PRIVACY: AN INALIENABLE RIGHT?

by
BISHOP MARK J. HURLEY

SECRETARIAT FOR
HUMAN VALUES

BISHOP HURLEY IS THE MODERATOR OF THE SECRETARIAT FOR HUMAN VALUES, BISHOPS' COMMITTEE FOR ECUMENICAL AND INTERRELIGIOUS AFFAIRS, NATIONAL CONFERENCE OF CATHOLIC BISHOPS

Privacy: An Inalienable Right?

I

The citizens of California awoke on Nov. 8, 1972, to read in the daily papers that they had amended their State Constitution by the passage of Proposition XI. Proposition XI? What in heaven was that?

There had been practically no campaign of any appreciable magnitude pro or con. The press, surprisingly, by-and-large did not show enthusiastic support or intense opposition, but generally took the view that the proposition was unnecessary, redundant, already a matter of law. Opponents labeled it a scheme to protect welfare fraud on the part of the poor and tax evasion on the part of the rich. Even the guardians of the law, judges and lawyers, took little or no notice. Proposition XI by all odds was a "sleeper," and the people passed it by a large majority. It involved only three words: "people" and "and privacy."

The first article of the State Constitution now reads: "Inalienable Rights: All people are by nature free and independent and have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety, happiness, and privacy."

The substitution of the word "people" for "men" may well be claimed as a victory for women's liberation; and the addition of "privacy" to the inalienable rights an earnest and harbinger of things to come involving the executive, legislative, judicial branches of government, not to mention the political, philosophical, and theological implications.

With the astonishing growth and amazing development of technology—and specifically the computer, magnetic tapes and microfilms—there has been born concomitantly an insatiable appetite for information-

gathering by government and by private enterprise, a gourmand hunger and endless craving to gather, store and retrieve data of all kinds. Moreover, "throughout the public and private sectors, the amount of information collected and stored about individuals is increasing at exponential rates." This appetite for information is at once desultory, capricious, and dangerous.

Thanks to the Watergate "caper," the Pentagon papers trial, and similar escapades, electronic surveillance has captured the attention of the nation. Reports of Army intelligence agents spying on civilians during civilian riots and protest marches; the "prophecies" to foretell potential rioters, the bugging of offices, public and private; wiretaps and videotapes and all the rest make chilling reading.

But even more ominous and portentous is the potential inherent in the technology which has given birth to databanks and methods of systems analysis which technology encourages. With speed akin to light, gifted with a prodigious memory, databanks are becoming the repository of a vast amount of information about people, data that can be kept in storage indefinitely.

The Constitutional Rights Subcommittee of the Senate sponsored a study (1969) which noted, inter alia, that the more economical computer technology has become, the more "an army of specialists in the information-processing field . . . and battalions of investigators and analysts specializing in seeking out and reporting derogatory information on individuals" grow and wax strong. Zeal to know the "total man" has kept government and private computers filling dossiers "to overflowing with the daily lives of people."

Computers have come of age, and databanks have achieved a sophistication suggestive of Orwell's 1984.

The Federal Government has at least 27 agencies and bureaus gathering information, much of it quite private and personal. The Department of Health, Education and Welfare "owns" the Social Security numbers. It used to be that a youth would receive his Social Security number when he got his first job. Today that number may be assigned on entrance to first grade or even earlier. Can the newborn babe escape?

The Internal Revenue Service, now computerized, gathers tax return data; similarly the Passport Bureau, welfare departments, civilian personnel departments

in government, the Department of Commerce with its file on seafarers, the Census Bureau, the Center of Narcotics, the Naturalization Service, the Department of State with its "lookout file", the Customs Bureau, Secret Service, and the F.B.I., the C.I.A., etc., all seek data, much of it private and personal, not to mention confidential and compromising in some instances.

Employers in the private sector are wont to gather personal information on prospective employes, seeking even security clearances, at times without the subjects themselves having any access to these same records. In an economy heavily dependent on credit, bankers make extensive use of computers; credit-card companies build credit dossiers on millions of customers. A fairly accurate profile of a person's actions can be constructed from the transactions of a steady credit-card user. Doctors, too, build up files—often of a very personal and intimate nature. Seven hundred insurance companies rely upon the Medical Information Bureau of Boston to check prospective insurees. Student records are a major source of information for dozens of purposes, from granting scholarships to employment.

Even the driver's license has become a source of special attention; many states have sold drivers' lists commercially.

Finally, not merely the criminal records of all law enforcement agencies, but their general files as well—the police files—contain vast quantities of information, much of it confidential and, at times, compromising to individuals and groups.

The potential for dossier-building staggers the imagination; the womb-to-tomb history of each person retrievable on demand becomes a possibility, at the very least.

But what if all these files and dossiers could be centralized, cross-referenced, and, in one place, made available? Is it possible to evolve the "total identifier" in a master file, perhaps under the Social Security number?

