PERSONAL PRIVACY AND THE LAW

by Kent Greenawalt

During the last decade, the right to personal privacy has gained the status of a central social value in America. This new emphasis is, of course, related to the long-standing American belief in personal freedom and the basic dignity and worth of the individual. But the more immediate cause has been public anxiety about the increasing dominance of government, corporations, and other large bureaucratic organizations—and fears of what these organizations may do with the vast amounts of personal information they accumulate.

Americans, with their traditions of English common law, Protestantism, and reliance on constitutional protection, have tended to be less tolerant than their European brethren of surveillance by government, the church, and other authority. Among the chief irritants of British colonial rule in America were the official inspections carried out under "writs of assistance"—general warrants that authorized searches of someone's property, home, and place of business for evidence of customs violations. American merchants, to be sure, did engage in extensive smuggling to avoid paying taxes to the British Crown, and some thus grew rich. Nevertheless, these searches contributed to the resentment that led to the Revolution of 1776.

The Bill of Rights, which followed closely upon the original Constitution of 1789, contains three explicit protections of privacy:

> The Third Amendment prohibits the quartering of soldiers in people's homes during peacetime.
>
> The Fourth Amendment bars unreasonable searches and seizures.
>
> The Fifth Amendment contains the privilege against self-incrimination.

Many state constitutions have similar provisions. Yet, apart from these limits on the powers of government, and the traditional legal barriers against trespass and personal assault, American "law" played only a modest role in the protection of privacy through the 19th century.

At a basic level, privacy is a universal value. In all societies there is some compelling need for separateness and protection against encroachment. Yet, what is perceived as one's own, proper, personal space, and what are regarded as encroachments, vary greatly from one society to another.

Cultural anthropologist Edward T. Hall has noted, for example, that Germans tend to claim a larger sphere of privacy than do Americans or Englishmen—a demand epitomized by the German law that prohibits photographing strangers in public without their consent.[1] The English exhibit a certain reserve, which keeps others at a distance. The French appear to enjoy, or tolerate, physical contact in public places, but seldom permit outsiders to intrude upon the privacy of the home.

Beyond some minimal protection of personal space, the value attached to privacy is largely dependent on other varying social concepts. Marxist regimes preaching an anti-individualist ethic of social cooperation, not surprisingly, place little store on privacy. Liberal democracies, on the other hand, accord special privileges of privacy to the family, to religion, and to the sanctity of communication between doctor and patient, lawyer and client, and within the confessional.

Yet, in America, it was not always so. Our Puritan forefathers tried to regulate one another's activities with meticulous care. The Puritans allotted themselves quiet and solitude for private prayer, but church members also took seriously their mandate to expose one another's sins. Unmarried men and women, for example, were required to live within a family household so that they would not be free of observation and constraint. Even in later periods, despite our professed belief in liberty, we have tended to be intolerant of solitary eccentrics and suspicious of those holding minority views. Intense scrutiny of those with odd personal habits or unpopular political views

---

Kent Greenawalt, 41, is professor of law at Columbia University Law School. Born in Brooklyn, he was educated at Swarthmore (B.A. 1958), Oxford (B.Phil. 1960), and Columbia (LL.B. 1963). He served as law clerk to Supreme Court Justice John Marshall Harlan from 1963–64 and as deputy solicitor general of the United States from 1971–72. He is the co-author (with Walter Gellhorn) of The Sectarian College and the Public Purse *(1970) and author of* Legal Protections of Privacy *(1975).*

has been, as during the McCarthy era, a forceful weapon in the suppression of deviance. And, as political scientist Alan Westin has indicated, a strong "populist" strain has nurtured the belief that democracy in America requires that political activity be open and that governmental bodies and associational groups have little legitimate claim to privacy.

The Sanctity of Solitude

Nevertheless, prevailing American conceptions have continued to attach importance both to individual and group privacy. The American notion arises from a set of needs present, if not always satisfied, in every society. At various moments, individuals seek solitude and intimate companionship. Privacy, in the most obvious sense, is freedom from outside interference, whether from a curious neighbor, a police officer, or from a radio blaring music from the apartment next door. In a more subtle, but perhaps even more significant respect, privacy can be invaded by intrusions into one's thought processes, as by brainwashing, psychosurgery, or, on a more mundane level, subliminal advertising.

