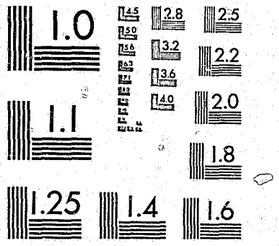
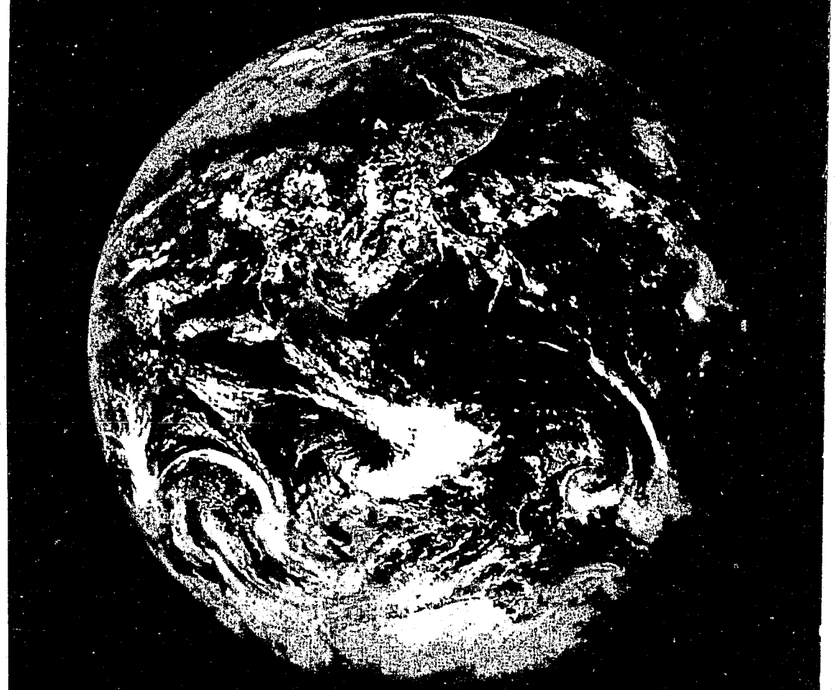


94791

CR-Sent
11-8-84

CREATING A GLOBAL AGENDA

Assessments, Solutions, and Action Plans



Edited by
Howard F. Didsbury, Jr.

16475

Contents

Note

This volume was prepared in conjunction with the World Future Society's Fifth General Assembly and Exposition, "WorldView '84," held in Washington, D.C., June 10-14, 1984. Kenneth W. Hunter served as general chairman of the conference. He was assisted by David Smith, staff coordinator.

The papers presented here were selected from the very large number submitted to the Editorial Review Committee. The emphasis in this volume, *Creating a Global Agenda: Assessments, Solutions, and Action Plans,* precluded the inclusion of a number of distinguished papers whose subject matter did not fall within the general theme of the volume. The committee regrets that space limitations permitted only a small number of papers to be published in this volume. In addition, many papers had to be cut substantially. Footnotes and other scholarly paraphernalia were minimized so that as wide a selection of thoughts as possible could be presented.

Computers and the Future of Privacy

by

Robert L. Pisani

Every step you take,
Every move you make,
Every vow you break,
Every smile you fake
I'll be watching you.

from *Every Step You Take* by the rock group The Police, the top popular song in the summer of 1983; copyright 1983 by A & M Records

In 1890, jurists Samuel Warren and Louis Brandeis, outraged by press reports on social events in the upper-class homes of Boston, wrote an article for the *Harvard Law Review* declaring the "right to be let alone."[1] Though they wrote the article in response to a specific series of events, they made it clear that the main support for their thesis lay in the common-law tradition stretching back over many centruies. Even then, Brandeis and Warren were bemoaning the "numerous mechanical devices [that] threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.' "

Today, faced with government surveillance and the growing sophistication of data bases, the concept of privacy has evolved to reflect a different standard. The National Bureau of Standards defines "privacy" as "the right of individuals and organizations to control the collection, storage and dissemination of their information or information about themselves."[2] Clearly, this is much more than merely the traditional "right to be let alone."

While much has been made of the great benefits of the information revolution, little attention has been focused on the fundamental threat to our concept of privacy, both the "traditional" and "modern" type, that is inherent in the use of these technologies. Another area of great concern is the centralization of information that the federal government will attain as a result of the new technology, allowing power to flow into a single source. Senator Sam Ervin, who held some of the very first hearings on federal

Robert L. Pisani is executive director, International Legal Defense Counsel, Philadelphia, Pennsylvania.

data banks in 1970, expressed precisely this concern by noting that "the undisputed and unlimited possession of the resources to build and operate data banks on individuals, and to make decisions about people with the aid of computers and electronic data systems, is fast securing to executive branch officials a political power which the authors of the Constitution never meant any one group of men to have over all others. It threatens to unsettle forever the balance of power established by our Federal Constitution."[3]

Data-base linkage by both government and business is growing at such an alarming rate that it is outstripping our ability to comprehend or cope with the many privacy issues inherent in such systems. The inability to cope with the growth of these systems extends to all levels—intellectual, social, and legislative—and means that these systems will be in place for years before abuses are detected or before the full social impact of such systems can be evaluated. Of special concern is the explosive growth in surveillance technology, which the author believes will first be used to monitor "deviant" subgroups in which the government has an interest. Such surveillance has become significantly easier due to inadequate laws, recent court rulings, and technological advances.

To counter this threat, measures must be taken to protect privacy. The author discusses several such measures, including legislation, wholesale or partial dismantling of such systems, technological means to procure surveillance-free communications systems, public education, press involvement in the privacy issue, and the development of special-interest groups dedicated to the issue.

Data Bases

In the past, what was known about an individual was usually limited to his friends and acquaintances. Because most communities were self-sufficient, there was little need to rely on outside sources. Nor were there many to rely on—it has only been in the last century that the large government and corporate bureaucracies that we know of have come into existence. In 1816, for example, the total civilian employment of the federal government was 4,500 people, amounting to 0.05% of the total population—half of whom worked for the post office![4]

However, as time passed two things happened to change this relationship: (1) citizen need for services (health, education, etc.) increased; and (2) government and business began demanding more information to assess these needs. Not all of these "demands" were made as a result of citizen "needs," of course. The questions posed by the U.S. Census, for example, expanded almost exponentially in response to business demands to know more about marketing demographics. Whatever the relationship between citizen "need" and government "demand," American (and

especially federal) involvement in formal governmental bureaucracies grew tremendously after the turn of the century. Because this relationship required that the government deal with virtually millions of anonymous people over an extended period of time, data bases were created to keep track of the complex relationships (taxation, Social Security, welfare, etc.) that were developing between citizen and state. The advent of the computer has enabled manipulation of these data and their linkage with other data bases.

Most of us do not realize that we leave a "paper trail" of our lives almost everywhere we go. Imagine if all the receipts we received, all the credit-card transactions, doctor's and dentist's visits, insurance policies, magazine and book club subscriptions, memberships in organizations, even a list of the type of food we bought, were available for inspection at a central source. Such a "paper trail" would enable the government to form a detailed composite of the type of person we are, permitting a fairly accurate determination of our personal tastes and lifestyle, including our health, where we like to travel, what we like to read or eat, our political beliefs, perhaps even our thoughts themselves.

Access to this kind of information would be invaluable to corporations seeking to gain marketing data on certain segments of the population, but it has even greater value to a government that may seek to keep track of real or potential "deviants" such as anti-nuclear protesters, homosexuals, those convicted of a crime, marijuana users, members of minority political groups, or anyone else the government views as a threat to either itself or "society."

Moreover, the growing sophistication of commercial data banks can hardly be viewed as a "benign" development. By way of example, consider that immense corporate data banks exist in the following areas:

Credit. The five largest credit-reporting companies in the United States maintain 150 million individual credit records in their computers, including an individual's marital status, place of work, salary, other sources of income, arrest records, lawsuits, etc.[5] The largest of these companies, Equifax, Inc., maintains a staff of 13,000 employees who work out of 1,800 offices in the United States and Canada and who produce over 25 million credit reports a year. It sells this information to 62,000 customers, including the federal government. Equifax grosses about one-third of a billion dollars each year from the sale of credit reports.[6]

Financial transactions. The records of financial transactions are becoming increasingly easier to access due to the use of Electronic Funds Transfer (EFT). EFT can make it considerably easier to disclose financial information to third parties and increase government or private surveillance of an individual and his or

her activities. The inner workings of such systems are virtually invisible to customers, who have no way of knowing what information they contain and who is gaining access to the information. Moreover, there is almost no legislation protecting dissemination to third-party sources, nor requiring the institution to divulge that it is even disseminating such information. In a report on EFTs published in 1981, the U.S. Office of Technology Assessment concluded that:

> With increased use of EFT there will be a large number of points at which traditional norms of privacy could be invaded. More EFT terminals will be online, making electronic surveillance a more credible possibility. Single-statement reporting of all kinds of financial transactions will become common; more data will be aggregated and thus easier to access. At the same time, there could be broader and swifter dissemination of inaccurate data. Even if customer correction of data is facilitated, it will be more difficult for corrections to catch up with and replace faulty information[7]

Health records. Two out of three Americans have life insurance, nine out of ten working Americans are covered by individual or group health insurance policies. Americans make more than 1 billion visits a year to the doctor; millions visit hospitals each year.[8] The widespread availability of computerized health records makes unauthorized dissemination a growing threat. A doctor's ethical obligation not to disclose details of his patients' health is daily compromised by the demands of health institutions, insurance agencies, and government bureaucracies, all of whom regard detailed information on a patient's history as essential to the maintenance of their information system. As with EFTs, centralization of health records promotes greater ease of access. Health-insurance agencies have recently created a single computerized clearinghouse to process insurance claims. Called the National Electronic Information Corporation (NEIC), it will process up to 85% of all the claims handled by commercial insurance companies through a single computer.[9]

These three areas are only representative of the group as a whole. Other massive data banks are maintained by mailing list companies, employers, other insurance companies, investigative reporting agencies, educational institutions, cable companies, and others. All of this information on individuals is available on computers—computers that are simply waiting to be linked together.

The fact that so much information on individuals is available at a single source leaves the system wide open to abuses. Revelations of such records can intimidate, harass, and embarrass certain individuals if revealed at the right time. So pervasive is the public's fear about disclosure that the National Institute of Mental Health estimates that 15% of all Americans who have medical insurance and are undergoing mental therapy pay for therapy out of their own pocket.[10] That these fears are well-

grounded would seem to be confirmed by the experience of Senator Thomas Eagleton, whose vice-presidential nomination was aborted when it was revealed that he had had therapy some years before.

Imagine if the manipulation capability inherent in EFTs were made legally available to government agencies such as the IRS. If the agency felt that you owed it money, why should it not be authorized to remove the money from your account using EFT, with or without your permission? If this sounds unlikely, bear in mind that parents who have reneged on their child-support agreement are now having this money removed automatically from the money that they receive from the IRS on their tax return. In 1982, the IRS used its computers to prevent the distribution of $168 million in refunds scheduled to go to 275,479 delinquent parents.[11] It does not require a great leap of imagination or technology to allow the IRS or any other governmental agency direct access to your account.

