Catholic University Law Review

Volume 25
Issue 4 *Summer 1976*

Article 8

1976

Privacy Rights and Electronic Funds Transfer Systems – An Overview

Phillip J. Scaletta

PRIVACY RIGHTS AND ELECTRONIC FUNDS TRANSFER SYSTEMS—AN OVERVIEW

*Phillip J. Scaletta**

During the past two decades, Americans have been faced with an information explosion that threatens to drown them in a sea of paper. Contemporary technology, however, affords a solution in the computer. In little more than a score of years, our society has experienced a computer revolution. The computer has evolved from a sophisticated adding machine into a complicated system for the processing, manipulation, retrieval and transmission of data. Today we depend on the computer in every aspect of modern life.

While the computer has been a great boon for mankind, it has also created new legal problems. The most serious problem is the threat of encroachment upon individual privacy. Today's computers have an almost infinite capacity for storing, retrieving and transmitting information. Information may now be entered into a computer which can assemble the information and transmit it to other computers anywhere in the world. Compatible electronic storage units harnessed through telephone networks or other transmission devices have created a potential surveillance system of a magnitude and comprehension heretofore impossible.

With this new technological capacity to store and retrieve data, there comes a seemingly insatiable desire on the part of government and business to gather and store information on everything and everyone. Information which previously demanded thousands of square feet can now be stored on only a few thousand feet of magnetic tape. The computer can then search the tapes in seconds and provide a printout or display of the information. As a result, financial, commercial, and governmental institutions, among others too numerous to mention, have been amassing great amounts of personal information about individuals.

Some records about individuals have always existed. Most have contained such facts as name, date and place of birth, occupation, address, and telephone number. Today many records are more subjective, such as records

* Professor of Business and Labor Law at Krannert Graduate School of Industrial Administration, Purdue University. B.S., 1948, Morningside College; J.D., 1950, University of Iowa.

of credit transactions, recommendations, credit ratings, ownership of real and personal property, arrests, and law suits. These items are considerably more sensitive and of more concern to the individual. Thus, their revelation to unauthorized sources seriously violates an individual's privacy. We are not only experiencing a computer revolution, therefore, but an information revolution.

In the past, informational privacy was not a serious problem for a number of reasons:

> (1) large quantities of information about individuals had not been collected, and therefore, have not been available; (2) available information was relatively superficial in character and often was allowed to atrophy to the point of uselessness; (3) the available information generally was maintained on a decentralized basis; (4) access to available information was difficult to secure; (5) people in a highly mobile society were difficult to keep track of; and (6) most people are unable to interpret and infer the revealing information from the available data.[1]

In our highly computerized environment these conditions no longer exist, and privacy is difficult to protect.

One of the foremost advocates of legislation designed to protect an individual's privacy, Senator Sam Ervin, Jr., in a speech before the United States Senate on February 8, 1971, said:

> It has become increasingly clear that unless we take command now of the new technology with all that it means in terms of substantive due process for the individual who is computerized, we may well discover some day that the machines stand above the laws. By then, it will make no difference who mans the systems or what political party makes use of them, for the pattern of mechanized surveillance will have become so institutionalized throughout our land that it may defeat the ingenuity of the God-given powers of man to alter our national course. "Liberty" will then sound only as a word in our history books, the lamented dream of our Founding Fathers.[2]

Professor Arthur Miller, in a statement to the Senate Judiciary Subcommittee on Constitutional Rights on February 23, 1971, stated:

> First, Americans are scrutinized, measured, watched, counted, and interrogated by more governmental agencies, law enforcement officials, social scientists, and poll takers than any time in our history. Second, probably in no nation on earth is as much individualized

1. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information Oriented Society*, 67 MICH. L. REV. 1091, 1108 (1969).

2. 117 CONG. REC. 2024 (1971).

> information collected, recorded, and disseminated as in the United States. Third, the information gathering and surveillance activities of the federal government have expanded to such an extent that they are becoming a threat to several basic rights of every American—privacy, speech, assembly, association, and petition of the government.[3]
>
> . . . .
>
> At present there are no effective restraints on the national government's information activities and no one has undertaken to ensure that individuals are protected against the misuse of the burgeoning data banks.[4]

Professor Miller suggested that legislative action by Congress was necessary to prescribe technical and procedural safeguards for data bank systems. Congress should establish some regulatory group outside present administrative channels that can limit the type of information to be collected and stored, ensure the accuracy of the data, guard against breaches of security, and provide the individual with some degree of control over his file.[5] This concern over the control and use of sensitive information has prompted considerable discussion, legislation and litigation.