A second aspect involves the protection of private information. Indeed, some scholars have gone so far as to define privacy solely in terms of the control that individuals have over information about themselves.[2] One can feel "penetrated" or "exposed" or "threatened" as much by the awareness that one's intimate thoughts and feelings are known by others as by an unwanted visitor. Our expectations of privacy of information extend to some facts that are initially public. If, for example, we attend a controversial political meeting, we may expect our presence to go unnoted. No doubt, many who attended a speech by black activist Eldridge Cleaver at Iona College in 1970 were disturbed to learn later that police officers had recorded their names and the license numbers of their cars.

There is a third aspect of what has become the modern conception of privacy: the freedom to make autonomous decisions about one's personal life without interference—to work out one's own form of sexual satisfaction, to use drugs, to wear one's hair long. Individuals are freer to make many of these choices if their private lives are not exposed to public view. Thus privacy of information supports the value of autonomy. If there were broader public tolerance of deviant personal habits and behavior, there would be less need for secrecy and some forms of privacy might be less important than they are now.

During most of the 19th century, since the main threat to

privacy was the curiosity of one's neighbors, there was little need or possibility of curbing intrusions through extensive legal controls. What has caused a radical transformation in the problems of privacy are such changes as the development of mass media; the urbanization of American society; the expansion of federal, state, and local bureaucracies; the growth of huge corporations; and the much-publicized advances in the technology of information acquisition, retention, and dissemination.

It was the thirst for gossip and scandal of the mass-circulation newspapers and journals in the heyday of "yellow journalism" that triggered the initial formulation of a right to privacy in a famous 1890 law review article by two young lawyers, Samuel D. Warren and Louis D. Brandeis.[3] "Gossip is no longer the resource of the idle and the vicious, but has become a trade, which is pursued with industry as well as effrontery," they wrote. Worried about exposure of private and family matters, they urged that the courts explicitly recognize the right of citizens to recover damages for unreasonable publicity.

The common law, they argued, granted "to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."

Newspapers, magazines, and now television seek to appeal to audiences with news about the lives of the very rich, the very famous, and the very powerful, whether they be politicians, rock singers, or tennis stars. They also give us vivid details of the lives of ordinary people, like Karen Quinlan, who become caught up in dramas of compelling journalistic interest.

The Limits of Unreasonableness

The law in most states has made a response to the argument made by Warren and Brandeis. Between 1890 and 1950, the common law principle of an individual's right to privacy was adopted by most states. The courts now routinely support the notion that damages may be recovered if one's name or picture is used for advertising or other commercial purpose without one's consent; one's private life is exposed to unreasonable publicity; one is placed in a false light by publicity; or one's seclusion is intruded upon.*

*Ralph Nader, in a suit settled out of court in August 1970 for $425,000, charged that General Motors invaded his privacy by interviewing acquaintances about his private life, tapping his telephone, having him followed by private detectives, and attempting to entice him into indiscretions with attractive women. In another noteworthy case, Jacqueline Kennedy Onassis in 1972 won the protection of a federal court from the attentions of an energetic free-lance photographer, Ron Gallela, who constantly lay in wait for her and her children in order to take candid photographs of them.

Ironically, the shakiest branch of this law is the one that concerned Warren and Brandeis most—the right to be free of unreasonable publicity. The difficulty lies in the First Amendment right of freedom of the press, which sets limits on what can be considered unreasonable publicity.

The Price of Anonymity

Other changes in society have been more complex than the development of the mass media, making appropriate legal responses more difficult to determine. A city environment brings people close together and thereby impinges on privacy, yet urban living is notoriously anonymous. In contrast to the gossipy folksiness of many small towns, big city people today frequently eschew involvement with others, even to the extent of ignoring pleas for help from victims of crime.* One typical aspect of city and suburban life is the separation of one's neighbors, work associates, and relatives. Even if neighbors acquire unwelcome information about one's personal life, it is not likely to be communicated to the persons one most cares about.

