accountability given by personal identification systems, the ability to transmit a variety of data, the chance to return messages instead of being a passive recipient and enhanced political and social participation are a few of the many ways that information technology can enhance the quality of life for those with access to the technology.

Participation particularly may increase for women, children and the physically handicapped who have traditionally spent more time at home. Some of the techniques may offer means to mediate the traditional conflict between privacy and community as old as the competing conceptions of the good society offered by Plato and Aristotle (Keohane, 1988).

Contemporary information extractive technologies can be used to protect liberty and privacy. 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 back-up 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 to verify arms control treaties. Electronic monitors can locate lost children and hikers caught in an avalanche. Whether through encryption and distinctive signatures or by providing alternative sources of communication and information, such technologies can aid democracy and help keep government, organizations and individuals accountable.

But elements of a Greek tragedy also are present. The technology's unique power also is its tragic flaw. What serves also can destroy, without increased public awareness and new public policies. With a topic as complicated and changing as this, it is easier to ask the right questions than to produce the right answers. But some policy directions that seem reasonable can be noted.

Cheerleaders for the developments considered in this paper are much louder than are the doomsayers. To redress the balance I have focused on the negative side. But I don't wish to suggest that things are out of control or that there are no positive developments. Privacy questions

are likely to become increasingly important to public policy in the next decade. There have been judicial and legislative gains in recent years – in some ways traditional privacy has been enhanced in the workplace, in schools and in the bedroom. The Supreme Court has inferred a right to privacy in some contexts, though this is not unqualified and must be weighted against "important state interests." Privacy legislation has been extended to some important areas in recent years such as cable television and electronic communication that does not travel over a wire.[10] There are also a rich variety of counter-technologies to block electronic snooping and protect privacy and autonomy. The implications of technical solutions are mixed since a society in which everyone suspects everyone is likely to be neither a pleasant, nor a creative place in which to live. As Judge Learned Hand wrote in 1943, "Liberty lies in the hearts of the people. When it dies there, no constitution, no law, no court [no technology] can save it."

Yet the pace of this change has not kept up with the need. A variety of interrelated actions should be taken, including:

1. The creation of a National Privacy Commission to study and recommend safeguards relative to important changes that have occurred (e.g. the ability to network computers without a central data base) since the last such commission's work of more than a decade ago.

2. Enhanced public education efforts aimed at making citizens aware of their rights with respect to privacy.

3. Development of an annual GNPI measure (Gross National Privacy Invasion) to indicate how many wiretaps, polygraphs, drug tests, computer matches and the like were carried out.

4. Development of consumer and public interest group data bases.

5. Development of strong codes of ethics for professionals such as computer designers and media service providers.

6. Development of legislation that extends the provisions of the Fair Credit Reporting Act to tenant screening services and that extends the warrant protection of audio to video surveillance and that provides for a periodic beep on phones that are monitored.

[10] For example the Electronic Privacy Protection Act of 1986 and the Cable Television Act of 1986.

[] Gandy, O. Jr. 1984. "Media Technology and Targeting: Patching the Cracks in Hegemony." Paper delivered at International Association for Mass Communication Research.

[] Griffin, J. 1984. "Towards a Substantive Theory of Rights." *Utility and Rights*, ed. R.G. Frey. Minneapolis: University of Minnesota Press. Cited in Hixon, p. 101.

[] Hart, G. 1985. "Computerized Surveillance via Utility Power Flows." Unpublished paper, MIT.

[] Hixon D. 1987. *Privacy in a Public Society*. New York: Oxford Univ. Press.

[] Hoffman, A., J. Silvers 1987. *Steal This Urine Test*. New York: Penguin Books.

[] Keohane, N. 1988. "The Public and the Private as Categories of Human Experience." Unpublished paper, Wellesley College.

[] MacFadden, C. 1977. *The Serial*. New York: Knopf.

[] McCarthy, B.R. ed. 1987. *Intermediate Punishments: Intensive Supervision, Home Confinement and Electronic Surveillance*. Monsey, N.Y.: Criminal Justice Press.

[] Marx, G. 1987. "The Maximum Security Society." Paper presented at conference on Technology and the Criminal Justice System., Univ. of Montreal.

[] Marx, G. 1987. "Raising Your Hand Just Won't Do." *Los Angeles Times*. April 1.

[] Marx, G. 1988. *Undercover: Police Surveillance in America*. Berkeley, Calif.: Univ. of California Press.

[] Marx, G., N. Reichman 1984. "Routinizing the Discovery of Secrets: Computers as Informants." *American Behavioral Scientist* 2 (March).

[] Marx, G., S. Sherizen 1986. "How to Protect Property Without Destroying Privacy." *Technology Review*, (Nov. Dec.).

[] Meyrowitz, J. 1985. *No Sense of Place*. New York: Oxford University Press.

[] *New York Times*, 1988. July 22.

[] *New York Times*, 1985. July 7.

[] *New York Times*, 1988. Sept. 20.

[] *New York Times*, 1988. Sept. 8.

[] *PC Magazine*, 1988. June 28.

[] Perrole, J. 1987. *Computers and Social Change*. Belmont, Calif.: Wadsworth.

[] Rathje, W., 1984. "Archaeological Ethnography ... Because Sometimes it is Better to Give to Than to Receive." R. Gould, ed. *Explorations in Ethnoarchaeology*. Albuquerque, NM: University of New Mexico Press.

[] Rubin, Z. 1987. Note: "Parent-Child Loyalty and Testimonial Privilege." *Harvard Law Review* 100 no. 4 Feb.

[] Schiller, H. 1982-83. "First Amendment Dialogue and Subliminal Messages." *Review of Law and Social Change* 11.

[] Shattuck, J., M. Spence 1988. "The Danger of Information Control." *Technology Review* (April).

[] Shearing, C.D., P.C. Stenning 1983. "Private Security: Implications for Social Control." *Social Problems* 30:493-506.

[] Stephens, G., W. Tafoya 1985. "Crime and Justice: Taking a Futuristic Approach." *The Futurist* (February).

[] U.S. Congress. Senate. Committee of the Judiciary. Subcommittee on Constitutional Rights. *Staff Report on Surveillance Technology*. 94th Cong. 1976.

[] Westrum, R. 1986. "Technologies and Society." Unpublished ms. Eastern Michigan University.□