Even data bases containing what may seem like "benign" information can be used for questionable purposes. Consider two "up and coming" services that will, as an aside from their primary purpose, create a whole new series of "lifestyle" data banks:

Home banking. New York's Chemical Bank and the Knight-Ridder newspaper chain recently unveiled their home banking systems, known as Pronto and Viewtron, respectively.[12] Viewtron is the more sophisticated of the two, allowing not only home banking but also the ability to read help-wanted ads, order merchandise, check movie and sports schedules, find an airline flight, and more.

Videotex. Two-way interactive cable television, despite a slow start, is taking off. Such systems allow the subscribers to vote in opinion surveys, order products, choose topics of conversation, and in general to reveal important information on a customer's personal beliefs and preferences to the company. In addition, sophisticated videotex systems will soon be available via most popular home computers. IBM, CBS, and Sears recently announced a joint venture to have such a system commercially available within a year.[13]

Because both of these systems offer a variety of services in different areas, they are capable of creating new, more broadly based data systems that reveal a great deal about the subscriber's general lifestyle, a topic of intense interest to thousands of service-oriented businesses as well as a government intent on suppressing or monitoring select groups leading a certain lifestyle. For example, Warner-Amex's Qube interactive cable system in Columbus, Ohio, has a computer that "sweeps" the system every six seconds to determine, among other things, whether the set is on, what channel is being watched, what political opinions

customers are expressing or merchandise they are ordering through their response buttons.[14]

Governments, too, can be intensely interested in this type of information. Consider the fact that the IRS is now advertising in business publications for "lifestyle" mailing lists that it can rent. The purpose? To compare tax returns with the lists to see if tax payers are paying taxes commensurate with their lifestyle.[15] The IRS recently obtained a computerized list of the estimated incomes of 2 million American households in Brooklyn, Wisconsin, Indiana, and Nevada and will be matching that list against a list of people who filed income tax returns for the tax year 1982.[16] Thus, a seemingly harmless practice such as a lifestyle data compilation can be turned into a surveillance instrument in the proper hands.

In addition, the creation of such "lifestyle" data bases can be so important to service-oriented industries such as Warner Communications and American Express that one could speculate that the primary purpose of owning such systems is to develop "lifestyle" mailing lists to use to market a company's other products, or to sell such data to others.[17] As *Privacy Journal* editor Robert Ellis Smith has remarked: "A single two-way cable television service in a mid-American community can be a gold mine of marketing information. . . . even if the company itself never produces a profit."[18] Even though three states—California, Illinois, and Wisconsin—have laws prohibiting dissemination of information to third-party sources, this apparently does not prevent the parent corporation from using the information as it wishes.[19]

Furthermore, although these corporate data bases are proliferating at an alarming rate, recent court cases have indicated that the Fourth Amendment does not extend to third-party holders of information such as insurance companies and credit agencies.[20] The U.S. government may thus have access to most of these third-party data bases without a warrant and without the need to notify the individual that such an investigation is occurring.

Even more extensive than the corporate data bases are those maintained by the government, especially the federal government. Though there are many, I will concentrate for the moment on criminal data bases, which I consider to be among the most insidious because of the effect that dissemination of these data can have.

The FBI has two large data bases: the Identification Division and the National Crime Information Center (NCIC). The Identification Division maintains the fingerprints of over 63 million people, fewer than half (24 million) of whom have a criminal record.[21] NCIC is a computerized network designed to link all the individuals who work with the country's 57,000 different federal, state, and local criminal-justice agencies.[22] The ostensive purpose of NCIC is to increase the efficiency of law-enforcement

agencies by facilitating exchange of information.

The Attorney General's Task Force on Violent Crime has recommended that the federal government create a new data-base system called the Interstate Identification Index (III) that would allow the user to interact with all the other computers of criminal-justice agencies linked with the system, greatly expanding the data base of the system as a whole.

A police officer in a patrol car will thus have the entire FBI files at his disposal at any time. While a system that would inform a police officer about a potentially violent arrestee may seem appealing at first, the type of information transmitted through such a system should give us pause. There are two concerns here: (1) Is the information transmitted relevant information for the arresting officer to have? and (2) Will it really help the police improve the efficiency of their work?

The argument that such a system will protect police from violent professional criminals by giving them prior knowledge of their behavior might have merit if the whole concept of the violent criminal were not so terribly overblown. Most arrests are made at the local level and under circumstances that a district attorney can check by talking to the arresting officer. No such check could exist in this nationwide hookup. In addition, we are talking about *arrests,* not *convictions.* A large percentage of arrests (30 to 40%, according to some) are dismissed before coming to trial. In addition, many of the records in which an arrest is noted do not make clear what the final disposition of the case was. A recent Office of Technology Assessment (OTA) report noted that federal courts have found violations of civil and constitutional rights regarding the completeness or accuracy of criminal-justice records, particularly when arrest-only information is used in minority employment decisions and when arrest information without disposition information is used in criminal-justice decisions such as setting bail.[23] The same study noted that, on the average, only 66% of the files reported what the final disposition of the case was.[24] Such inaccuracies have not gone entirely unnoticed; the governor of Illinois, for example, recently signed a Uniform Disposition Reporting Law to require state law enforcement agencies to include the disposition of each case in their criminal records.[25]

In addition, there are questions that must be raised as to whether it is relevant for an officer in San Diego to know that an individual was arrested in Portland for public drunkenness 10 years ago. Since the vast majority of all crimes are misdemeanors, this is an important question, since the existence of any kind of previous record may dispose an officer to arrest where he otherwise would have not. In the words of David Burnham, "Do we want the police making arrests for *current* activities based partly on the basis of past behavior?"[26]

Of equal importance with the questions of how much information the government collects is how much information the govern-

ment disseminates and what percentage of that information is accurate. In a 1982 study, the OTA found that about one-fifth of the FBI Identification Division and NCIC arrest records were inaccurate when compared with charging, disposition, and/or sentencing information in local records.[27] The 50 states alone handed out 10.1 million records in 1978, with 2 million going to private corporations and government agencies not part of the system itself. The OTA report noted that, as of mid-1981, 27 states authorized dissemination of criminal-justice records to private-sector organizations and individuals.[28] The same report noted that, as of 1979, an estimated 36 million living U.S. citizens had criminal history records held by federal, state, and/or local repositories.[29] With millions of employers seeking this type of information, much of which appears to be inaccurate, there is a very real possibility that we are creating a permanent class of unemployed or underemployed individuals with criminal records, given the obvious reluctance of employers to hire people with such records.

Despite these concerns, the FBI is continuing to test and refine the III system. Eventually, the system will be completely computerized and will consist of the NCIC along with the FBI Automated Identification Division (AIDS), which maintains fingerprint files, the National Law Enforcement Telecommunications System (NLETS, an interstate electronic switching system), participating state files, and state and local telecommunications networks.[30]

The NCIC, with all its inaccuracies and erroneous information, is tied into a much larger computer system, the El Paso Information Center (EPIC). EPIC originally began as a liaison system between the Drug Enforcement Administration (DEA) and the Immigration and Naturalization Service (INS). It grew rapidly and today includes data not only from the DEA and INS but also from the Coast Guard, the Customs Service, the Bureau of Alcohol, Tobacco, and Firearms, the Federal Aviation Administration, the U.S. Marshals Service, and the FBI. A recent Progress and Activity Report from EPIC reads like an advertisement for the Center, noting that "today EPIC is a full-service intelligence center, providing round-the-clock operational support and intelligence on smuggling of drugs, aliens, and weapons."[31] EPIC contains the names of millions of individuals, boats, and planes.

Another organization, the Internal Revenue Service, has also proposed making its data base easier to access. The IRS proposed in 1976 that it be given authority to create a new computer system entitled the Tax Administrative System (TAS), a $1 billion system that according to the Office of Technology Assessment would have allowed the IRS to decentralize IRS files, making them instantaneously available to those who share and use federal tax information. Most ominously of all, it would have allowed the IRS to significantly increase its intelligence-gathering capabilities by

greatly increasing the amount of information the system could hold, thus allowing the IRS to begin keeping information of a non-tax type. The threat this poses for civil liberties and its potential for harassment of "deviate" subgroups was clear enough that the Carter administration scuttled the project in 1978.[32]

However, the IRS has continued to seek to expand its data base by gaining access to local governmental data banks. It has recently attempted to establish electronic links with the computers of 80 counties in Texas in an effort to gain access to information on voter registration, property taxes, and automobile ownership.[33] Though the IRS claimed that it would use such information only to track down individuals who had failed to pay their taxes, the move has been strongly opposed by local and state officials as well as by civil rights groups on the grounds that such information could be used to compile a huge centralized data base and that the Privacy Act provides that information collected by the government for one purpose will not be used for another without the individual's permission.

What is to prevent the government from taking the information gleaned from these data banks and applying it to other projects that lack specific legislative and even societal approval? Practically nothing, given the fact that the Privacy Act's many "external-disclosure" clauses, including the "routine use" provision,[34] have been so broadly interpreted that it allows dissemination for practically any reason; witness the recent debate over "computer matching" to detect fraud.[35] And since it is almost a principle of bureaucracy that organizations constantly seek to expand their power, we must assume that they will use it for other purposes.

Indeed, there is ample evidence already that the NCIC is being expanded far beyond its original purpose. The NCIC's Policy Board recently began discussing the expansion of the system to include information about people who are considered "suspicious" but are not wanted for crimes.[36] The new guidelines would allow information to be stored on whether an individual was *thought* to be involved in organized crime or terrorism, or was a "known associate" of someone who had been convicted of "possession for sale, sale, or traffic in narcotics." The path would thus be left open to monitor drug users and other "suspicious" people. This recommendation comes only six months after the Bureau agreed to work with the Secret Service to include the names of individuals whom the Service decides might represent a danger to the president or other people it guards.[37] Perhaps most importantly, the FBI does not consider that the expansion of the NCIC to include such "suspicious" persons would require Congressional approval.[38]

All of these government agencies claim, of course, that their machines are designed for a purely "neutral" purpose, i.e., to improve efficiency. Since efficiency is not in itself political, fears that an authoritarian government will develop as a result of these

"improvements" is unfounded.

This argument merely serves to confuse the means with the end. In the words of James B. Rule: "Incremental developments over a long period are bound to bring about qualitative change. These changes will amount to new kinds of social relations between central investigations and 'private' citizens. The question is, What social interests are the new systems most apt to serve?"[39] Thus, a slavish, mindless devotion to efficiency as an end in itself serves only to obscure the more fundamental issues underlying the "efficiency criterion," to wit, at what point does efficiency become too much of a good thing? Does efficiency always serve a benevolent end? The answer to this question, of course, depends on who is doing the asking, but one look at the issue of government surveillance should cast reasonable doubt on the maxim of "efficiency at all cost."