Paradoxically, this increased freedom is offset by a different form of intrusion. Prospective employers, banks, government agencies, and the like can no longer depend on the widely held knowledge of a person's character and circumstances that used to exist in the traditional small town. As a result, the collection of dossiers substitutes for personal acquaintance.

Because of the demands of public education, taxation, social security, welfare, and law enforcement, government agencies now acquire enormous quantities of information about people, including those who have never served in the military or been on the public payroll. A 1976 inventory showed that within 97 federal agencies there were 6,753 systems of records and 3.8 billion dossiers—many of them computerized—on individuals.

It is not sufficient to say that most information in public and private records is obtained from the subject or with his consent. Few people will forego the chance to obtain a job or other important benefit if that is the price of preserving privacy. What is needed is some fair assessment of whether the social value of information outweighs the cost to privacy.

The computerization of records poses a special problem. When a person supplies data about various aspects of his daily life—whether it involves banking, education, or whatever—he often does so with the hope or expectation that it will be held in a confidential manner by the collecting organization, used for a

* See, for example, A. M. Rosenthal, *Thirty-Eight Witnesses*, New York: McGraw-Hill, 1964.

specific purpose, and not released except as required by law or with the person's consent.

But record keepers—including corporations, insurance companies, hospitals, and credit bureaus—now routinely exchange information on a mutual basis. And computers can gather bits of information that, when assembled, may be used to support conclusions that would be impossible for those in possession only of the individual pieces of information. For example, if all of a person's personal checks are centrally recorded, an investigator with access to those records may be able to conclude that the person is living way beyond his normal income. Of course, the assumption that he has unreported income will sometimes be erroneous, as when he is spending savings or serving as a legitimate purchasing agent for a group. But even if the inferences drawn from records systems were uniformly accurate, the increased exposure of our lives to outside scrutiny would be disturbing.

Another fearsome feature of records systems—one symbolized by computers but not unique to computerized records —is their impersonality. Decisions affecting a person's credit, the availability of insurance, even access to a job may be influenced by records that are based on false or incomplete information. The problem is compounded when the individual involved has no ready access to the information filed and thus may be unaware of damaging data until he has already been victimized.

James C. Millstone, a highly respected assistant managing editor and former Washington correspondent for the St. Louis *Post-Dispatch,* was one victim. Only when his insurance was abruptly canceled did he discover that he was the subject of a consumer credit report filled with innuendo, misstatements, and slander. It cost Millstone a lawsuit in 1976 to compel the credit reporting company to reveal fully its derogatory and inaccurate dossier on him.

Truth in Spending

Civil libertarians and others are giving close attention to the implications of "electronic fund transfer" (EFT) systems now undergoing widespread testing by banks and retailers in California and the Midwest. With EFT, payment for purchases is made at the point of sale by using telecommunications and computers to transfer money automatically from the bank account of the buyer to that of the seller.

Justice William O. Douglas once observed: "The banking transactions of an individual give a fairly accurate account of

his religion, ideology, opinion, and interest . . ."[4] But the Supreme Court, in *U.S. v. Miller* (1976), recently rejected the argument that the confidentiality of personal banking transactions is constitutionally protected against federally imposed disclosure requirements.

"The Supreme Court decision," according to the July 1977 report of the Privacy Protection Study Commission, "comes at a time when electronic funds transfer services, and other developments in personal data record keeping, promise far-reaching consequences. . . ." The commission, which was created by the Privacy Act of 1974, worried that transformed EFT systems could become "generalized information-transfer systems." For example, as with credit cards, both the payer and payee under EFT are likely to want a written record of the date and place of purchase and a description of the items bought. Thus, the monitoring of electronic transactions "could become an effective way of tracking an individual's movements."[5]

Privacy Post–Katz

Record-keeping systems, of course, are not the only technological threat to privacy. Electronic eavesdropping and wiretapping have been especially useful to police, to federal security agencies—and to those engaged in industrial espionage. And both courts and legislatures have sought to bring electronic surveillance under some control.

