THE UNDERPINNINGS OF PRIVACY PROTECTION

Frank M. Tuerkheimer

The concept of privacy as a separate right was first articulated over 100 years ago when then attorney Louis Brandeis and Samuel Warren wrote an article in the *Harvard Law Review* urging recognition of a right to privacy, or as they so eloquently phrased it, the "right to be let alone" [1]. Law review articles, however, are not the same as legislative acts. For several decades only a scattering of jurisdictions have recognized this right, permitting private tort actions and invasions of privacy. For example, the Court of Appeals for the District of Columbia cited the Brandeis and Warren article as the source of the District's common-law action for invasion of privacy in *Pearson vs. Dodd,* 410 F.2d 701, 703 (1968). Significantly, these early privacy cases do not deal with the question of governmental invasions of privacy, but with civil tort actions brought by one individual against another.

The government's involvement in privacy was the subject of an important Supreme Court decision in *Olmstead vs. United States* [13]. Before discussing this constitutional milestone, it is important to elaborate on an axiom which underlies much of the privacy discussion to follow.

The U.S. Constitution is essentially a limitation on government power. It was written over 200 years ago in an effort to strike a balance between the need for greater governmental authority in the 13 newly independent colonies and the fears that government represented the greatest threat to individual liberty. The founding fathers based their fears on several hundred years of British history during which the Crown fought intensively to retain its political and economic prerogatives.

Ultimately, the Constitution represented the compromise between the twin evils of anarchy and tyranny. The principal mechanism by which this compromise was reached was to separate powers at the federal level into three branches and then to specifically enumerate the totality of those powers, inferentially leaving the remaining powers to the states. This compromise was not enough to ensure adoption of the Constitution. Many were concerned that it did not contain sufficient specific restraints on government power. As a result, 10 amendments, which we call the Bill of Rights, were added to the Constitution.

There can be no doubt that the drafters of the Bill of Rights looked to the British experience and the abuses of the Crown to determine exactly what kind of governmental conduct should be prohibited.[1] One of those abuses was the historical practice of the Crown of invading and searching persons' homes and then utilizing the information obtained in subsequent criminal prosecution. As a result, the Fourth Amendment to the Constitution provides that:

The right of the people to be secure in their persons, house, papers and effects against unreasonable searches and seizures shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.

To understand some of the major privacy issues currently on the national agenda in the U.S., the scope of the Bill of Rights must be examined. Persons generally labeled as "conservative" in legal parlance say judges should not be allowed to expand the protections of the Bill of Rights beyond its specifically enumerated provisions. The argument underlying this view is that judges with lifetime tenure will legislate their own particular views of constitutional scope if allowed to expand the document in that manner. Such judicial legislation is undemocratic and undesirable because federal judges are the government officials least responsible to the electorate.

The opposing view, which was at one time the prevailing Supreme Court view on the Constitution but may no longer be, is that the Constitution represents a broad statement against governmental excess. Thus, it cannot retain any vitality if it is interpreted to prohibit only those excesses engaged in by the British Crown in the 500 years before the American revolution.[2] According to this view, the intent of the writers of the Constitution in limiting government's powers is a guide to its interpretation, not a limitation on it. Some of the leading constitutional cases of the past half century have been predicated on this approach, including *Brown vs. Board of Education* [5] (striking down school segregation), *Griswold vs. Connecticut* [8] (striking down Connecticut's prohibitions on the

[1]For example, the right to cross-examine witnesses was directed against the Crown's practice of convicting political opponents through hearsay witnesses; the right to a jury trial and to a grand jury indictment was designed to preserve the insulation against prosecutorial abuse provided by such citizen intermediaries; the First Amendment guarantees of free speech, petition and assembly were directed at governmental efforts to stifle free speech.

[2]In the milestone case of *McCulloch vs. Maryland,* 4 Wheat. 316, 407 (1819), Chief Justice Marshall set forth the expansionist notion of constitutional interpretation that "we must never forget that is a constitution we are expounding." This notion was articulated in a case upholding government action under the Commerce Clause of the Constitution that was probably beyond what the founding fathers would have articulated as legitimate governmental action.

sale of contraceptives), and *Roe vs. Wade* [15] (striking down prohibitions against abortion). Certainly the latter two contain explicit privacy protection components.