Government Surveillance

The growing sophistication of governmental surveillance programs is of even greater concern than that of corporate and government data-base linkage. Surveillance itself, of course, is not a new development: Abraham Lincoln's administration successfully monitored telegraph communications during the early months of the Civil War.[40] The U.S. Army has kept information on potential dissidents for many years going back to WWI. By the late 1960s, it had an estimated 100,000 people under surveillance, most of them protesters against the war in Vietnam.[41]

During this time, the CIA also conducted Operation CHAOS and Project RESISTANCE. Though CHAOS was ostensibly designed to investigate foreign influences on domestic dissent, in practice that mandate was exceeded and much of the surveillance was purely domestic. Project RESISTANCE was a CIA study of dissident groups in the U.S. that developed an index of approximately 12,600-16,000 names.[42]

What is new is the technology that is now becoming available for surveillance and the growing power of the executive branch's intelligence agencies. President Reagan's Executive Order in December 1981 allowing the CIA to conduct covert operations in the U.S.A., despite his claim that these new powers would not include the right to investigate the domestic activities of U.S. citizens or corporations, provoked a howl of concern from many citizen organizations, including religious groups.

Even local police organizations got into the surveillance business in the 1960s. The Los Angeles Police Department, for example, established a Public Disorder Intelligence Division that kept track of thousands of individuals and organizations between 1971 and 1983. The extent of the surveillance has prompted an ACLU lawsuit against the LAPD.[43]

Despite the tremendous increase in the power of the CIA, its role in the surveillance business is dwarfed by that of the National Security Agency (NSA). To this day, there is no statutory law defining the NSA or its work. It was created by President Truman in 1952 by an Executive Order whose contents remain a secret. As of 1975, the NSA had an estimated 25,000 employees and a budget of $1.2 billion.[44] It has two goals—offensive and defensive. First, it seeks out relevant foreign intelligence by intercepting electronic and written communication. Second, it seeks to protect information bearing on the national security of the United States. To accomplish this goal, the NSA employs sophisticated, state-of-the-art surveillance technology, including satellites, aircraft, sea vessels, and some 2,000 manned interception posts at fixed locations all over the world. All of this information is fed into NSA headquarters in Fort Meade, Maryland, where it is analyzed by computers.[45]

As part of its functions, the NSA monitors incoming and outgoing international electronic communications made from or to the United States. However, interception of international telephone and telegraph messages had been going on even before the NSA was created. In 1948, the U.S. Communications Intelligence Board issued a top-secret directive stating in part that: "Orders, directives, policies or recommendations of any authority of the Executive Branch relating to the collection. . . . of intelligence shall not be applicable to Communications Intelligence activities, unless specifically so stated. . . ."[46] The Communications Intelligence (COMINT) community thus exempted itself from any ban on electronic surveillance almost from the beginning, despite the existence of the Communications Act of 1934, which specifically forbade eavesdropping.

Since 1946, the NSA and its predecessors have conducted Operation Shamrock, whereby *all* the incoming and outgoing commercial and private cable traffic of Western Union, ITT, and RCA was read on a daily basis.[47] The NSA is also permitted to monitor international phone calls of U.S. citizens. Their computer system enables them to monitor 54,000 telephone calls and cable messages in the U.S. simultaneously.[48]

However, the NSA rarely initiates surveillance by itself, relying instead on requests from the CIA, the FBI, the Defense Department, and the Secret Service.[49] To accomplish this goal, the NSA creates "watchlists"—lists of words and phrases designed to identify communications of intelligence interest. Selected communication spectrums are then scanned by NSA computers in search of watchlists entries; any relevant information so obtained is selected for further analysis and then disseminated to the appropriate agencies.[50]

Despite the substantial Fourth Amendment and Privacy Act considerations inherent in the dissemination of such reports to other governmental agencies, the U.S. Court of Appeals for the Sixth District ruled in *Jabara v. Webster* that such agencies do not require a warrant in order to obtain information from the

NSA.[51]

The *Jabara* case is an instructive one that illustrates the fragility of the wiretapping laws. Abdeen Jabara, a Michigan lawyer who was active representing Arab-American citizens and alien residents, was targeted for surveillance by the FBI in 1967. At that time, the FBI asked the NSA to supply any information on Jabara, who traveled extensively in the Mideast. Jabara was never accused of a crime, and the government has admitted that they did not believe he was involved in any criminal activity. The NSA did supply information to the FBI, relating to phone conversations that Jabara had made, and then disseminated the information to 17 other law-enforcement agencies. The court, in ruling that the NSA may disseminate such information to law-enforcement agencies without a warrant, essentially left the NSA free to act as a clearinghouse for intelligence information for virtually all law-enforcement agencies. Law-enforcement agencies frustrated by legal constraints can now simply go to the NSA, and they are apparently free to use any information so obtained in court.

Nor is Jabara an isolated example; hearings held in the mid-1970s revealed that the FBI and Secret Service had both asked the NSA to supply information on 1,200 Americans whom they suspected were involved in civil and anti-war demonstrations.[52] In testimony before the Senate, former NSA Director General Lew Allen estimated that the Agency had issued about 3,900 reports to other domestic U.S. spy agencies concerning approximately 1,680 U.S. citizens who had engaged in international phone conversations.[53]

Even the ability to litigate a claim that one's Fourth Amendment rights have been violated by the NSA is in doubt. In *Halkin v. Helms,* the Court of Appeals for the District of Columbia circuit ruled that *the mere admission or denial of acquisition of information about individuals by the NSA was a state secret.*[54] The Vietnam protesters who filed the suit were thus denied the right even to know if they had been part of a watchlist. A dissenting judge in the case noted that upholding the state-secret privilege in the case "precludes all judicial scrutiny of the signals intelligence operations of the NSA, regardless of the degree to which such activity invades the protections of the Fourth Amendment."[55]

The "right" of the NSA to conduct warrantless surveillance of international communications was supposedly grounded in the Constitutional right of the president to control the conduct of foreign affairs.[56] Such surveillance generated intense criticism, however, and in response Congress passed the Foreign Intelligence Surveillance Act of 1978.[57] The Act limits electronic surveillance of U.S. citizens and resident aliens in the United States to situations where there is probable cause to believe that the target of the communications is a foreign power or an agent of a foreign power, and requires that such surveillance be conducted pursuant

to a warrant issued by special judges appointed by the Chief Justice.

While attractive on the surface, the FISA statute does not offer as many reforms as would appear. What it does do is prevent the specific targeting by name of an American citizen without a warrant. However, the FISA court has never once denied a warrant to the government to conduct such surveillance.[58] Moreover, such requirements exist only so long as the American citizen is in the United States. Once the citizen is outside the U.S., the provisions of the FISA statute do not apply and the NSA is free to monitor U.S. citizens in any way it wishes. In addition, the FISA statute in no way prevents general monitoring by the NSA; it is free to monitor every telephone call and message entering or leaving the country on a random basis, so long as it is done by microwave interception.[59]

Additionally, concern has been expressed over the differences between the FISA and federal Title III wiretapping laws,[60] especially over disclosure of the surveillance application before the evidence may be used (required under Title III, discretionary under FISA), the probable cause standard required (less precise under FISA than under Title III), and the method by which the legality of the surveillance can be challenged (an adversary hearing is held under Title III, an *in camera, ex parte* determination is made under FISA when national security interests are declared in danger).[61] While Congress, in enacting FISA, clearly refused to recognize any inherent power of the Executive to conduct warrantless national security surveillance, a recent court decision, *United States v. Falvey,*[62] left open the possibility of legal warrantless national security surveillance outside of FISA.

Does the NSA monitor conversations between U.S. citizens in the United States? General Allen himself, when asked by Senator Richard Schweiker if the Agency had the capability to monitor domestic conversations of Americans, replied that "such a thing is technically possible."[63] Although this is "technically" forbidden under the Foreign Intelligence Surveillance Act, there is no prohibition preventing agents of other governments, such as the British Government Communications Headquarters (GCHQ), from intercepting and disseminating such information.[64]

By way of addendum, it should be noted that signals intelligence operations in the United States are not just limited to the U.S. and its allies; the Russians have been monitoring phone calls in this country, especially those in and around Washington, for many years.[65] In fact, the Russians have one of the prime spots in Washington for monitoring; their Embassy on Tunlaw Road in the Capital sits on one of the highest hills in the city and directly in the line of a number of important microwave beams.

Moreover, this type of monitoring will only become easier thanks to direct data-base linkage; in 1983, the NSA planned to

put into operation an enormous worldwide computer network, code named Platform, that will tie together 52 separate computer systems around the world.[66] Among the participants will be GCHQ, making direct communication and information dissemination even easier.

What little is known about the NSA reveals a frightening methodology. Not only does it seek to gather any kind of information that even remotely can affect "national security interests" but it actively seeks to prevent Americans from disseminating new devices or techniques to protect their privacy or expand technical know-how. Nowhere is this more obvious than the NSA's involvement in encryption devices designed for "secure" (read: "surveillance-free") electronic communications.

As corporate awareness of the fragility of conventional means of communications such as phone lines has grown, there has been a corresponding increase in private research into encryption devices that could encode electronic data in a form that would be indecipherable to anyone who did not possess such devices.

The NSA views such developments with a suspicious eye, and has consistently sought to either stop such private research altogether or co-opt it by taking over the research itself. However, the scientific community has reacted suspiciously to attempts by the NSA to take over private research. One of the most outspoken critics of the NSA has been George Davida, a professor of electrical engineering and computer science at the University of Wisconsin, who developed an encryption device known as a "stream" cipher system. When he applied for a patent for the device in 1977, he was issued a secrecy order by the Commerce Department at the request of the NSA. The order was later rescinded only after Davida succeeded in focusing attention on the NSA's censorship of academic research. In the words of Carl Nicolai, an inventor who developed a new type of voice scrambler and who had similar problems with the NSA, "They've been bugging people's telephones for years and now someone comes along with a device that makes this a little harder to do and they oppose this under the guise of national security."[67]

Without the use of private encryption devices, it will only become easier for the government to monitor electronic activities such as phone conversations. The chances are good that within the next five years most of the voice communications in this country will be converted from analog technology, where sound is carried by waves of electricity, to digital technology, where sound is converted into electronic pulses.[68] This conversion process, known as the Integrated Services Digital Network (ISDN), will enable the intelligence agencies to have access to vast new amounts of information, since such signals can be run through a computer that can electronically "scan" the signals for key words. Due to the wording of the 1968 federal wiretapping law, the interception of such digital signals by computers is not illegal

under current law.[69]

Given that the NSA now has a relatively free hand in gathering information for itself and other intelligence agencies, we can only assume that technical limitations are the last barriers preventing near total acquisition of information the NSA deems necessary to accomplish its job. For example, much speculation is currently under way as to whether the Agency has developed a computer that can automatically "scan" human voices and pick out key words and phrases it has been programmed to recognize. Such a computer would be a tremendous technological advance and would enable mass monitoring on a level undreamed of previously. According to author Ford Rowan, voiceprints can already be computerized so that the computer can spot key individuals.[70] When the computer recognizes the voice of a person on its watchlist, a copy of the message can be produced for analysis.