Pressures to introduce a single identifying number for each citizen, known as S.I.N., are obvious for hospitals, credit card companies, schools, banks, police and others. All chartered banks in the U.S.A., for example, have recently been required to record the Social Security numbers of depositors to facilitate the retrieval of information for tax purposes, a breach in the initial law on Social Security. Contrariwise,

Congress refused to allow the Social Security number cross-reference on the 1970 census forms.

Sweden introduced identification numbers for all citizens in 1947; Israel in 1948, Norway, 1974; and other countries expected to follow suit include the Benelux countries, West Germany, Spain, Japan and Switzerland.

The single identification number and the concomitant "total identifier" pose both a temptation and a threat. The enormous value in time saved, in costs, in accuracy, whether to employers, police, the I.R.S., banks, life insurance companies, doctors and educators can scarcely be exaggerated and constitutes a real temptation. At the same time, in terms of individual—and even corporate and institutional—liberties, they pose a threat of no mean proportions. A master-file under a single Social Security number does not now exist; the U.S. Health, Education and Welfare Department (HEW) study of this matter states, however, that "automated personal data systems present a serious potential for harmful consequences, including infringement of basic liberties."

II

In his *Data Banks in a Free Society*, Alan F. Westin labels as "mostly fantasy" the image of computers storing up data, talking among themselves, and linking up tapes and discs to form a surveillance net from which no fact about an individual's life can escape. Vast centralized computer databanks simply do not exist, despite a widespread conviction to the contrary in the mass media and the public.

Experts affirm that it is scarcely feasible economically to store data of vast magnitude directly in the "on line" memory of the computer. But they also point out that the computer can be programmed to key in on the "off-line" memory with data stored on discs, magnetic tapes, and on microfilm, as well as cards.

The Taxation Division of Canada, for example, stores on 125 reels of magnetic tape the records of 10.5 million taxpayers, consisting of 500 characters each. At the same time, all experts agree that computers will become smaller in size, more versatile in operation, and much less expensive to purchase and operate.

While the "total identifier" does not as yet exist, it cannot so easily be dismissed as not feasible

simply on economic grounds. Rather, Westin's study recommends a social and legal policy be effected "with built-in safeguards hammered out before the inevitable development of centralized computer record-keeping."

A Canadian government task force in its study, *Privacy and Computers* (1972), which enjoyed "close liaison" with Prof. Westin's study group, stated in its opening words the dimensions of its work: "The widespread development of highly computerized databanks has given rise to increasing concern about their potential use for invasions of personal privacy." This study rejected the proposition that, in mid-1972, "a social crisis" exists and that invasions of privacy are so widespread as to cause alarm. Yet "continuing worries exist" because few databanks have been designed and installed with a concern for privacy built into the planning process, except for institutional self-interest."

"The privacy crisis," the study concludes, "unlike the ecology crisis, which was predicted but largely ignored until severe damage had been done to the environment, need never happen. Appropriate preventive measures can make certain it never will."

While there is no doomsday syndrome forming in this matter, no need for prophets of doom, yet the Canadian task force warns that "insensitive or wilful use of the computer could lead us closer to 1984."

The city of Huntington Beach, Calif., is reported in the press to be the first American community to have entered each one of its citizens—man, woman and child, guilty or innocent, accused or unindicted—on its police department's computer. On the basis of home address, the data includes medical information, abandoned cars, water bills, credit history, and even the name of the family dog. Financial support comes from the Law Enforcement Assistance Administration of the Federal government.

The question can reasonably be asked if the citizens of Huntington Beach or anywhere else in the U.S.A. realize the extent and range of information-gathering going on without their knowledge in many, if not most, cases.

Do they realize that dossiers are being built up without the knowledge of the persons involved; without the possibility of review and correction of "raw files" and "raw data"; without the knowledge of who—in or out of government—has access to these files?

This same Law Enforcement Assistance Administration is pumping millions of dollars into state and local police departments to promote computerization, "108 computer projects in 1971" alone. Similarly the FBI-managed National Crime Information Center is creating a network which ultimately will join over 6,000 law-enforcing agencies, a single source of data.

"All of these trends must be looked at as a unit because their confluence represents a terrifying spectre," writes law professor Arthur Miller.

One need only reflect on the Watergate hearings to note that "informal" interchanges of FBI files took place between the Attorney General's office and the Committee to Re-elect the President. The computer hasn't much changed the methods of political campaigns, but it has made such exchanges easier, more efficient, and most tempting. Moreover, under the old manual files, it was possible to get away from one's past and begin again a new life free of damaging information.

Technology, however, promises to create a "dossier prison" wherein every entry will remain for life, a possible "hearsay narrative" without literal or contextual accuracy. The prospective employe may be asked if he were ever "arrested." Even though subsequently acquitted, his "yes" answer may well foredoom his chance for employment.