The defendants in *Olmstead* were convicted of violating the National Prohibition Act. Evidence of the defendants' involvement in a large-scale liquor importation and distribution conspiracy originated with a wiretap placed on several of their telephones by federal agents without a court order. The defendants urged that this violated their Fourth Amendment rights. A majority of the Supreme Court held that protection of the sanctity of one's home, governed by the Fourth Amendment, did not apply to telephone communications. Justice Brandeis, the author of the famous *Law Review* article on privacy 30 years earlier, dissented.

Justice Brandeis's dissent was predicated on the notion that the words of the Constitution were designed to "approach immortality as nearly as human institutions can approach it" and that "in the application of a constitution, . . . our contemplation cannot be only of what has been but of what may be" [2]. He readily acknowledged that the Fourth Amendment was directed against invasions of the sanctity of the home, but added that "time works changes, brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the Government. . . . [A] principle to be vital must be capable of a wider application than the mischief which gave it birth. This is particularly true of constitutions" [2].

Brandeis then shifted privacy concepts from the "right to be let alone" value of his earlier article to communications privacy. Relying on a case that applied constitutional protection to the mail, he noted there was no difference between a sealed letter and a private phone call. In fact, "the evil incident to invasion of the privacy of the telephone is far greater" because "the privacy of persons at both ends of the line is invaded. . . . [t]he tapping of a man's telephone line involves the tapping of every other person whom he may call or who may call him" [3]. His synthesis of the two privacy concepts under what he felt should be constitutional protection then followed:

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, 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 men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual whatever the means employed, must be deemed a violation of the Fourth Amendment.[3]

Brandeis's dissent in *Olmstead* became the law in the U.S. approximately 40 years later in *Katz vs. United States* [10]. In overruling the *Olmstead* case, the Supreme Court in *Katz* held that "the Fourth Amendment protects people, not places. . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Because there was a "reasonable expectation of privacy" [11] in connection with a call placed in a public telephone booth, the Fourth Amendment was held to apply, requiring that a court order be obtained before a telephone tap was placed. Legislation specifying the need for a court order to permit a wiretap was then passed. It set forth standards for permitted wiretaps and also for conduct designed to minimize privacy invasions once taps were permitted. Use of information obtained from a tap was also restricted. Thus, under federal law today, for either the federal government or state government to obtain a domestic wiretap, an application must be made to a magistrate or a judge in which the government establishes reasonable grounds to believe such a wiretap will reveal evidence of a crime. (Such taps were obtained and used with great success in the recent conviction of organized crime boss John Gotti in New York City.)

While the wiretap legislation passed in the wake of the *Katz* decision contemplated assistance to law enforcement on a case-by-case basis, the legislation did not require that systems facilitate wire surveillance. The FBI has proposed that communications systems not be wiretap proof. If adopted, such subordination of technology to law enforcement techniques would be a major first.

From *Katz* to the Present

Since *Olmstead* and *Katz*, advances in electronics, computers, and other technologies have accentuated privacy concerns in two broad arenas—surveillance and personal data protection.

The surveillance category embraces, among other things, the government's increasing facility for undetectable electronic wiretapping and monitoring of computer network traffic. The most profound expansion in surveillance monitoring, however, is not governmental but private. Today, businesses routinely monitor employee work habits and personal proclivities by recording keystrokes per minute at employee workstations, by scanning employees' email messages, or by recording the destination, duration and time of outgoing personal phone calls by employees. In the interest of efficiency, airlines instruct their reservation clerks to take reservations in under two minutes "total average talk time (TATT)" [12]. Directory assistance operators are evaluated against a standard that imposes a 29-second average call length [12]. There are even reports of journalists drafting stories at their computers being interrupted by networked supervisors objecting to the author's choice of words [12].

The inclusion of personal information in a myriad of databases and the ease with which one's name, address and personal information are transferred and used for purposes unrelated to the one for which it was originally obtained is a source of great concern. Such lists are often effortlessly integrated with one an-

[3]The inevitable involvement of third parties so feared by Brandeis had led to a requirement to minimize the scope of intercepted material. See [4].

The legislatures in many countries recognize both the political and emotional value of privacy protection

and have, in the last 20 years, adopted a variety of strategies for achieving meaningful protection.

other (often by reference to a common identifier such as the U.S. Social Security Number) to produce rather detailed portraits of individuals and their habits, purchases, histories. Often the individual is unable to avoid inclusion or to correct informational errors.