The potential that such devices can have for domestic law enforcement cannot be overlooked. Today, even the simplest wiretapping operations are highly labor-intensive, requiring hundreds of hours of monitoring. Even given such labor intensiveness, the number of surveillance orders issued by the Reagan administration increased nearly 280% between January 1981 and September 1982; an increase was also registered with regard to the Foreign Intelligence Surveillance Act (FISA) warrants.[71] In 1981, 589 wiretaps were authorized under state and federal laws, excluding FISA warrants. While this may not seem like an excessive number at first, it becomes a much larger one when we discover that *the voices of 50,000 persons were overheard by those 589 wiretaps.*[72] Moreover, even though most of those whose conversations were intercepted are not suspected of any criminal wrongdoing, the mere fact that they called a tapped line may be enough to land them in yet another of the FBI's computers, the Electronic Surveillance Index (ELSUR). ELSUR cross-references names of persons mentioned in wiretaps and keeps a running "record" of such persons, even if no criminal activity is suspected.[73]

The average citizen, when faced with such overwhelming technical material, may well throw up his hands in despair and forget about trying to understand what is happening. However, a way out of the intellectual quagmire is suggested by discarding such technical information and merely trying to discern the logical outcome of such surveillance efforts. Or, more to the point, the citizen should ask, "What is the ultimate goal of a modern intelligence agency such as the NSA?" Any answer to such a question must clearly be tentative, but we can speculate by offering a modernized theory of intelligence gathering. Under this theory, widespread social upheavals around the world have forced intelligence agencies to change the nature of their security collection apparatus, which prior to this time had concentrated on tracking a few individuals and trends on a macro level. Such an approach

did not work well (witness the CIA's failure to forewarn of the collapse of the Shah's regime), and in response to the question "How can we best predict future political, social, and economic changes around the world in order to influence events and protect our interests?" a new approach evolves concentrating not just on information of obvious intelligence interest but also on hundreds of thousands of events on a micro level, such as newspaper articles, social and political gatherings, even private conversations—what might collectively be referred to as "microintelligence." Such intelligence may not have much value individually but when considered with millions of other pieces of information and in a synergistic fashion begins to make sense in terms of discerning trends, patterns, and modes of possible action on a macropolitical level.

What I am describing is not merely fanciful speculation; it has practical applications on many different levels. For example, James Danowski, a university-based communications researcher, has developed computer programs that analyze the telephone-traffic patterns inside an organization and can yield an accurate picture of who the leaders are and how they function—just from analyzing dialing information. Seemingly innocuous actions, such as misdialing calls, can reveal information about an individual's state of mind. Danowski told *InfoWorld* that his techniques can be applied to groups of phones in a ghetto or student community, thus making invisible social networks visible and identifying key members of a community.[74] Such methodologies can be employed on a much larger, i.e., societal, scale, though they would require correspondingly greater amounts of information.

If we accept the premise of the need for the collection of such "microintelligence," and that seemingly innocuous or disconnected pieces of information can attain great importance when considered as parts of the whole, then we must conclude that the goal of the modern intelligence agency is *total awareness of all events*. As such, the apparatus of the intelligence agencies must be directed toward the attainment of that goal. The means required to attain the goal are: 1) massive computer capabilities, and 2) unrelenting surveillance of individuals and organizations who may not themselves be specific targets but are necessary to understanding developments within the system as a whole. This goal has not yet been attained; however it is technologically within their grasp. Once the technology is firmly in place, the will to attain the goal is undeniably present.

We can assume that as more sophisticated technology is introduced and the ease with which electronic surveillance can be accomplished is increased, the surveillance of citizens, whether it be for "foreign intelligence," "national security," "law enforcement," or whatever, will greatly increase. If experience is our guide, the parameters under which such surveillance is conducted will be expanded (or, alternately, the definition of "national security" or "law enforcement" will be expanded) until virtually the entire population is under some form of surveillance.

While the use of such technology in a democratic society such as the United States is cause for concern, its use in a non-democratic or authoritarian society can be devastating. SAVAK, the Shah of Iran's secret police, used telephone technology developed by Stanford Technology Corporation to monitor thousands of telephone conversations and to keep track of dissidents within Iran.[75] The technology employed was primitive compared to what is available today. In the hands of an authoritarian leader without the constraints of a Bill of Rights, such surveillance could be used to keep track of the movements of the entire population, which would have no legal recourse to prevent such actions.

Deviance and Mass Monitoring

It seems clear that data-base linkage and the advances in the technology of surveillance will permit greatly increased monitoring of citizens by the government. While certain types of monitoring can be beneficial for the citizen when services are provided (e.g., education, health care, etc.), I am primarily concerned with the negative impact that monitoring can have on individuals or groups by whom the government feels threatened. Such groups can include anti-nuclear or anti-war activists, civil rights demonstrators, socialists, draft protesters, labor union organizers, marijuana users, homosexuals, women's rights groups, John Birchers, Hare Krishnas, Iranians, fundamentalist Christians, Scientologists, and others. Surveillance techniques are now becoming so efficient that such "deviant" groups are at a special risk of privacy invasion, and we should not doubt the will of the government in its desire to monitor such groups. As James Rule has written: "When a given form of deviant behavior offends particularly powerful interests, the efforts to seek out information on its possible correlates can become intense."[76]

Surveillance is also capable of influencing one's actions independently of anything done with the information itself. Judge Abner Mikva, a former member of the House of Representatives from Illinois and now a judge for the U.S. Court of Appeals for the District of Columbia Circuit, was himself one of the subjects of the Army's surveillance program in the 1960s. In testimony before the U.S. Senate in December 1971, he described how surveillance could corrupt the electoral process by tainting those under surveillance:

> The scenario might go like this. Those who speak out strongly in opposition to those in power are subjected to precautionary surveillance by the military. Constituents learn that their elected representative is under surveillance. The inference is made, either explicitly or implicitly, that he must be doing something wrong or at least questionable, and that suspicion will be evident in the next election results. After all, who wants to be represented by a man who is so disreputable

that the Army feels that the national security requires that his activities be monitored?[77]

Despite the enormous difficulty in monitoring the financial activity of every American, the IRS manages a remarkably high degree of conformity with the tax laws because it has managed to project an omnipresent image to the American public. *Fear* keeps us paying our taxes, fear that the IRS would somehow know if we cheated.

Imagine now if the same omnipresence that the IRS manages to project with regard to our finances was available to all the other branches of the federal bureaucracy with regard to our other activities. Imagine if every time we signed a petition, or joined an organization whose goals were antithetical to those of the government, or attended a rally, or ordered a subscription to a periodical, these acts were recorded and noted by the government. Imagine further if we were *aware* that the government was aware of all our actions. There is no doubt that many people would voice their opinions or participate in dissent only if they could assume a reasonable expectation of privacy. Absent such an expectation, many would simply choose not to participate.

Kent Greenawalt, a professor at Columbia University and a former member of the Privacy Protection Study Commission, discussed some of the possible effects that surveillance could have on "deviant" members of society:

> If there is increased surveillance and disclosure and it is not offset by greater tolerance, the casualties of modern society are likely to increase as fewer misfits and past wrongdoers are able to find jobs and fruitful associations. The knowledge that one cannot discard one's past, that advancement in society depends heavily on a good record, will create considerable pressure for conformist actions. Many people will try harder than they do now to keep their records clean, avoid controversy or "deviant" actions, whatever their private views or inclination. Diversity and social vitality is almost certain to suffer, and in the long run independent private thoughts will be reduced.[78]

Should large segments of the public ever come to widely believe that the government and corporations are storing information on them to be used to their detriment, this fact could have enormous implications for the manner in which the public deals with these bureaucracies. Increased distrust, coupled with a greater inclination to refuse requests for information, could become commonplace. Such distrust may, however, prove to be a blessing in disguise, as it would create a huge pool of disaffected consumers. Competitive market pressures would force the creation of new companies to cater to this disaffected group, perhaps with the promise that their privacy would be observed absolutely within the bounds of the law and that full disclosure would be made to their customers if they were required to divulge such information.

The public, however, would have less recourse with regard to government bureaucracies, which of necessity possess a monopoly

on certain types of services. It can, of course, lobby for legislative change, but it is then faced with three difficulties: (1) Given the enormous increase in the ability of the government to handle constituent requests for services due to the computer, does the legislative branch possess the political will to mandate that less information should be demanded, that data-base linkages should be halted; (2) Is the public prepared to accept any possible reduction of services that this might entail; and (3) Can every problem concerning dissemination or collection of information be cured by legislative fiat? For example, what political and technical difficulties are presented by the difficulty in monitoring an enormous intelligence agency such as the NSA that is itself shrouded in secrecy?

While it is possible to concede that it is unlikely that we are headed toward the same kind of totalitarian system as practiced by Stalin, it is possible to make a plausible argument that subtler forms of tyranny, perhaps more properly labeled an "informational tyranny," revolving around the government's total access to the facts of an individual's life, may well be developing.

Under this thesis, the relevant question becomes, How much will the government and the corporations ultimately know about each of us, and to what use will they put this information? I believe that the technology now exists to enable the government to know as much as it wants to know about each and every one of us. I further believe that this knowledge will be used not only to "improve efficiency" but also to harass, intimidate, and force a certain type of behavior on each of us that we may not have engaged in otherwise.

Arguments that such an "informational tyranny" will not occur usually revolve around the thesis that a new set of checks and balances is developing to counter the government's growing power. Whenever this theory is advanced, it is usually explained by noting that everyone will have their own computers shortly and this will give individuals rough parity with the government and the corporations, i.e., we will all be able to spy on each other and everyone will enjoy equal surveillance under the law. However, my concerns over privacy will not be assuaged by allowing citizens access to government data banks. Secondly, it is obvious that we will not all enjoy equal access to the same data bases, even if we do have computers. Hardware is not software, and the recent publicity surrounding computer break-ins by technological whiz-kids should not deceive us into thinking that this represents a "check" to government excess. What is important is *power* (read: "access to information") and the motivations of those seeking to develop such systems.

Just what are the interests and motivations of the government and those developing these systems? Are there really hordes of deformed, dwarfish men and women locked in silicon dungeons who are eagerly at work on new ways to destroy our last ounce

of privacy and freedom—technological Igors rubbing their hands and smacking their lips in delight at the thought of serving their corporate and governmental Frankensteins toward the ultimate goal of *total information, total power?*

I doubt it. While one should never be so naive as to dismiss the sinister intent of many at the top of the corporate and governmental hierarchy, most of those actively involved in the development of these systems are technocrats who are motivated by competitive desires and, in the case of government researchers, by a genuine desire to improve efficiency. However, this fact should not leave us any more complacent, for we are now in the paradoxical position where the lack of a stated desire to attain a goal does not mean that the goal will not be achieved. The difficulty is that technology is a hydra; it is a means to many ends. One can easily work toward an end of improved efficiency, while at the same time remaining unaware of another totalitarian "end" resulting from the same means. As James B. Rule has written:

> Orwell foresaw—and made unforgettable—a world in which ruthless political interests mobilized intrusive technologies for totalitarian ends. What he did not consider was the possibility that the development of the intrusive technologies *would occur on its own, without the spur of totalitarian intent.* This, in fact, is what is now happening.[79]

What Can Be Done

We are entering an era where wealth will no longer necessarily be physical; it will be electronic. Knowledge will be power. Modern bureaucracy is now following an "informational imperative" that seeks to gather all possible information on its constantly expanding objectives. These objectives have never been properly confronted or analyzed. Whatever their motives, it is a non sequitur to state that the government or the corporations will create new informational systems and not choose to use them. If the government is using these systems to keep track of "deviant" groups within the meaning of this paper, it is absurd to think that they will not act to protect their interests.