The computer will keep that "fact" indefinitely. In his official inquiry for the House of Representatives, Congressman Cornelius Gallagher contrasted the Judeo-Christian concept "to forgive and forget, to make amends and begin again" with the "computer that cannot forget and that is incapable of forgiving."

Assemblyman Kenneth Cory, who introduced the "privacy" amendment in California, summed up the matter in these words:

"The frightening thing about many of these files is the individual may never know he is in them or who has seen the information recorded. If this information were centralized and augmented (by cross-reference files), government could truly know more about many of us than we know ourselves."

The June 25, 1973, *U.S. News and World Report* reported, "A Fight Over Who Can Look at Your Tax Return," in which a presidential order to open the income-tax returns of 3 million farmers to the U.S.

Department of Agriculture has engendered a reaction in Congress described as "explosive." The department sought the requested data "on tapes" directly from the I.R.S. computers at Martinsburg, W. Va.

Sen. Sam Ervin has recited a litany of offenses against personal privacy: the selling or lending of lists of names on government files; the sharing of "blacklists" among agencies; the sharing of credit lists; check on the finances, sex life, personal beliefs and associations of famous and unknown people alike; and even the questioning of women by the Federal Housing Administration on birth control practices, the private advice of doctors, in reference to loans on homes. "Unchecked, we will have the trappings of a police state," he concluded.

One technical expert said simply: "Considering what I know about micro-electronics, I must conclude that the worst is yet to come. We must manage the keepers of the machines!"

Computer technology and databanks serve men and are controlled by humans. They are not autonomous. But who controls the human factor? Who protects not only the individual citizen, but as well groups, associations, corporate entities, racial and ethnic and religious assemblies from the misuse and abuse of technological data gathering? How control the insatiable appetite and inordinate zeal of some of those in power, whether in the public or private sector? *Quis custodit custodem?* Who will watch the watcher?

The computer is a many-splendored animal; consequently, there is much potential protection right in the technology itself, sophisticated means whereby safeguards can be part and parcel of the databanks themselves. Most observers call for new laws. Others, while conceding the role of law, would add the need for a public morality and moral consensus on the protection of privacy.

But no databank system can ever be fully secure and "security measures can be broken if the payoff warrants the trouble." Thus, physical security and control of access as well as steps taken to insure honest personnel are at least as important as some of the sophisticated protection measures programmed in the computer system itself.

Computer systems use such devices as "passwords" stored in two places, i.e., with the user and the system, for the retrieval of data; various codes for

scrambling and unscrambling data; limited access control not only as to "who" but as to access to "what"; audit trails to detect unauthorized usage. IBM, for example, has announced an investment of $40 million in the next few years to develop security protective hardware for its computer systems.

With its wondrous capacity to accept, store and retrieve information, the computer in its very sophistication can as easily be programmed to destroy data. Medical facts, for example, can be processed for research and statistical purposes and then "forgotten." Similarly the facts may be stored but the identity of the human subject erased. Furthermore, the computers can be taught to require the identity of the person who takes information.

The salient point is, however, that security up to this date has been geared toward the protection of industrial and political security against espionage, and not in the context of individual privacy.

Data banks that contain sensitive information require technical programming that protects the human right to privacy insofar as is reasonable. Much can be done, then, to build in certain safeguards. But this is but a first step; the law of the land must reckon the new technology and its ramifications even beyond the invasion of privacy.

This legal approach to the protection of privacy is not so simple. To leave it to the courts and judiciary will not solve the problem of proper protection; nor will legislatures solve the questions alone.

There is a necessary interplay between the judiciary and legislative branches of government; but equally there is similar relationship between them and the administrative and regulatory agencies of government.

Courts can be slow; litigation costly and time-consuming. Principles are developed over a long period, case by case; the redress of wrongs is past history. More is needed, yet the court's role is crucial. Similarly, the need for new laws that will undoubtedly emerge as challenges, particularly to the regulatory agencies, is raised.

Yet the key question seems to be: Is there a superior public interest to which individuals must yield their privacy?

III

While the courts have long been active in the area of "privacy," and even the U.S. Supreme Court based its decision in the Connecticut contraception case (Griswold v. Connecticut) on the right to privacy, the legal experts, judging from the law school reviews, labeled the decision as "none-too-clear" yet "the clearest to date" on the "elusive nature of privacy," "a broad, abstract, ambiguous concept."

Nor have the legislatures fared much better. Their work on the protection of privacy has been judged "spotty and non-comprehensive." The administrative branches of government have patently failed in serious ways as the recitations of the invasions of privacy grow longer and sadder, to wit, the record of wiretaps, electronic surveillance right in the President's own offices; the sterilization of young girls with or without parental consent (as if it mattered morally) under the aegis of governmental agencies and at taxpayers' expense; the experimentation on human beings with venereal disease, etc.