The legislatures in many countries recognize both the political and emotional value of privacy protection and have, in the last 20 years adopted a variety of strategies for achieving meaningful protection. At the heart of these efforts are a set of guiding principles concerning collection, use and dissemination of personal information.

In the U.S., those principles were articulated in a 1973 report by the Department of Health, Education and Welfare, which proposed a Code of Fair Information Practices for automatic personal data systems.[4] These, however, apply only to the federal government. The following year, Congress passed the Privacy Act, which purported to incorporate the Code in restricting public sector uses of federal, but not state, local or private, records. Yet, in practice the Act has come to be recognized as a weak protector of personal privacy because an exception, which permitted "routine use" of data, has been so widely applied as to diminish the Act's force [6].

The U.S. Congress has passed laws attempting to deal in part with Privacy Act limitations, such as "routine use" and specific subjects not covered by the Privacy Act. These have addressed individual problems with separate pieces of legislation, each of which functions under the broad canopy of the 1974 Privacy Act. In the communications privacy sector, the leading legislation is the Electronic Communications Privacy Act of 1986. That Act requires the government to obtain a court order before intercepting most forms of electronic communications, broadly defined. Exceptions that permit electronic monitoring in the regular course of business and with an individual's prior consent many permit employer monitoring of email systems, though this issue has yet to be settled by a court [9]. Legislation since the enactment of the Privacy Act has not, however, created an effective oversight mechanism to give teeth to existing privacy protections.

In contrast to the U.S.'s approach of adopting specialized legislation to fix particular problems as they arise, other nations have adopted broad prospective data protection codes which may require data collectors to register with the government (UK, Sweden), or may impose a blanket prohibition on public and private data uses without the consent of the data subject (as in a proposed directive by the European Community).

The broad approach to data protection was expressed in a set of Guidelines issued in 1980 by the Organization of Economic Development. The Guidelines, which echo the principles behind the Code of Fair Information Practices, apply minimum standards to data collected, stored, processed or disseminated in either the public or private sector which identifies or could identify an individual. Many member nations and private organizations look to the Guidelines when drafting data privacy laws or policies.[5]

Recently, the European Community has debated adopting a directive that would harmonize the data protection laws of its member states and, restrict transfer of personal data from a member state to another state that lacks "adequate"[6] protection for personal data. Furthermore, a more recent proposal would protect personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network and public digital mobile networks. The new proposal would extend existing principles to the collection, storage and processing of personal data by a telecommunications organization.

It should be apparent from this brief overview of present privacy protections that we are behind. Historically, it is clear that the law has adapted to technological changes, but not at a fast pace. The antecedents of electronic communications had been in place for almost a century by the time *Katz* was decided. The rate of technological change

[4]The five principles underlying the Code are (1) There must be no personal data record-keeping systems whose very existence is secret, (2) There must be a way for an individual to find out what information about him is in a record and how it is used, (3) There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent, (4) There must be a way for an individual to correct or amend a record of identifiable information about him, and (5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens xx (1973).

[5]The U.S. is not a signatory to the Guidelines, though 140 U.S. companies have adopted them. See [14].

[6]The scope of "adequacy" is an obvious source of dispute.

since *Katz* makes it unthinkable that a comparable period will lapse before legal constraints are developed that take into account the extraordinary changes in technology that computer electronics represent.

Certainly, we are not there today. In the U.S. a patch-work of laws deal with smaller problems,[7] but none approaches the breadth of the problem, either at the governmental or the private level. While Guidelines and Codes represent broader efforts in the right direction, these are just guidelines and are not self-enforcing. They do not give anyone a legal claim that can be used across the board to deal with governmental or nongovernmental privacy invasions. We are, then, approaching a crossroads: either legislation with teeth will be enacted or the technological changes will simply swallow up privacy rights. As this task is approached, it must be remembered, however, that privacy is not the sole interest involved.

Countervailing Considerations

A world of total privacy is neither attainable nor desirable. Perhaps the most compelling policy against total privacy is the government's right to prosecute violations of the law. For example, if one's financial records were totally protected by a right to privacy, it would be difficult, if not impossible, for the government to prove tax evasion. Surely, it cannot be contended that the government's power to enforce its tax laws should be subordinated to a citizen's right to privacy so that tax evasion prosecutions would be a practical impossibility.