In days gone by, power was of a different sort. Who can forget the words of Stalin when he wondered aloud, "How many legions does the Pope have?" Today, as intelligence surpasses the physical accoutrements of war in importance, such a question is almost an anachronism. Instead, the civil libertarian must ask, "How many data bases does the government have, and what will it do with them?"

What, then, is the answer? What possible "solutions" can be advanced to stem the steady erosion of privacy? It may be instructive for us to turn the question on its head and ask, "Why is it so desirable to seek such a 'solution'? Since people are voluntarily surrendering information, why is this not viewed as an evolution of the concept of privacy that should be permitted to develop?"

This is a reasonable question to ask, and is in fact frequently brought forth by those who feel that rising concern over privacy is really much ado about nothing. According to this thesis, the concept of privacy as I have been attempting to define it stems from a very quaint colonial notion of the right to be left alone that has no place in a modern technological society governed by interdependence and ease of information flow. As such, I am essentially engaged in a debate over a non-issue.

The difficulty I have with this laissez-faire attitude is that the logical outcome of such a position involves such a heightened level of governmental and corporate intrusion in and awareness of the smallest details of one's life. The mere fact of such awareness is enough to cause concern, but when one realizes that both these groups will employ this knowledge for their own purposes (much of which, if not outright illegal, is certainly ethically questionable), the cost becomes intolerable.

Let us examine one possible scenario revolving around the "laissez-faire" approach to privacy. A very good one has already been advanced by science-fiction author John Brunner in his 1975 book, *The Shockwave Rider.*[80] In that book, Brunner depicted a not-too-distant future where detailed knowledge on the lives of all the inhabitants of the United States is stored in computers. In this society, money has practically disappeared in favor of electronic "debits" each individual must spend in order to use the communications system. Since using the system is practically indispensable, the government is capable of constantly monitoring the whereabouts of its citizens. Moreover, the society is almost totally information-open; that is, the average citizen has almost total access to any information via a phone booth. However, instead of spreading joy and happiness, the system creates considerable anxiety since everyone can learn virtually every detail of anyone's life merely by plugging into the computer.

In Brunner's scenario, all communications are monitored by the government to keep track of "deviants" and computer saboteurs. Those who are repulsed by such surveillance form small communities, known as "paid avoidance areas," where cash is accepted and monitoring by the government is very difficult. However, even the fact that one does not use the electronic debit system is noted by the government and you are consequently automatically labeled as a "deviant."

In order to alleviate much of the anxiety caused by technological oppression, many of the citizens use a computerized system known as Hearing Aid, which is operated entirely by the citizens in a particularly remote paid-avoidance town known as Precipice. What makes Hearing Aid such a godsend is that there is always someone listening, though never conversing, with the caller, and the system cannot be tapped by the government due to the existence of "worms" in the system that electronically "eat" the tracer. Much of the book revolves around the efforts of a single person

as he attempts to outwit and harass the government's information monitors.

It should be noted that Brunner's scenario (which he created after speaking with Alvin Toffler about the privacy implications of the technology) involved a largely incremental evolution toward loss of privacy. However, an equally plausible scenario could be created revolving around a "shattering discontinuity" (to use Arthur Schlesinger's term), where privacy is suddenly "revoked" by government to deal with a real or perceived threat.

Author David Goodman described a very plausible scenario along these lines while writing for *The Futurist* several years ago.[81] Goodman described a situation in which the threat of nuclear blackmail by ideology-crazed students created a mass panic among both civilians and the government, leading to calls by some for a Constitutional Convention to amend or dissolve the Bill of Rights in order to deal with the extraordinary security needs presented by the problem. When the terrorists are suddenly captured and the crisis abates, the president abruptly goes on television, states that the problem is likely to occur again, and that in order to take as many precautions as possible the Constitutional Convention should be convened and the Bill of Rights should be suspended indefinitely. Though the story ends there, Goodman clearly implies that the populace would willingly give up civil rights for the "promise" of survival, hence creating the same conditions for a *1984*-type government without ever actually exploding a nuclear device.

Other scenarios have also been described revolving around nuclear blackmail, notably by authors Larry Collins and Dominique Lapierre in their 1980 book, *The Fifth Horseman*.[82]

Though not strictly laissez-faire in their approach to the privacy issue, the latter two scenarios lead to the same state as does Brunner's: a new, subtler form of tyranny bordering on totalitarianism. Because of this threat, I believe that a "laissez-faire" approach, or the failure to speak out against loss of privacy and other liberties should a "shattering discontinuity" occur, is unacceptable.

Another, far more rational approach to the issue involves the legislative approach: to simply prevent the government or corporations from linking data bases together. Such an approach has been going on for many years over the FBI III system, opposed by many in the executive and legislative branches. Taken to its logical extreme, such an approach would involve the partial or wholesale dismantling of data-base-linkage or surveillance systems.

This approach does have a certain appeal. Many previous attempts to deal with legislative means to protect privacy have resulted in legislation that merely improves the efficiency of data banks. Everyone has an interest in eliminating false information—the citizen, the buyer, and the seller of such information

all want files as accurate as possible. It is therefore easier for corporations and government agencies to support "reforms" aimed at eliminating inaccuracies (such as the Fair Credit Reporting Act), which offer mild procedural reforms that are advantageous to the company or agency while at the same time legitimizing the activities they are engaging in, i.e., the collection and dissemination of information. By concentrating exclusively on efficiency we miss the point: do we want such systems *at all?*

This issue has troubled a number of authorities, most notably James Rule.[83] Rule concluded that the intrusive power of these technologies is so great that less information gathering, not improvements in the system, is the answer: "All of these considerations—the dangers of excessive concentrations of social power, the visceral revulsion at excessively intrusive monitoring, and the drawbacks of punishing people too severely for past misdeeds—may warrant curtailment of surveillance under some conditions."[84]

The Privacy Protection Study Commission acknowledged the dilemma posed by Rule without endorsing his (or anyone else's) conclusion: "Quite simply, there is no vehicle for answering the question: 'Should a particular record-keeping policy, practice, or system exist at all?' . . . To deal with this situation, the Congress and the Executive Branch will have to take action."[85]

One difficulty with dismantling systems is the perceived disruption that it would have on services and the threat to the ever-growing "informational imperative" that governs large information systems. If the public were actually presented with this option, many may choose lesser services once appraised of the effect on privacy that the continued growth of these systems entails. However, it may be a mistake for data-system operators to simply *assume* that there is a direct correlation between amount of information gathered and services provided. No one has yet attempted to demonstrate that similar services could be delivered employing less-intrusive information demands. Indeed, as postulated earlier, commercial alternatives could very well arise that promise less-intrusive data collection without loss of services and become commercially viable *as a result of offering such an option.*

The most plausible alternative at this point appears to be legislative and technological attempts to stem loss of privacy. Under this proposal, a mix of legislation to better protect the traditional concept of privacy, combined with technological innovations such as data encryption and other secure communications systems, could, if properly implemented, significantly retard erosion of privacy.

It should be noted that there are already a number of federal and state laws, as well as private regulations, in existence that directly address various aspects of the privacy issue. For example, the Right to Financial Privacy Act of 1978[86] was passed to provide

a mechanism regulating government access to bank records. The Act requires a court order in order for a federal agency to gain access to bank records and prohibits a federal agency from disclosing an individual's financial records to another agency without informing the individual concerned and receiving assurances that the records are required for some legitimate law-enforcement purpose. The Act, however, only covers disclosure of records of financial institutions to federal agencies, not to state or local governments or private institutions.[87] At least nine states have laws modeled on the Act that regulates government access to financial records in possession of banks and other financial institutions.[88]

The Fair Credit Reporting Act of 1970[89] regulates the use by consumer reporting agencies of personal and financial data regarding individuals. Its stated purpose is to assure that information collected by the credit agencies is accurate, that it is relevant for the purposes for which it is used, and that the privacy of the consumer is respected. It forbids the collection of obsolete information, allows the consumer to find out the "nature and substance" of information about him or her in the file, requires the user of such information to notify the consumer if a credit agency report is responsible for the refusal to issue credit and provide the consumer with the name and address of the company, establishes a procedure for the consumer to correct inaccurate or erroneous information, and allows a plaintiff to sue for violations of the Act. Approximately 11 states have enacted similar consumer credit reporting statutes.[90]

A number of other federal laws touch upon the privacy issue at least in part. For example, the Electronic Funds Transfer Act[91] established consumer rights with respect to electronic funds transfer (EFT). The Act requires that banks inform consumers of the terms and conditions governing use of EFTs, including under what circumstances information will be disclosed to third parties. The Equal Credit Opportunity Act[92] imposed limits on the type of information that could be collected by a creditor, specifically forbidding inquiries into a person's sex, marital status, race, color, or religion, except for limited purposes. However, it permits such information to be retained when gathered from third-party sources such as credit agencies. It also requires the applicant to be notified if credit has been revoked and the reasons why. The Fair Credit Billing Act of 1974 [93] was enacted to protect consumers against unfair credit billing practices. It establishes procedures for the correction of billing errors, and forbids the agency from notifying a third party that the bill is outstanding until the agency complies with specific procedures. The Fair Debt Collection Practices Act[94] limits the communications that debt-collection agencies may make about debtors whose accounts they are attempting to collect.

Before more federal laws are proposed to prevent data-base

linkages, however, it may be instructive to see how little existing federal laws have prevented dissemination. The most important piece of federal legislation with regard to this issue is the Privacy Act. Its purpose was summarized in a recent report by the Office of Management and Budget to the Congress:

> The Privacy Act of 1974 (Public Law 93-579) was enacted to ensure an appropriate balance between the Federal Government's need for information about its citizens and the individual's right to privacy. The Act seeks to achieve this objective by establishing procedures to regulate the collection, maintenance, use and dissemination of personal information by federal agencies. The Act establishes a system of checks and balances to ensure the effective operation of these procedures. These checks and balances include provisions for the exercise of individual rights, public scrutiny of agency recordkeeping practices, Office of Management and Budget and congressional oversight of agency activities, and both civil and criminal sanctions.[95]

While the Act prohibits most exchanges of personal information among federal agencies, the "external disclosure" clauses of the Act, especially the "routine use" provision permitting dissemination of information to other agencies compatible with the use for which the information was originally gathered, has been so broadly interpreted that it is hardly an effective barrier to dissemination.[96] There are now 11 "external disclosure" clauses permitting an agency exemption from the terms of the Act, the most recent allowing disclosure to a consumer reporting agency by a federal agency to whom the consumer owes money.[97]

A recent congressional study of the Privacy Act concluded that the Office of Management and Budget, entrusted with developing guidelines for implementation of the Act, had little interest in overseeing the Act and that it "does not actively supervise, review, or monitor agency compliance with Privacy Act guidelines."[98] A 1977 study by the Commission on Federal Paperwork concluded that "implementation and compliance with the Act have been rather poor."[99] Moreover, several witnesses at the recent congressional hearings "agreed that the routine use provision was interpreted so flexibly that an agency could make virtually any disclosure of information that it wanted as long as the proper notice was published in the Federal Register."[100]

One of the most important legislative tasks is thus the strengthening of the Privacy Act. In recent testimony in front of the House of Representatives Committee on Government Operations, a number of groups and individuals urged that an independent agency be created to monitor compliance with the Act.[101] Such a Privacy Commission was part of the original legislation that became the Privacy Act, but was later omitted from the final bill.[102] Representative Glenn English, chairman of the subcommittee that held the most recent oversight hearings, noted that one of the main reasons to conduct oversight hearings on the Privacy Act was to "generate some discussion about the need for

some type of privacy protection board."[103] Such a plan is similar to that of the Privacy Protection Study Commission, which proposed the creation of a "Federal Privacy Board" to monitor compliance with privacy legislation in general.[104] The agency should be given broad powers to set standards for the operation of every personal data bank in the country.