I. Historical Background to the Right of Privacy

Where does one look to find a legal right to privacy? The United States Constitution explicitly guarantees freedom of speech, freedom of religion, and freedom of assembly, but where does it grant the freedom "to be left alone"; the freedom from invasion or unwarranted intrusion into our personal affairs; the right to determine when, how, and to what extent data about us is communicated to or used by others; the protection from harm or damage as a result of the operation of a record system; the protection from unwelcome, unfair, improper, or excessive collection or dissemination of information about ourselves? The Bill of Rights evidences the concern of the framers of the Constitution for the privacy of an individual in certain areas. For example, the third amendment prohibits the quartering of soldiers in homes without the consent of the owner. The fourth amendment protects people against unreasonable searches and seizures of their persons, papers, homes and effects. The fifth amendment prohibits the government from forcing one to be a witness against oneself in a criminal trial. However, the concept of lib-

3. *Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. 32 (1971).

4. *Id.* at 35.

5. *Id.* at 37-40.

erty embodied in the Bill of Rights was limited to the person and his physical property, since the current myriad of informational privacy problems were unforeseeable at that time. In addition, the Constitution protects individuals only from governmental action and does not speak to the actions of individuals. Thus, the Constitution does not afford the individual the right to privacy which he now needs.

In 1890, Samuel Warren and Louis Brandeis wrote an article entitled "The Right to Privacy"[6] in which they argued strongly that each individual has an inherent right to privacy, a right which protects one from unwarranted intrusion into the circumstances of one's personal life. The authors were concerned not only with governmental threats but also nongovernmental threats to privacy. They felt the individual should have a remedy at law if his privacy were invaded. Obviously they could not have anticipated the problems created by today's technology; however, their article was the cornerstone upon which our judicial system constructed a right to privacy.

In the 86 years since the publication of "The Right to Privacy," there have been a plethora of cases brought in the name of individual privacy. These cases have involved nearly every conceivable aspect of privacy. In the mid-1960's, however, the public concern about the loss of personal privacy dramatically increased. The federal government proposed a National Data Center which would have centralized all governmental files into one massive data bank. While the economic advantages of data centralization may be great, such a centralized data bank poses a further threat to individual privacy.

The threat is no longer simply one of unauthorized access to the papers or effects of the individual. Rather, the problem now presented is the right of an individual to control the distribution of information about himself, regardless of whether the information was voluntarily given. This is a new concept of privacy which can be termed informational privacy.

Numerous books and articles were written warning of the dangers of the computer.[7] For the first time, the public became aware of its inability to determine the content, distribution and accuracy of its records. Public

---

6. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

7. *See Hearings, supra* note 3; HEW SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973); A. MILLER, THE ASSAULT ON PRIVACY (1971); J. RULE, PRIVATE LINES AND PUBLIC SURVEILLANCE (1973); M. STONE & M. WARNER, THE DATA BANK SOCIETY: ORGANIZATIONS, COMPUTERS, AND SOCIAL FREEDOM (1970); A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORDKEEPING, AND PRIVACY (1972); S. WHEELER, ON RECORD: FILES AND DOSSIERS IN AMERICAN LIFE (1969); Lusky, *Invasion of Privacy: A Clarification of Concepts*, 72 COLUM. L. REV. 693 (1972); Note, *Privacy in the First Amendment*, 82 YALE L.J. 1462 (1973).

awareness and pressure from citizens groups brought prompt legislative action to protect the individual. In 1970, Congress passed the Fair Credit Reporting Act.[8] This Act gave the consumer the right to see the credit file compiled

8. Senate Bill 823, entitled the Fair Credit Reporting Act, was aimed at the abuses by credit bureaus which became obvious during data bank hearings. The bill, incorporated with H.R. 15073 and S. 721, was passed by both houses and sent to the President for signing on October 26, 1970. The Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1127 (codified at 15 U.S.C. § 1681 *et seq.* (1970)), was signed and became effective on April 25, 1971. The following is a digest of some of its pertinent provisions:

(a) The new law authorized credit reporting agencies to furnish credit information only in connection with credit, insurance, and employment applications, a government license for which a consumer had applied, or any other business transaction in which a consumer was involved, and only by written consent of the consumer involved or in compliance with a court order.