This illustration is, however, merely part of a larger perspective in law enforcement. If law enforcement is left to investigate only crimes in which neither communications nor data are essential proof, it is unlikely that prosecution of crimes such as murder, assault, rape, and robbery, would be significantly affected. What would be affected, however, is prosecution of business crime. The end result would be a contour to law enforcement that is decidedly class-focused.

Generally speaking, persons commit crimes in the most likely manner to get what they want—usually money or injury to another—in a way least likely to result in detection. Thus, crimes of violence tend to be committed by persons without the means of committing more subtle criminality. The robber of a bank or the mugger on the street does not have the means to steal more quietly. The president of a bank, or a Savings and Loan institution, however, has the luxury of stealing quietly, where not just the criminal, but the crime itself, must be uncovered, unlike the case of the robbery or mugging. If privacy rights precluded the government's ability to obtain information necessary to prosecute the crimes of those with means, the wealthy would essentially be immune from criminal prosecution and law enforcement's efforts would be directed almost totally at the poor.

While investigation and prosecution necessarily require the government to obtain information that might otherwise be private, the government's obtaining of information does not necessarily mean it will be made public. When the government subpoenas bank or other financial records as part of a criminal investigation, these records are subject to the same secrecy constraints that apply to any information obtained by a grand jury.[8] It is only if criminal charges are brought that such data may become public. However, in such cases, the government's interest in enforcing its criminal laws seems paramount. While privacy protections may weaken in the case of criminal investigation, it should be remembered that such an investigation is an exceptional case and establishes no general rule. Moreover, even in the case of a criminal investigation, there are internal privacy constraints such as the need for a warrant and grand jury secrecy.

Not all litigation is criminal litigation. When a person sues for injuries relating to an automobile accident, the person sued has the right to obtain the plaintiff's medical records in an effort to show that either the injuries complained of are not as severe as alleged or that they are attributable to an injury antedating the accident. In such a case, the plaintiff has no valid privacy right to such records, and court process—a subpoena or a formal discovery request is the mechanism by which otherwise confidential information is provided to the defendant and perhaps, ultimately made a part of the public record. It makes no sense to say that the plaintiff, who has placed his or her medical condition in issue, should have a privacy right to keep that condition from being fully litigated. And because it is court process that permits access to otherwise confidential data, the court is available to curb excesses or needlessly broad discovery into the plaintiff's medical condition.[9]

Conclusion

There is little doubt that in the future, many records presently stored in nonelectronic form will be retained in electronic databases. This poses the risk that through networks such records will be accessible to large numbers of persons to whom these records would otherwise be inaccessible. It is axiomatic that whatever privacy protections apply to such records must not be lost simply because the mechanism of retention has changed. Thus, for example, medical or bank records which are afforded privacy protection under existing law[10] should not lose the privacy protection they have under present law simply because the way in which they are stored leaves them vulnerable to electronic detection. The required privacy must be maintained.

There is an inverse to this conclusion. Just as privacy should not be lost when the storage mechanism

[7]Recent U.S. privacy legislation touches many aspects of daily life including arrest records, bank records, cable television billing, computer data banks (public and private), credit reporting, electronic eavesdropping, employment polygraphing, employment records, medical records, school records, social security numbers, surveillance technology, tax records and wiretaps. See [7].

[8]Rule 6 of the Federal Rules of Criminal Procedure makes grand jury proceedings secret and prohibits the participants from disclosing information gained during an investigation. While there are dozens, if not hundreds, of federal grand juries functioning at any one time, grand jury leaks are rare.

[9]The defendant, in an automobile case alleging injury to plaintiff's leg ought not, for example, be able to obtain financial records relating to a digestive disorder.

becomes electronic, privacy rights should not be acquired when otherwise nonprivate records are stored electronically. If business records, for example, are transferred from cumbersome books and ledgers onto an electronic data base, that transfer does not render them subject to privacy constraints simply because they are stored electronically. Otherwise, law enforcement of any kind of business crime would be heavily burdened and for no valid reason.[11]

With respect to communications privacy, the constitutional prohibition against unlawful searches and seizures, held to create a zone of protection within a reasonable expectation of privacy, should and does extend to electronic communications. The 1986 Electronic Communications Protection Act prohibits government interception of electronic communications without probable cause [17]. Similar constraints apply in other countries.[12] Caller-ID technology, which gives the recipient of a phone call access to the source of the call raises additional privacy issues.