John Wicklein has suggested that the Board should require private and governmental agencies to register their computerized files with regional offices of the Board and to indicate what steps they have taken to insure compliance with regulations. The Board should have authority to inspect such files, and aggrieved citizens should have direct administrative redress by applying to the Board's regional offices. Those offices should have the power to order the expungement of improper or incorrect entries from a person's dossier.[105]

A similar system has been operating in Sweden since 1972. In that year, the Swedish Parliament created the Swedish Data Inspection Board, which was empowered to inspect data systems and to license operators to run such systems. An 11-member board oversees the operations, consisting of representatives from the major parties, labor unions, industry, and the public sector. A citizen has the right to see his files once every year, and to seek the assistance of the Board in correcting inaccuracies. The Board can take those who refuse to correct files to court, where they are liable to a fine or a year in prison. By 1982, Denmark, West Germany, Canada, Norway, Finland, and Austria had also set up data boards.[106] The West German law has been described as a particularly effective model.[107] Unlike in Sweden, the Federal Data Protection Commission in West Germany does not have legal power to order that something should or should not be done, but its access to the media as well as the yearly reports it is required to file have been persuasive enough.

Though President Carter rejected the concept of a Federal Privacy Board, he did propose several pieces of legislation, among them the Fair Financial Information Practices Act. The Act would have given consumers the right to see and copy credit and investigative reports about them. Under present law (the Fair Credit Reporting Act), credit agencies can merely supply a summary of the nature and substance of the records. The Act would also have required the credit grantor to allow the consumer to see the original of the report sent by the credit agency. Given the growing use of credit agencies, a law of this type should be enacted in some form.

Other parts of the Privacy Act also need to be reevaluated. It has often been noted that the Act has no effective enforcement mechanism; that the right of a person to see and copy records about himself is actually fairly restricted, especially with regard to criminal records; and that the "routine use" provisions are overly broad and effectively destroy the very purposes for which

the Act was created.[108] Since the creation of the Privacy Act over a decade ago, it has not been amended to reflect the considerable changes that have occurred since its inception. If the Act is to have any meaning at all, it is time for it to be seriously evaluated and amended.

Another area that should be closely examined is computer matching, which is the comparison of unrelated computer files to identify suspected violators of the law. The use of this technique has been growing rapidly since the Department of Health, Education, and Welfare began its hunt for welfare cheats in 1977. The privacy implications of such matching are enormous. Aside from the problems with accuracy and presenting an incomplete picture of the person, there are substantial constitutional questions involving presumption of innocence, the right to due process, and the right to limit information voluntarily turned over to the government to the purpose for which it was collected. Finally, uncontrolled use of computer matching could easily cause the creation of a national data bank on all Americans. For this reason, the Privacy Act should be clarified to state that computer matches cannot automatically be considered "routine uses," and no further computer matching should be done without thorough study and authorization by Congress.

In addition, hearings should be held in Congress on the feasibility of revising the Communications Act of 1934[109] and Title III of the Omnibus Crime Control Act of 1968 (Wiretap Act).[110] The Wiretap Act in particular should be amended to prevent interception of digitized voice communications. Consideration should also be given to amending the 1968 Act in such a way as to prevent unauthorized interception in any form, thus negating the necessity of revising the Act constantly in order to keep up with new technological developments. The House of Representatives recently held hearings on "Civil Liberties and the National Security State" at which this issue was discussed.[111]

Another important, albeit far more difficult, legislative goal is to replace Truman's 1952 directive establishing the NSA with a legislative charter. In the words of David Kahn, one of the foremost civilian experts on cryptology and the NSA, "An institutionalized mechanism to seek out violations and punish the guilty can best deter the sort of intrusion that so many Americans fear—and that destroys the very freedom that the NSA was created to protect."[112] The Senate Committee that investigated the NSA found that "there is a compelling need for an NSA charter to spell out limitations which will protect individual constitutional rights without impairing NSA's necessary foreign intelligence mission."[113] The House intelligence committee, in its own report, came to the same conclusion.

In addition, private efforts to protect against surveillance can and should be pursued. The technology now exists to make it possible to install small scrambler devices on telephone and elec-

tronic communications that would make it nearly impossible for all but the most insistent organizations to eavesdrop. Indeed, cryptology has advanced to the point where it is now theoretically possible to develop an unbreakable code.[114] James Bamford, in the final pages of his book on the NSA, *The Puzzle Palace*, came to a similar conclusion:

> If there are defenses to such technotyranny, it would appear, at least from past experience, that they will not come from Congress. Rather, they will most likely come from academe and industry in the form of secure cryptographic application to private and commercial telecommunications equipment. The same technology that is used against free speech can be used to protect it, for without protection the future may be grim.[115]

Increased civilian use of cryptology will not come without opposition. As noted earlier, the NSA has been actively opposed to civilian involvement in cryptology, primarily because it fears that successful cryptological techniques developed here will be employed by other countries, thus severely reducing the amount of signals intelligence the NSA will be able to decipher. However, the NSA is already severely limited in the quantity of information it can collect by such means. In the words of David Kahn, "The NSA, in other words, cannot get the most desirable communications intelligence—the high-level messages of the Soviet Union and Communist China."[116] What it is limited to primarily are codes of Third World countries, and it is only a matter of time before they switch to more secure communications systems. The NSA's attempt to "buy time" should not require that civilian organizations halt cryptological research and development.

Technological efforts to protect privacy represents, in my view, the strongest tool available. Many aspects of the privacy issue, such as clandestine intelligence gathering by the government, are not as responsive to legislation. In addition, the difficulty in adequately monitoring government information is enormous, even assuming the existence of adequate legislation. Technological responses such as data-encryption systems assume the existence of monitoring and act to thwart its accomplishment.

So important are technological efforts to protect privacy that the government should actively assist private enterprise in the development of secure cryptographic systems. In the last several years, much of private industry has come to accept the 56-bit Data Encryption Standard (DES).[117] Despite some criticism that the standard promoted was just strong enough to protect from private codebreaking efforts but not strong enough to withstand the efforts of a determined NSA,[118] no other standard seems to have evolved. The DES is now accepted by the National Bureau of Standards, the American National Standards Institute, and the National Communication System. It is also recommended by the American Bankers Association and the International Organization for Standardization.[119]

David Chaum, a computer scientist at the University of California at Santa Barbara, has proposed an unusual method of protecting privacy based on a cryptographic system of identification by pseudonyms.[120] He proposes that individuals would provide each institution with which they have business with a different pseudonym, generated by cryptographic techniques. The pseudonym would be able to serve as identification because certain cryptologic techniques make third-party identification of the pseudonyms possible. However, these pseudonyms could not be connected. Under this system, an individual could not be traced against his will, but could use third-party identification to prove his identity. He would be able to pay his bills without identifying himself, and payment could be authenticated using a cryptographic process. Information about an individual could be passed from organization to organization, but the organizations would not be able to collaborate to derive which pseudonyms belong to which individuals. An individual would also be able to change pseudonyms periodically. This unusual proposal deserves further investigation.

In the long run, however, little real privacy protection will emerge without two of the pillars of modern society: an informed, aroused citizenry and a free press. The press needs to maintain an aggressive posture on the privacy issue, not only to expose the more blatant attempts at invasion of privacy, but also to focus on privacy as an issue in order to assemble the disparate pieces of its loss in an intelligible form. The public needs to recognize the existence of the incremental loss of privacy and to debate the degree to which it wishes to surrender such privacy. Before it can engage in such debates, however, it needs to be educated on the issue. In our society, this means the formation of a special-interest group dedicated to the privacy issue. Because privacy lacks a natural constituent "base," it has been unable to attract sufficient numbers of people to make it a true issue; it has been, in effect, a cause in search of a constituency. Therefore, one of the most essential first steps in raising public consciousness on the privacy issue is to form a special-interest group dedicated to the privacy issue. Ideally, such a group should be a coalition of many interests, from civil liberties and consumer groups to business associations to academic and university organizations.

A good example of building coalitions around the privacy issue was demonstrated recently in Canada. On May 18, 1983, the solicitor general of Canada, Bob Kaplan, introduced Bill C-157, a bill to establish the Canadian Security Intelligence Service (CSIS).[121] The bill would have removed responsibility for national security from the Royal Canadian Mounted Police and placed it in the hands of the civilian CSIS. It would have authorized formerly illegal practices such as opening mail and accessing confidential files. The Service would not have been subject to direct ministerial control or parliamentary review. The CSIS would

have had almost unlimited power to investigate four threats to Canadian security: 1) espionage or sabotage; 2) clandestine attempts by foreigners to advance their interests to the detriment of Canada; 3) political violence or terrorism; and 4) attempts to undermine or destroy the constitutionally established system of government in Canada.[122] The bill was so vaguely worded, however, that the CSIS could have investigated almost any type of political activity, from supporters of the British in the Falklands war to church groups to Third World support groups to socialists.[123]

The implications that Bill C-157 held for privacy and other civil liberties in Canada, especially in light of the recently enacted Canadian Charter of Rights and Freedoms,[124] were apparent to the Canadian Rights and Liberties Federation, which immediately organized a national coalition to oppose the bill. One local coalition, the Ottawa-Hull Coalition Against Bill C-157, which consisted of a large number of labor, women's, and civil rights groups together with several district councils, was particularly effective. News stories were written on the implications of the bill for civil liberties, and public rallies and forums were held in Ottawa and Toronto.[125] Shortly thereafter, the solicitor general agreed to let the bill die. In November 1983, the Canadian Senate published a report on the bill prepared by a special committee that considered many of the concerns of the national coalition. The report concluded that, while there was a need for the CSIS, the bill needed to be tightened considerably to adequately protect the right to privacy and other civil liberties. Specifically, proposals were made to narrow the mandate of the CSIS, to increase ministerial responsibility, and to enhance the provisions for control and review. In January 1984, the solicitor general again introduced the bill, renamed C-9, this time incorporating most of the changes recommended by the Senate Committee.[126]

Since many of the concerns involved in the privacy issue, such as cable television, are in the province of local jurisdictions, small but vocal regional privacy organizations can have a significant impact. One good example is Citizens for Privacy in Cable TV, a Nashville, Tennessee-based organization that organized to educate local citizens on the privacy implications of cable TV and to write privacy protections into the ordinance establishing the system. They sought to require the cable company to tell subscribers what information the computer would be collecting on them, to forbid them to sell or transfer information obtained from the system to any third party without the express consent of each subscriber, and to require the erasure of most information on a subscriber upon the termination of service to that subscriber.[127] They are now seeking to pass a state law to require similar terms from any cable company seeking to operate in Tennessee.