(b) The reporting of adverse information about arrests and other matters regarding suits more than seven years old is generally prohibited. Bankruptcy is an exception, for information may be available for 14 years. If the inquiry concerns an application for a life insurance policy of $50,000 or more, or an application for a job with an annual salary of $20,000 or more, there is no such restriction on records and all information may be furnished. The bureaus, therefore, have an excuse not to delete the information entirely.

(c) The reporting of adverse information from investigative reports more than three months old, unless the information is reverified, is generally prohibited.

(d) The law requires all reporting agencies to "follow reasonable procedures to assure maximum accuracy of the information" contained in reports.

(e) The type of information which can be furnished to government agencies without a court order is limited.

(f) Upon the request of a consumer, a reporting agency must disclose to the consumer all information about him in the agency's files or the sources of such information, except medical information.

(g) A person or business ordering an investigative report must notify the consumer that an investigation is being made.

(h) An agency must disclose to a consumer on request the names of persons and businesses who have furnished credit information about the consumer in the preceding six months (two years for employment purposes).

(i) Agencies must reinvestigate disputed information unless there are "reasonable grounds to believe that the dispute by the consumer is frivolous or irrelevant." If the information is inaccurate, the bureau must delete the information from the record. The consumer has the right to have the agency or bureau put in the file a statement of not more than 100 words explaining disputed information and have the agency send copies of the statement to the persons and businesses to whom the disputed information was previously sent.

(j) A person or business rejecting a consumer for credit, insurance or employment on the basis of a credit report must advise the consumer of the fact and identify the reporting agency.

(k) A consumer is given a civil cause of action to recover damages resulting from willful and negligent noncompliance with the law.

(l) Obtaining information under false pretenses and willfully giving out such information to unauthorized persons is punishable by a fine of up to $5,000 and imprisonment for up to one year.

on him, to correct or explain any misleading or incorrect information, and to know why he was denied credit. The law also limited access to the records to specific parties for specific purposes. In 1971, then Secretary of Health, Education and Welfare Elliot Richardson formed the Secretary's Advisory Committee on Automated Personal Data Systems. The Committee consisted of computer experts, prominent educators, and state politicians. The Committee's report, "Records, Computers and the Rights of Citizens,"[9] issued in 1973, set forth recommendations for the proper handling of personal information, and the policies and procedures to be used by federal agencies.[10]

In addition, in the Ninety-third Congress some 200 bills were introduced concerning various privacy invasions by electronic data processing systems.

---

9. *See* note 7 *supra.*

10. The HEW report stated that "privacy" entails control by the individual over the uses made of information about himself. The report recognized, however, that in many circumstances in modern life, an individual must either surrender some of that control or forego the services that an agency provides. Although there is nothing inherently unfair in trading some measure of privacy for a benefit, the Report continues, both parties to the exchange should participate in setting the terms. In other words, even though an individual chooses to give up certain information about himself in order to obtain a benefit, he still has the right to expect that the information made available will be recorded accurately and will not be misused. *Id.* at 38-40. These expectations form the basis for the "principles of a code of fair information practices" which are set out in the HEW report:

> There must be no personal data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> There must be a way for an individual to prevent information obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> 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 reasonable precautions to prevent misuse of the data.

Id. at 41.

In addition to the above, two other principles must be considered—relevancy and timeliness. Data should be collected by an agency only if it is directly related to its function of carrying out an existing law or regulation. *Id.* at 79. "[W]hen personal data are collected for administrative purposes, individuals should under no circumstances be coerced into providing additional personal data that are to be used exclusively for statistical reporting and research. When application forms or other means of collecting personal data for an administrative data system are designed, the mandatory or voluntary character of an individual's response should be made clear." *Id.* at 85. Data should not be maintained by an agency when the purpose for which it was collected has ceased or when the data is no longer relevant. *Id.* at 56-57. Obsolete data may be retained for "archival purposes" but should "not [be] available for routine use." *Id.* at 57.

Finally, the Privacy Act of 1974[11] was enacted in the closing days of that Congress. The new law established a Federal Privacy Protection Study Commission and placed many restrictions on recordkeeping and handling. This law, however, only applied to federal government agencies.

In the Ninety-fourth Congress, shortly after the Privacy Act became law, Congressmen Edward Koch and Barry Goldwater, Jr. introduced the Comprehensive Right of Privacy Act.[12] This bill would extend the provisions of the Privacy Act of 1974 to cover private institutions and would require adherence to the "principles of fair information practices: similar to those outlined in the HEW report."[13] The bill would also establish a federal privacy board with extensive powers to regulate and control personal data and information systems.