Although private wiretaps are also prohibited [16], restraints on private interception of email and network communications are presently not promising in terms of individual privacy protections.[13] Certainly if the "reasonable expectation" standard is the legal basis for private privacy protection, an employer, by notice, can effectively remove such expectation from an employee by simply stating that all information placed on a company computer is the property of the employer, a practice that has been followed.[14] It would follow almost inevitably that if an employer does not so advise an employee, the expectation of privacy would be reasonable.

There is no doubt that we are now at a crossroad. Technology will have a major impact on our lives and values as we understand them, unless we act and act quickly. Those to whom Brandeis's description of privacy and its importance in a civilized society evokes assent do not have much time. The rate of technological change will render privacy obsolete. During the critical period in which we can prevent the destruction of privacy, we cannot proceed on the assumption that those with power share our views and can be counted on to preserve our values. Brandeis saw the pitfall in such hopes as well when he said that "the greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding [13].

We must understand, and we must act.

Acknowledgment

Bennett Berson, a third-year law student at the University of Wisconsin, provided invaluable assistance in the preparation of this article. ■

References

1. Brandeis, L., Warren, S. *The Right to Privacy. Harvard Law Rev. 4,* 193 (1890), 195.
2. Brandeis, L. *U.S. 277,* 473.
3. Brandeis, L. *U.S. 277,* 475–76.
4. Brandeis, L. *U.S. 277,* 478.
5. *Brown vs. Board of Education. U.S. 347* (1954), 483.
6. Flaherty, D. Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada and the U.S. 306 (1989).
7. Freedman, The Right of Privacy in the Computer Age, 93 (1987).
8. *Griswold vs. Connecticut. U.S. 381* (1965), 479.
9. *Harvard Law Rev. 104,* Addressing the New Hazards of the High Technology Workplace, 1898, 1906 n.66–70 (1991).
10. *Katz vs. U.S., U.S. 389* (1967), 347.
11. *Katz vs. U.S., U.S. 389* (1967), 353.
12. Nussbaum, K. In *The First Conference on Computers Freedom and Privacy Proceedings 128* (1991).
13. *Olmstead vs. United States. U.S. 277* (1928), 438.
14. Plesser, R. *First Conference on Computers, Freedom and Privacy Proceedings 28* (1991).
15. *Roe vs. Wade. U.S. 410* (1973), 113.
16. *U.S.C. 18,* Section 2511.
17. *U.S.C. 18,* Section 2518 (3).

CR Categories and Subject Descriptors: K.4.1 [**Computers and Society**]: Public Policy Issues—*privacy*; K.5.2 [**Legal Aspects of Computing**]: Governmental Issues

General Terms: Legal Aspects

Additional Key Words and Phrases: Privacy and Bill of Rights, privacy and Constitution

About the Author:

FRANK M. TUERKHEIMER is the Habush-Bascom Professor of law at the University of Wisconsin. His research interests include the interplay between the right to privacy and modern technology. **Author's Present Address:** University of Wisconsin Law School, Madison, WI 53706

[10]See, for example, the Ban Secrecy Act, codified at 12 U.S.C. 1829b which requires banks to retain certain private records useful in criminal prosecution.

[11]As a parallel, documents otherwise producible pursuant to subpoena do not lose their discoverable status simply because they are transferred to an attorney. The attorney/client privilege covers confidential communications, but does not make the attorney an impregnable warehouse to documents antedating such communications.

[12]*See, e.g.,* Japanese Constitution, art. IIIV.

[13]The first case on the subject is believed to be *Shoars vs. Epson* (SWC 112749).(A group of employees sued Epson America for invasion of privacy under Cal. Penal Code Sec. 631. Shoars alleged that Epson management routinely read her email. After protesting this policy, Shoars was fired.)

Under an exception to ECPA's general prohibiting against interception of electronic mail, Epson's actions might be legal. See 18 U.S.C. 2511(2)(a)(i) (permits officers, employees, or agents of electronics communication services to intercept and use such communications "in the normal course of his employment while engaged in any activity which is necessary incident to . . . the protection of the rights or property of the provider"). The court ultimately ruled that the California statute did not cover email. Several additional cases against employers for similar violations are now pending in the California courts.

[14]The Electronic Mail Association (EMA) offers useful material entitled "Access to and Use and Disclosure of email on Company Computer Systems: A toolkit for Formulating Your Company's Policy" is available from the EMA, 1555 Wilson Blvd., Arlington, VA 22209; (703) 875-8620.