The Supreme Court's most significant step came in *Katz v. U.S.* (1967). The Justices overruled a 1928 decision *(Olmstead v. U.S.)* in which a sharply divided Court had held that a wiretap was not an illegal search and seizure within the meaning of the Fourth Amendment. Four decades of scientific advance had produced miniature recorders and transmitters and a host of other electronic marvels with which it was possible to listen in on conversations without the awareness of those involved.

The Justice Department argued that Katz's conviction for illegal gambling—based on evidence obtained from an FBI wiretap of his conversations with bookies from a public telephone booth—was perfectly proper; there had been no physical penetration of the phone booth. The majority opinion, delivered by Justice Potter Stewart, held that "the Fourth Amendment protects people, not places," and that what a person seeks and expects to preserve as private, even in an area accessible to the public, may be constitutionally protected.

The Court decision left the government free to engage in court-ordered eavesdropping if law enforcement officials could

establish in advance, to a judge's satisfaction, that a wiretap or listening device would probably produce evidence of criminal activities. Prior to 1968, Section 605 of the Federal Communications Act had been interpreted to forbid wiretapping. But federal officials had done almost nothing to discourage wiretapping by local law enforcement officials, and the Justice Department asserted the right to wiretap as long as it did not disclose what it discovered. The result was federally authorized wiretapping against suspected foreign agents and domestic political activists, including civil rights leader Dr. Martin Luther King, Jr.

Surveillance Without Warrant

In the 1968 Crime Control and Safe Streets Act, Congress banned all private electronic eavesdropping but permitted law enforcement agencies to eavesdrop under court order when investigating a broad range of serious criminal offenses, including, for example, all drug violations and illegal gambling. Whether wiretapping and roombugging should be allowed in ordinary criminal cases is the subject of recurrent debate, and many states continue to prohibit it. Advocates stress society's need for better weapons against organized crime; opponents argue that the net of electronic surveillance catches innocent as well as criminal conversations. Even if one accepts the need for some eavesdropping, the present act permits it, in my view, for too many crimes and for too long a period.

The 1968 act left open the legitimacy of surveillance without a warrant for national security purposes. But the Supreme Court in 1972 *(U.S. v. U.S. District Court)* rejected the Nixon administration's theory that "domestic subversives," such as radical political groups, should be subject to surveillance without a court order. The Court left unresolved the constitutional status of warrantless surveillance by federal officials for foreign intelligence and counterintelligence purposes both here and abroad.

Hearings on various proposals to curb national security wiretapping within the United States were held through the 1970s, spurred by intelligence agency abuses reported by the Senate Select Committee on Intelligence headed by Senator Frank Church (D.-Idaho). The committee found that: ". . . through the uncontrolled or illegal use of intrusive techniques—ranging from simple theft to sophisticated electronic surveillance—the government has collected, and then used improperly, huge amounts of information about the private lives,

political beliefs and associations of numerous Americans."[6]

Proposals have been made by both the Ford and Carter administrations for congressional legislation authorizing electronic surveillance for security purposes under court orders issued on the basis of a less stringent standard of "probable cause" than would be permitted in an ordinary criminal case.

Such legislation would impose a degree of regularity and control that is now absent, but some civil libertarians are made very uneasy by the idea that wiretapping should ever be explicitly authorized without prior evidence of crime.

Certainly one lesson of the Watergate era, and of the post-Watergate disclosures of CIA and FBI excesses, is that even when the legal restrictions are spelled out there is a danger that overzealous officials will disregard them. Throughout the 1960s and early 1970s, U.S. intelligence agencies conducted surveillance of thousands of American citizens. Most of these citizens were not themselves suspected of committing crimes or contemplating espionage, but the government wanted to know more about their *lawful* political activities, on the theory that such monitoring might uncover covert criminal activities or connections to groups threatening national security. Some agencies, like the Internal Revenue Service, went further and undertook tax audits intended to harass individuals and groups believed to be politically hostile.

Alternative Intrusions

While government wiretapping and eavesdropping represent the most dramatic threats to personal privacy, there is a more mundane problem posed by the growing use of lie detectors and intrusive questionnaires to monitor the honesty of existing employees and to screen prospective employees for sensitive jobs.