It is important to note that neither the Privacy Act of 1974 nor the Koch-Goldwater bill would preempt state legislation or create a moratorium on additional legislation. Many states have introduced privacy bills in their current legislative sessions. The various state bills that mirror or extend the federal proposal are best characterized as "omnibus" because of their scope. They seek to regulate with a single legislative approach all individual and organizational handling of personal information. Five states, Arkansas, Massachusetts, Minnesota, Utah and Virginia, have already enacted privacy laws[14] and a majority of other states have privacy bills pending. Some have omnibus laws that include the private sector.[15] Many of these laws also create commissions to administer the statutes or study and report on the privacy issue to the legislatures.[16] Thus privacy is certainly a key issue in our society today.

---

11. 5 U.S.C. § 552a (Supp. IV, 1974). The new law, which became effective on September 27, 1975, gives the individual access to records concerning himself, and the right to copy, correct and challenge personal information held by the federal government. The existence, nature and scope of all federal government files containing personal data is required to be published in the *Federal Register*. The Act also prohibits nonroutine dissemination of records without notification of the individuals involved. Restrictions have also been placed upon the expanded use of the social security number. The Act establishes a Privacy Protection Study Commission to study and make recommendations on data banks and information processing programs in both the government and the private sector.

12. H.R. REP. No. 1984, 94th Cong., 1st Sess. (1975).

13. *See* note 10 *supra*.

14. ARK. STAT. ANN. § 16-806 (Supp. 1975); MASS. GEN. LAWS ANN. ch. 66A §§ 1-3 (Supp. 1976); MINN. STAT. ANN. § 15:165 (Supp. 1976); UTAH CODE ANN. §§ 63-50-1 *et seq.* (1968); VA. CODE ANN. § 2.1-382 (Supp. 1976).

15. *See, e.g.*, MINN. STAT. ANN. § 15:169 (Supp. 1976).

16. *See, e.g., id.*

II. Electronic Funds Transfer Systems—Privacy Implications

The cashless society is no longer simply an esoteric concept; it is fast becoming a reality. Electronic funds transfer systems (EFTS) are in use in varying degrees all over the country. The systems range from the relatively simple process involving automatic cash machines, which allow customers to withdraw cash from their accounts after bank closing hours, to very sophisticated systems which transfer checks and other commercial paper via electronic impulses for clearing house purposes. The most advanced system is the point-of-sale delivery system (POS) wherein a terminal, either manned or unmanned, is installed in a retail establishment and connected with a banking institution. When the customer activates the machine with his card and code, his account is immediately debited. Other systems presently in use automatically debit mortgage payments and deposit payroll checks.

An EFTS is a technological innovation which will save many hours of check processing. The advantages of electronic funds transfer over the traditional cash or check transfer of funds are many, but there are also many social and legal problems which must be resolved, particularly the protection of individual privacy and autonomy. The fear that the individual will become the pawn of the system with no rights in it and no access to it is being voiced by many critics.

The records kept on an individual in an EFT system will be considerably different from the traditional records. For example, a comprehensive EFT system will necessitate massive storage of data about individuals and their financial transactions. It will be necessary for credit purposes to have data about assets, debts, business activities, possessions and many other sensitive bits of information. This data must be susceptible to easy, fast retrieval, thus creating the potential for access by unauthorized persons. Ralph Nader's Public Interest Research Group claims that the financial profiles of individuals and organizations in an EFT system would be of great commercial value and subject to possible theft or unauthorized transfer.[17] One illustration suggested by the Nader organization was that the parent bank in a bank holding company which had a centralized computer facility would have an incentive to make data available to subsidiary businesses, such as an insurance company, a travel bureau, or a leasing company.[18] Computerized transfers of data are hard to detect and prevent. Since we have already experienced

17. Statement of John Brown, *Hearings on Customer-Bank Communication Terminals before the Comptroller* 105-07 (1975).

18. *Id.*

scores of examples of computer abuse and computer theft,[19] what guarantee does the individual have that his private information will not get into the wrong hands?

Consumers are demanding safeguards to insure that information concerning the individual and his financial transactions not be improperly used or made available to unauthorized persons. Such safeguards are not presently required by any federal law, and the privacy provisions in the state EFT laws are for the most part superficial.[20] These privacy provisions relate primarily to the problems of disclosure of information to unauthorized individuals. An equally serious problem involves the use of the data in an EFT system for internal bank purposes, such as mailing.