The federal government has also been taking a look at interactive cable technologies. Two bills, S. 66 and H.R. 4103, are presently being considered that would address at least in part some of the privacy issues inherent in these systems. Both bills would limit a company's right to collect data on individual subscribers unless it is for billing purposes or consented to in writing. However, S. 66 has an override clause that would prohibit states from enacting stronger efforts to protect privacy. Because S. 66 is weaker than many of the state bills now being considered, many of those involved in the privacy issue have argued that this provision should be removed from the bill.[128]

A strong movement to enact state and local privacy ordinances will undoubtedly encourage those in the data-marketing business to enact industry standards of their own. The Videotex Industry Association (VIA), for example, recently announced the promulgation of its own set of privacy guidelines that would prohibit disclosure of information on individuals without either their permission or a court order.[129] It also provides that an individual will be promptly notified if a government agency without a court order seeks information about the individual in conjunction with an investigation.

The insurance business has also attempted to promote standards in the insurance industry. In 1979, the National Association of Insurance Commissioners approved a model privacy law known as the Insurance Information and Privacy Protection Model Act.[130] The law was designed to establish standards for the collection, use, and dissemination of information collected by the insurance industry. It requires insurance companies to notify policy holders of the nature and scope of information that may be collected about them, including from third parties, and to maintain accuracy of records and right of access to them by the policy holder; it also defines to whom insurance information may be disseminated, and provides a procedural review mechanism through the state insurance commissioners in the event of a dispute between the policy holder and the insurance company.

There is good evidence that enhanced media discussion of privacy issues is causing an increase in public sensitivity to the issue in the United States as well. In a recent Harris poll, two-thirds of the people contacted through a random telephone sample felt that records were being stored on them without their knowledge. Large majorities felt that it was "possible" or "likely" that the government would use confidential information to intimidate individuals and that this information would be used to take away privacy and personal liberties.[131]

Clearly, we need to be moving toward what John Wicklein has referred to as a "philosophy of privacy protection." Wicklein, a former reporter for the *New York Times*, noted that such a philosophy would need to address the following minimum concerns:

> A person must have the right to see any file kept on him or her by a computer, make corrections in that file if it is in error, and have the

corrections transmitted to all third parties to whom information from the files will be sent. Beyond that, the individual has less-precisely defined rights that will have to be negotiated. These include the right to minimum intrusion by computers and their attendant investigators; an expectation of confidentiality concerning medical records, family data, and legitimate financial transactions; and the right not to have information about the individual known and transmittable by One Big Computer, either governmental or commercial.[132]

These principles should not be looked on as some sort of utopian ideal, but rather as a reasonable response to a growing problem. Indeed, a "philosophy of privacy" seems to be evolving on an international level. The Organization for Economic Cooperation and Development (OECD) has implemented voluntary guidelines for its members on the protection of privacy and transborder data flows.[133] In 1980, The Council of Europe approved a Convention for the Protection of Individuals With Regard to Automatic Processing of Data.[134] More recently, the United Nations Sub-Commission on Prevention of Discrimination and Protection of Minorities presented a report to the Commission on Human Rights concerned with international guidelines on data protection.[135] All three of these documents adhere to the main principles of fairness, accuracy, public knowledge, individual access, and security in information collection.[136]

Regardless of whatever legislative or private "answers" are proposed to the problem, I cannot believe that we will ever go back to the relatively pristine state we existed in before; the computer revolution, with all its implications, seems to be inexorable. If we then assume that some form of increasingly sophisticated monitoring will occur, we must wonder if the public is ready for the radical alteration in privacy that such a change would entail. For many, such a change is seen as beneficial; in the Candide-like world thus envisioned, all information is for the best of all possible worlds. While not in any way denying the benefits of the information revolution, nor the need for legitimate intelligence-gathering activities on the part of the government, I am convinced that we are engaged in a headlong plunge into a Great Experiment of whose consequences we have precious little knowledge. I am concerned that, in the future, privacy may become a precious commodity, sought after by many but in the possession of few.

In addition, I am concerned that, should the public's gradual acquiescence to a loss of privacy continue unabated, little or no outcry will occur when the government attempts to utilize the new technologies to monitor "deviant" groups and to act against them based on such knowledge. By then, the public may be so inured to intrusive technologies that little demand will exist for stringent anti-surveillance laws. Even assuming the existence of such legislation, I have doubts that laws would be able to adequately protect such groups, given the sophistication of the

systems and the adroitness of those employing them in avoiding detection.

Finally, the NSA's insistence on total control of data encryption technology for "national security" reasons can only be taken as a precursor for a much larger government involvement in science and everyday life. The Reagan administration's recent order requiring all government officials in sensitive positions to sign a statement indicating that they will submit any future writing for pre-publication review (a move only recently abandoned after intense adverse publicity[137]) is another example of how the government can gradually move into the private sphere and control not only actions but also thoughts and ideas.

Whether or not we possess the will to protect our traditional concept of privacy against these encroachments is subject to debate. Certainly, the concept of privacy as we understand it is not an immutable one. In the words of Anthony Oettinger, "At any moment in history it is a mix of politics, industrial organization and technology, among other factors, that determines how the privacy of individuals weighs in the balance with other values prized by both individuals and the society these individuals make up."[138]

In 1947, George Orwell wrote and published what was to be his most famous book, *1984*. In it, a continent named Oceania was perpetually at war with two other continents, Eurasia and Eastasia. Probably the two most outstanding features of Oceania were that the government knew everything about everyone and that the past was changed at will. One individual, Winston Smith, discovered the truth, and it was to change his life forever. The high point of the book came when Winston's tormenter, O'Brien, said to him, "If you want a picture of the future, imagine a boot stamping on a human face—forever."

Clearly, Orwell's vision has not materialized as he described it. It seems strange and alien to us because it depicts a world that seems antithetical to our concept of free will and privacy. However, our confidence that a brutal authoritarianism a la Orwell could not happen here should not leave us blind to the fact that subtler forms of tyranny may well be developing, nor should we lose sight of the fact that a slow, methodical trodding of the boot on the human face may well leave as indelible a mark on the human psyche as if that boot had come down on us with all the suddenness that Orwell himself had envisioned.

Notes

1. Brandeis, Louis, and Warren Samuel. "The Right to Privacy," 4 *Harvard Law Review* 193 (1890). For additional information on the history of privacy in the United States, see Flaherty, David H., *Privacy in Colonial New England,* Charlottesville, University Press of Virginia, 1972; and Seipp, David, *The Right to Privacy in American History,* Cambridge, Mass., Harvard University, Program on Information Resources Policy, 1978.

2. Commerce Department, National Bureau of Standards, *Computer Security Publications,* Glossary, p. 17.
3. Federal Data Banks, "Computers and the Bill of Rights," Hearings Before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, 92nd Congress, 1st Session, 1971—Part II, Relating to Departments of Army, Defense, and Justice, p. 1665.
4. Rule, James. B., et al. *The Politics of Privacy.* New York, Elsevier Press, 1980, p. 29.
5. Burnham, David. *The Rise of the Computer State.* New York, Random House, 1983, p. 42.
6. Wicklein, John. *Electronic Nightmare: The Home Communication Set and Your Freedom.* Boston, Beacon Press, 1981, p. 191.
7. Office of Technology Assessment, "Selected Electronic Funds Transfer Issues: Privacy, Security and Equity," OTA-BP-CIT-12, Washington, D.C., March 1982, p. 29. Hereafter referred to as "OTA Electronic Funds Report."
8. Burnham, op. cit., p. 42.
9. *Privacy Journal,* Washington, D.C., January 1983, p. 3.
10. Burnham, op. cit., p. 161.
11. Burnham, op. cit., p. 32.
12. *Time,* November 21, 1983, p. 85.
13. "Big firms team up on videotex project," *Infoworld,* March 12, 1983, p. 13.
14. Wicklein, *Electronic Nightmare,* op. cit., pp. 11, 18.
15. *Privacy Journal,* September 1983, p. 6.
16. Burnham, David. "IRS Starts Hunt for Tax Evaders Using Mail-Order Concerns List," *New York Times,* December 25, 1983, p. 1.
17. The two companies recently formed a single venture, Warner-Amex, to own and operate the Columbus, Ohio, based Qube interactive cable system. Warner owns Warner Brothers, Warner Publishing, D.C. Comics, Franklin Mint Corporation, Atari, Panavision, and Warner Records. American Express owns American Express International Banking, American Express Publishing, Fireman's Fund Insurance, and Showtime. *Privacy Journal,* February 1983, p. 4-5.
18. *Privacy Journal,* February 1983, p. 6.
19. *Privacy Journal, 1982-83 Supplement to Compilation of State and Federal Privacy Laws, 1981.* A similar bill was recently introduced in New York; see *Privacy Journal,* February 1984, p. 6.
20. *U.S. v. Miller,* 425 U.S. 435 (1976); see also *Personal Privacy in An Information Society: Report of the Privacy Protection Study Commission.* U.S. GPO, Washington, D.C., July 1977, pp. 20, 27, 34, 101, 106, 350, 351, 361.
21. Rule, op. cit., p. 39; Burnham, *Rise of the Computer State,* p. 66.
22. Burnham, *The Rise of the Computer State,* p. 54.
23. Office of Technology Assessment, "An Assessment of Alternatives for a National Computerized Criminal History System," Summary Report, OTA-CIT-162, Washington, D.C., October, 1982, pp. 15-16, 21-22. Hereafter referred to as "OTA Crime Report."
24. Ibid., p. 7.
25. P.A. 83-752; reported in *Privacy Journal,* January 1984, p. 4.
26. Burnham, *Rise of the Computer State,* p. 72. OTA Crime Report, p. 14.
27. OTA Crime Report, p. 14.
28. Ibid., p. 15.
29. Ibid., p. 22.
30. "Interstate Identification Index: Operational Summary"; also see "Report, National Crime Information Center, Interstate Identification Index Subcommittee of the Advisory Policy Board," Alexandria, Virginia, September 20, 1983.
31. El Paso Information Center, *1981 Annual Progress and Activity Report,* Washington, D.C.
32. Burnham, *The Rise of the Computer State,* p. 108.
33. Burnham, David. "IRS Seeks Links to County Computers in Texas to Find Debtors," *New York Times,* March 13, 1984, p. A23.
34. 5 U.S.C. 552a(b)(3).
35. *Privacy Journal,* December 1982, p. 1. See also *Oversight of Computer Matching To Detect Fraud and Mismanagement Programs,* Hearings Before the Subcommittee on Oversight of Government Affairs, U.S. Senate, December 15-16, 1982. Washington, D.C., U.S. GPO, pp. 79, 80-81, 84, 104, 120, 156-57.
36. Burnham, David. "FBI Panel Weighing a Plan on Expanded Access to Files," *New York Times,* January 1, 1984, p. 1.
37. For notification of modification of the NCIC records system, see *Federal Register,* Vol. 47, No. 236, December 8, 1983, pp. 55343 ff.
38. Burnham, op. cit., note infra at 26.
39. Rule, James B. "1984—The Ingredients of Totalitarianism." In Howe, Irving (editor), *1984 Revisited—Totalitarianism in Our Century,* New York, Perennial Library, 1983, p. 173. Emphasis in the original.
40. Rule, *The Politics of Privacy,* p. 16.
41. Burnham, *The Rise of the Computer State,* p. 36.
42. Center for National Security Studies, "Operation Chaos: Comparison of Documents Released in *Halkin v. Helms* with the Final Report of the Church Committee," CNSS Report No. 104, Washington, D.C., October 1979, p. 9.
43. "ACLU Lawsuit Questions Spying by L.A. Police Unit," *Philadelphia Inquirer,* January 29, 1984.
44. "NSA: Inside the Puzzle Palace," *Time,* November 10, 1975, p. 14.
45. The most detailed source on the workings of the NSA is found in 5 *Intelligence Activities: Hearings Before the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities,* 94th Congress, 1st Session (1975), and the *Final Report* of the Select Committee, S. Report No. 755, 94th Congress, 2nd Session, 1976.
46. Bamford, James. *The Puzzle Palace.* New York, Penguin Books, 1983, p. 69.
47. Bamford op. cit., pp. 304-8; Burnham, *The Rise of the Computer State,* 30; *Halkin v. Helms,* 598 F.2d at 4 (1978).
48. Krajick, Kevin. "Electronic Surveillance Makes a Comeback," *Police Magazine,* March 1983, p. 95.
49. Gruner, Richard. "Government Monitoring of International Electronic Communications: NSA Watchlist Surveillance and the Fourth Amendment," 51 S. Cal. Law Rev. 429 (1978).
50. *Halkin v. Helms,* 598 F.2d at 4; Gruner, op. cit., pp. 429-31.
51. *Jabara v. Webster,* 691 F.2d 272, *cert. denied,* case 82-1682, October term 1983.
52. *Halkin v. Helms,* 598 F.2d at 4.
53. Bamford, op. cit., p. 381.
54. *Halkin v. Helms,* 598 F.2d at 5.
55. Ibid., at 12.
56. Bamford, op. cit., p. 462.
57. Public Law 95-511, 92 Stat. 1783, 50 USC 1801 et seq.