Obviously, banks, educational and medical institutions, law enforcement agencies, and the like must protect themselves and the public from people with physical or moral disabilities that could impair their performance. It is certainly appropriate to ask a prospective bank teller if he has been convicted of fraud, and to inquire whether a would-be drugstore delivery boy has been a narcotics addict. But questions that require the most personal revelations, and techniques that seek to lay bare the applicant's emotional responses, often bear too little relation to any genuine need to be justified. Occasionally courts have intervened against overly intrusive inquiries. For example, a Pennsylvania junior high school was stopped from instituting a

program designed to identify potential drug abusers by questionnaires that asked about the home life of students and their attitudes toward fellow students.*

Thus far, Congress has placed few significant limits on the kinds of personal information that either the government or the private sector may seek. Obviously it is difficult to deal with such matters by general legislation. And Congress has proved unsympathetic to creating an agency that could evaluate the justifications and drawbacks of particular screening systems.

It has, however, sought to control the retention and transmission of information once it has been acquired by federal agencies. After finishing its 1974 inquiry into federal data banks, the House Subcommittee on Constitutional Rights concluded: "Once information about an individual is collected by a Federal agency, it is likely that information will be fairly readily passed on to other Federal, State and local agencies."

The ensuing Privacy Act of 1974 was based on the following premises: Individuals should be able to find out what information about them is contained in federal records and how it is used; they should be able to prevent data given by them for one purpose from being used for another without their consent; they should be able to correct or amend records about themselves; and organizations handling identifiable personal data should assure its reliability and timeliness, and prevent its misuse.

Routine Abuses

The law has not been a total success. Government agencies have found various ways to avoid some of its strictures, most notably by defining very broadly the "routine uses" of information that are exempt from the limits on dissemination imposed by the act. For example, the IRS is perfectly free to exchange income tax data with state and local tax authorities. Nevertheless, the law has compelled most agencies to be more careful, and it provides a reasonably solid foundation upon which improvements can be built.

Some years ago, it seemed likely that the judiciary would use constitutional concepts of privacy and due process of law to oversee the fairness of records systems, but the Supreme Court has evidenced little zeal for being drawn into such matters, rejecting individual claims in cases involving records of banking transactions, abortions, and the use of sensitive prescribed drugs. A few state courts have been more responsive, but the

Merriken v. Cressman, 364 F. Supp. 913 (E.D. Pa. 1973).

burden of protection now lies mainly on legislatures.

A logical further step in federal and state legislation is the extension of legal controls to cover record-keeping systems in state government and in certain key business sectors. Federal restrictions already exist to protect the privacy of personal information kept by schools and colleges that receive federal funds. The 1971 Fair Credit Reporting Act provides for some access by individuals to data about their credit ratings, as well as procedures for challenging inaccuracies. But the records held by banks, insurance companies, hospitals, and telephone companies are not yet sufficiently protected. We can, and should, continue to seek sensible and workable rules for record keeping and dissemination of information that can be broadly applied to major private organizations as well as all public agencies.

Too often in the past, incursions on control of information and other invasions of privacy have occurred as an unconsidered by-product of the pursuit of other objectives. The last decade and a half have taught us a lesson that must not be forgotten. New technology should be evaluated in light of its perceived effects on privacy and should be developed in a way that is responsive to society's values; for in the end, oddly enough, the loss of privacy represents a loss of control over our very lives.

1. Alan F. Westin, *Privacy and Freedom,* New York: Atheneum, 1967, p. 29.

2. *Ibid,* p. 7.

3. S. Warren and L. Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 289, 1890.

4. *California Bankers Association v. Shultz,* 416 U.S. 21, 94 S. Ct. 1494, 39 L. Ed. 2d 812 (1974).

5. Privacy Protection Study Commission, *Personal Privacy in an Information Society,* Washington, D.C.: Government Printing Office, 1977, pp. 101–118.

6. Quoted in *Congressional Quarterly,* Dec. 31, 1977, p. 2697.