Patently there are new dimensions to the problems of privacy in society today, problems exacerbated by technology itself.

The regulatory agency in the Federal government most deeply concerned with the information gathered on individuals, HEW, has been working on a study for over a year toward the protection of the right of privacy. As "owner" of the Social Security numbers (and who does not, among us, have a Social Security number?) HEW is particularly the target of information seekers, computer-experts, and all those devoted to S.I.N., the single identifying number.

The agency, at the request of the President of the United States, has drafted proposals for safeguarding personal information. Its faith in its project may be summed up in its draft report: "The application of automated data processing technology to the management of records containing personal data can be subjected to appropriate and effective social constraint without diminishing its usefulness."

"We share strongly the belief," it goes on to say ". . . that protective action should be taken and that the department (HEW) has a unique opportunity and responsibility to help safeguard against and overcome the potentially harmful consequences of automated personal data systems."

To such ends the Committee has proposed rules and regulations by way of safeguards to privacy:

One person should be responsible for the proper security and safeguards. Data must be eliminated after no longer truly useful, a sort of statute of limitations. Public notices must be posted when, for example, an agency has an automated personal data system. The agency must not only say it has such a system, but as well the categories of persons on whom data is kept; kinds, sources, and uses of data kept. Who has access to data, and how individuals may get redress, and what is legally required of persons, must be made a matter of public record.

But while HEW struggles with the problems, what of the private sector? Who has more sensitive and all-embracing information of a personal nature in one place than the central databank in Boston, the resource center for 700 insurance companies? What of the huge credit card operations of Mastercharge, Bank of America, and American Express? Such questions have prompted Prof. Miller to call upon "credit agencies and insurance companies to achieve a minimal level of ethical activity in the gathering of information."

Miller has advocated, in answer to the total problem, the formation of "an independent, non-operating agency specifically concerned with the task of monitoring information systems and preventing abuse," a National Data Center as first proposed by Richard Ruggles.

But when all is said and done, there still remains the moral climate in which the judicial, legislative and administrative branches of government, as well as private enterprise, live and breathe and have their being. A moral climate is fundamental to the solving of the problem of the threatened invasion of privacy. If Watergate has said anything, it has called for an ethical refurbishing of the climate of our society.

Theologians raised in the "natural law" tradition see the right of privacy, like the right to think, as deriving from the human personality "with no direct connection with the mission of the state." The natural law and the *jus gentium* demand privacy; people must be secure in consulting professional people in their personal problems; in the use of the mails; in the sanctuary of their homes.

Much like its legal history, the concept of "privacy" in moral theology has not been met head-on. Treatment of privacy centers mostly in the subject of "secrecy." Secrets must be kept inviolate to avoid

pain, offense, loss to the "owner" of a secret. Such a right is, of course, not absolute, except in the sacrament of confession. Secrets must be kept in order to insure free and confident access to the various levels of professional advice, and a violation of such secrets is an offense against social justice. A breach of secrecy demands a delicate assessment of all relevant factors, such as serious injury to an innocent third party, or national security, etc.

On a related matter of the "invasion" of the human mind and possible invasion of privacy, Pope Pius XII in 1958 warned psychoanalysts that "just as it is illicit to appropriate another's goods or to make an attempt on his bodily integrity without his consent, so it is not permissible to enter his inner domain against his will."

Thus there is a natural secrecy from the nature of the human person and of society itself protecting individuals and groups from harm or reasonable displeasure.

It can be fairly concluded that while the bases for the protection of privacy does exist in law and moral theology, yet the right to privacy has not been sufficiently enunciated in either, particularly in view of the advent of modern tools of information gathering and the temptations thereunto attached.

Some experts are calling for "a total and complete re-vamping of our legislative approach to informational privacy, including the regulation of computer transmissions and the movement of information in interstate commerce" (Miller). Most will admit that an "ethical refurbishing" is necessary, a change in the moral climate in the U.S.A. to protect the individual and groups against the threatened invasion of privacy, a value among those few values so fundamental and yet so undefined.

As was well stated in Stanley vs. Georgia (394 US, 564), the right to privacy is an aspect of the spiritual nature of man: "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by

civilized man."

That "many-splendored animal," the computer, promises great benefits and poses equally serious threats. New safeguards are in order and are imperative.

The people of California were walking much in advance of their legislators, judges, administrators and theologians when they voted affirmatively that the right to privacy should be singled out, underscored and emphasized in this our day and times. Implicitly, they agreed with the judgment that "The privacy crisis, unlike the ecology crisis which was predicted but largely ignored until severe damage had been done to the environment, need never happen!"

1974
Publications Office
UNITED STATES CATHOLIC CONFERENCE
1312 Massachusetts Avenue, N.W.
Washington, D.C. 20005