58. Bamford, op. cit., p. 466.
59. Ibid., p. 468.
60. 18 USC 2510-20.
61. For a discussion of these issues, see Anderson, Judith B., "The Constitutionality of the Foreign Intelligence Surveillance Act," 16 *Vanderbilt Journal of International Law* 231 (1983).
62. *United States v. Falvey*, 540 F. Supp. 1306 (1982). See also Anderson, op. cit., p. 251.
63. Quoted in Bamford, p. 382.
64. Ibid., p. 468.
65. Kahn, David. *Kahn on Codes*. New York, Macmillan Publishing Company, 1983, p. 190-91.
66. Bamford, op. cit., p. 138.
67. Ibid., p. 449; also see Davida's testimony at "1984: Civil Liberties and the National Security State," Hearings in the House Judiciary Committee, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, Washington, D.C., November 3, 1983. Hereafter referred to as "House Civil Liberties Hearings."
68. Schaffer, Richard. "Global Data System Is Seen As Telephones Use More Digital Gear," *The Wall Street Journal,* December 23, 1983, p.1.
69. Burnham, David. "Loophole in Law Raises Concern About Privacy in Computer Age," *The New York Times,* December 19, 1983, p.1.
70. "Electronic Surveillance Menaces Personal Privacy," *InfoWorld,* Vol. 5, No. 15, August 1983, p.16.
71. Krajick, op. cit., p. 98.
72. Ibid., p. 94.
73. Ibid.
74. "Technology and Privacy: Reach Out and Tap Someone." *InfoWorld,* Vol. 5, No. 14, August 1983, p. 10.
75. Ibid.
76. Rule et al. *The Politics of Privacy,* op. cit., p. 133.
77. Burnham, *The Rise of the Computer State,* p. 38.
78. Ibid., p. 47.
79. Rule, "1984—The Ingredients of Totalitarianism," op.cit., p. 179.
80 Brunner, John, *The Shockwave Rider,* New York, Ballantine Books, 1975.
81. Goodman, David. "Countdown to 1984," *The Futurist,* December 1978, p. 345. Goodman found that over 100 of 137 predictions made by Orwell in *1984* had come true by 1978.
82. Collins, Larry, and Dominique Lapierre. *The Fifth Horseman*. New York, Avon Books, 1980.
83. *The Politics of Privacy,* pp. 7, 8, 69-72, 116-17.
84. Ibid., p. 151.
85. *Report of the Privacy Protection Study Commission,* op. cit., p. 536.
86. Right to Financial Privacy Act, P.L. 95-630, 12 USC 3401 et seq.
87. OTA Electronic Funds Report, op. cit., p. 36. Specifically, the federal government is allowed access to financial records only under a court order for purposes related to law enforcement.
88. See Aldrich, Michael, "Privacy Act of 1974: Hearings Before a Subcommittee on Government Operations," 98th Congress, 1st Session, 1983, p. 507. Hereafter referred to as "Privacy Act Hearings."
89. Fair Credit Reporting Act, P.L. 90-321, 84 Stat. 1128, 15 USC 1681 et seq.
90. Aldrich, Privacy Act Hearings, p. 506.

91. Electronic Funds Transfer Act, P.L. 95-630, 92 Stat. 3728, 15 USC 1693 et seq.
92. Equal Credit Opportunity Act, P.L. 94-321; 15 USC 1591 et seq.
93. Fair Credit Billing Act, P.L. 90-321, as added Oct. 28, 1974, P.L. 93-495, 15 USC 1666 et seq.
94. Fair Debt Collection Practices Act, P.L. 90-321, as added Sept. 20, 1977, P.L. 95-109, 91 Stat. 874, 15 USC 1692 et seq.
95. "Administration of the Privacy Act of 1974," OMB, January 4, 1980, reprinted in Privacy Act Hearings, p. 605.
96. The routine-use provision has generated considerable controversy. See Privacy Act Hearings, pp. 46-47, 50-53, 90-93, 252-53, 261-62, 276-79.
97. Debt Collection Act of 1982, Public Law No. 97-3652, 96 Stat. 1749 (1982), 5 USC 552a(b)12.
98. "Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress," Eighth Report by the Committee on Government Operations, House Report No. 98-455, Washington, D.C., U.S. GPO, 1983, p. 2. Hereafter referred to as "Oversight Report."
99. Quoted in Oversight Report, p. 8.
100. Ibid., p. 22.
101. See, e.g., Statement of David Flaherty, Privacy Act Hearings, p. 188-222; Statement of Ronald Plesser, p. 249; Statement of John Shattuck, p. 261.
102. *Legislative History of the Privacy Act of 1974,* U.S. Senate Committee on Government Operations and U.S. House Committee on Government Operations, Subcommittee on Government Information and Individual Rights, Washington, D.C., U.S. GPO, p. 15.
103. Opening Statement of Congressman Glenn English, Privacy Act Hearings, p. 6.
104. *Report of the Privacy Protection Study Commission,* p. 36.
105. Wicklein, *Electronic Nightmare,* op. cit., p. 257.
106. For a summary of the Swedish Data Inspection Board, see Wicklein, *Electronic Nightmare,* op. cit., pp. 198-211.
107. See Privacy Act Hearings, Statement of David Flaherty, pp. 212-13.
108. See Privacy Act Hearings, Statement of Ronald Plesser, p. 231; Statement of John Landau, pp. 260-61, 281.
109. P.L. 19-416, 48 Stat. 1064.
110. P.L. 90-351, 82 Stat. 212, 18 USC 2510 et seq.
111. See esp. testimony of Willis Ware, Rand Corporation, House Civil Liberties Hearings, January 24, 1984.
112. Kahn, op. cit., p. 185.
113. Quoted in Kahn, op. cit., p. 185.
114. For an introduction to this subject, see Rapoport, Roger, "Unbreakable Code," in *The Omni Book of Computers and Robots,* New York, Zebra Books, 1983, pp. 359-70. Kahn has also commented on the general difficulty of breaking codes when the complexity level is raised. He quantifies this problem by advancing a rough rule of thumb: "If you double the capacity of a code, you square the work that the codebreaker has to do." Op. cit., p. 295.
115. Bamford, op. cit., pp. 476-77.
116. Kahn, op. cit., p. 182.
117. For a summary of recent developments in this field, see Branstead, Dennis K, and Smid, Miles E., "Integrity and Security Standards Based on Cryptography,," *Computers and Security,* Vol. 1, No. 3, November 1982, p. 255.

118. Kahn, op. cit., p. 170; see also Rapoport, op. cit., note at 114.
119. Oral communication to the author by Miles E. Smid, senior mathematician, U.S. Bureau of Standards, March 14, 1984.
120. "Taking a pseudonym can prevent 'dossier society,' " *InfoWorld*, September 12, 1983, p. 19.
121. Solicitor General of Canada, News Release: "The Hon. Bob Kaplan, P.C., M.P., Solicitor General of Canada, Introduces Legislation to Establish the Canadian Security Intelligence Service (CSIS)," May 18, 1983.
122. Ibid., p. 3.
123. Gandall, Marvin. "Bill C-157: The Real Threat to Security," *Labour-Focus, Bulletin of the Ottawa Committee for Labour Action*, Vol. 6, No. 4, October 1983, pp. 7-10.
124. The Canadian Constitution, 1981, a resolution adopted by the Canadian Parliament, December 1981.
125. Rapoch, Andy. "A Dry Run for 1984," *Rights and Freedoms*, Canadian Rights and Liberties Federation, No. 49, November-December 1983, p. 13.
126. Solicitor General of Canada, News Release: "The Hon. Bob Kaplan, P.C., Q.C., M.P., Solicitor General of Canada, Proposes Major Changes to the Canadian Security Intelligence Service (CSIS) Legislation," January 1984.
127. Oral communication to the author by Harry Lewis, attorney for Citizens for Privacy in Cable TV, March 13, 1984.
128. Personal communication, Harry Lewis, March 13, 1984. Also see American Civil Liberties Union, *Civil Liberties Alert*, Vol. 7, No. 3, March 1983, p. 3.
129. "Videotex association members set privacy guidelines," *InfoWorld*, Vol. 5, No. 31, August 1983, p. 14.
130. For a copy of the guidelines, see National Association of Insurance Commissioners, 633 West Wisconsin Avenue, Suite 1015, Milwaukee, Wisconsin 53203.
131. *Privacy Journal*, December 1983, p. 1.
132. Wicklein, *Electronic Nightmare*, op. cit., p. 217.
133. OECD, "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data," adopted by the Council in Paris, 23rd September 1980, Document C(80)58(Final).
134. Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, approved by the Council of Ministers in Strasbourg, September, 1980.
135. *Privacy Journal*, February 1984, p.2.
136. The general concept of "fair information practices" is also embedded in the U.S. Privacy Act. For a comparison of the Privacy Act, the OECD Standards, and the Council of Europe Convention, see Privacy Act Hearings, op. cit., p. 655.
137. "Reagan to Relent on Secrecy Pledge," *New York Times*, February 15, 1984, p. 1.
138. Testimony of Anthony Oettinger, Professor of Applied Mathematics, Harvard University, at the House Civil Liberties Hearings, op. cit., January 24, 1984.

END