Another consideration is the consumer's control over his own file. What if a machine or programming error occurs? What control does the consumer have? Does the consumer have a right to see his data file and correct or delete mistakes? Does he have a right to know who has had access to his file? How many remote terminals will have access to the main data bank? How much data is kept on each individual? Is every request for data filled with a complete copy of the file? The consumer will no longer have a record of checks he writes because there will be no more checkbooks. How will the consumer know if his bills have been paid by the bank? These are only a few of the fears concerning the lack of consumer control inherent in electronic funds transfer systems.

It becomes immediately apparent that these problems are not new and not particularly indigenous to EFTS. They are problems which will arise in any computerized data system containing sensitive information on individuals. What then is different about EFTS? The answer is simply that the present privacy law has not been applied to EFTS and, therefore, action must be taken to protect the privacy of this sensitive information.

A. EFTS Legislation: Passed and Pending

The Ninety-third Congress created a National Commission on Electronic Funds Transfers in 1974.[21] This 26-member commission was charged with the task of studying the various problems of electronic funds transfer systems and recommending appropriate legislation for the development of public or private systems. One of their prime considerations was the need to afford

19. *See* Bequai, *A Survey of Fraud and Privacy Obstacles to the Development of an Electronic Funds Transfer System*, 25 CATH. U.L. REV. 766 (1976).

20. Florida is the only state with extensive consumer protection provisions. FLA. STAT. ANN. § 659-062(13) (Supp. 1975). Iowa protects consumers to a lesser extent. IOWA CODE ANN. § 524:1211 (Supp. 1975).

21. 12 U.S.C. §§ 2401-08 (Supp. V, 1975).

maximum privacy and confidentiality to both users and consumers, while protecting their other legal rights. This report, however, is not due until October 28, 1977.

On the state level there has been a flurry of enabling legislation to allow electronic fund transfers in the various states. Twenty-one states enacted statutes in 1975.[22] Washington, Massachusetts, Oregon and Wisconsin already had enabling laws on the books and many other states have bills pending. These state laws, however, do not reflect a concern for privacy; rather, they amend the various state banking laws to give financial institutions the legal power to develop EFT systems. Privacy concerns have received only cursory treatment.[23] Thus there is an urgent need for specific federal or state legislation to protect the privacy of the individual whose personal data is being used in an EFT system. The present safeguards are clearly inadequate.

B. A Recent Court Decision Affecting EFTS

On April 21, 1976, the Supreme Court in *United States v. Miller*,[24] by a 7-2 majority, found that an individual's right of privacy did not extend to microfilmed records of his bank account when they were demanded from his bank by the Internal Revenue Service pursuant to the Bank Secrecy Act. Justice Powell, speaking for the majority, felt that the records did not constitute the property or private papers of the depositor and thus were not protected by the fourth amendment provision against unreasonable searches and seizures.[25] The Court also felt that there was no reasonable expectation of privacy by the depositor because the records subpoenaed consisted of checks and deposit slips, which are not confidential communications but negotiable instruments to be used in commercial transactions.[26] At first blush this decision would seem to be a drastic departure from the liberal trend toward privacy which appeared to be developing. However, the character of a check as a negotiable instrument, not a private document, may have been decisive in the Court's view, thereby narrowing the significance of the holding.

An EFTS file will contain information other than checks and deposit slips, and much of this information will be of a confidential and sensitive nature.

22. These states are: Alabama, Connecticut, Florida, Georgia, Idaho, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Nebraska, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Utah, Virginia, Washington and Wisconsin.

23. *See* Privies, The Explosion of State Laws on Electronic Fund Transfer Systems: Its Significance for Financial Institutions, Non-Financial Institutions and Customers, Harvard University Program on Information Technologies and Public Policy (1976).

24. 96 S. Ct. 1619 (1976).

25. *Id.* at 1623.

26. *Id.* at 1623-24.

Miller, therefore, may not represent a statement of the Court's thinking in regard to EFTS and the privacy of sensitive and confidential information contained therein. That issue seems, as yet, undecided.

III. Conclusion

No one seems to oppose drastically the concept of informational privacy, other than on the basis of the cost of such protection, but little has been done realistically to solve these problems. The Privacy Act of 1974 and the Fair Credit Reporting Act are now in effect, and a few states have passed privacy laws, but many areas are still completely unregulated. No law compels the privacy of confidential information in EFT systems. If the individual is to have a meaningful right of informational privacy, regulation concerning privacy should extend to any person or organization, governmental or nongovernmental, who obtains or uses information on individuals. Without such broad legislation the right of informational privacy for the individual will be an empty one.