Buffalo Law Review

Volume 25 | Number 1 Article 3

10-1-1975

Computerized Medical Records and the Right to Privacy: The Emerging Federal Response

Barry B. Boyer
University at Buffalo School of Law, boyer@buffalo.edu

COMPUTERIZED MEDICAL RECORDS AND THE RIGHT TO PRIVACY: THE EMERGING FEDERAL RESPONSE

BARRY B. BOYER*

INTRODUCTION

Only a few years ago, the issue of "computers and the right to privacy" was regarded as more appropriate for sensationalized speculation in the mass media than for serious analysis and policy debate. Events, however, have shown that intimate personal information, in a variety of uses and misuses, can powerfully affect the political fabric of society as well as the lives of individuals. Disclosure of governmental abuses such as the attempt to steal the records of Dr. Daniel Ellsberg's psychiatrist,[1] the admission that political "enemies lists" had been compiled to single out individuals for government harassment or disfavor,[2] and repeated allegations that military and law enforcement agencies have constructed massive surveillance dossiers on citizens engaged in political activity,[3] have all contributed to a growing realization that erosion of personal privacy can easily threaten freedom and the exercise of fundamental political rights.

While the computer was only a minor accessory to these highly publicized abuses—at most, a sophisticated filing cabinet—the surveillance-and-harassment incidents do serve to illustrate a more basic problem in contemporary organizations: the individual's loss of control over personal information that affects his life, as secret decisions are made by unaccountable decision-makers on the basis of wrong or

* Associate Professor of Law, State University of New York at Buffalo; J.D., University of Michigan, 1969. Portions of the research for this article were supported by a grant from the Christopher Baldy Fund, State University of New York at Buffalo. In addition, I am indebted to Prof. Arthur R. Miller of the Harvard Law School, Prof. Mary Kay Kane of the State University of New York at Buffalo, Ms. Margaret Gilhooley of the Administrative Conference of the United States, and the members of the Joint Task Group of the Medical Society of the County of Erie, New York, for their assistance in making thoughtful comments on earlier drafts of this article and providing relevant materials.

1. *See, e.g.*, N.Y. Times, April 28, 1973, at 1, col. 4.

2. *See, e.g.*, N.Y. Times, June 27, 1973, at 49, cols. 1-2; N.Y. Times, June 28, 1973, at 1, col. 5.

3. *See, e.g.*, C. PETERS & T. BRANCH, BLOWING THE WHISTLE: DISSENT IN THE PUBLIC INTEREST 43-76 (paper ed. 1972) (army surveillance of civilian political activity); The Washington Post, Jan. 19, 1975, at A-1, col. 7 (FBI collection of dossiers on members of Congress); The Washington Post, Dec. 24, 1974, at A-1, col. 7 (allegations of CIA surveillance of domestic political activity).

irrelevant or improperly gathered personal data. In this general trend, the computer is a key element. Increasingly complex institutional functions and relationships in public welfare and law enforcement programs and in private commercial dealings generate demands for correspondingly complex information systems. Computer technology meets this need by making it cheaper and more convenient for organizations to store, retrieve, analyze, transfer, and lift out of context great quantities of personal information. In the process, it may also threaten the congeries of interests encompassed in the phrase, "the right to privacy."[4]

The difficulties of trying to assess the computer's threats to personal privacy, and of trying to devise remedies for these perceived risks, are clearly demonstrated in the health care professions. Within the past decade, both the practice and the financing of medicine have changed markedly, and change seems likely to continue in the near future. As will be seen in the following section, computerization has been prominently involved in many recent developments in health care, including standardization and automation of clinical records, biomedical and social research, and, most dramatically, in the proliferation of "third-party payment" mechanisms to spread the cost of health care. Each of these areas poses different privacy questions, involving different tradeoffs between the privacy interests of the individual data

4. *E.g.*, Miller, *The Right of Privacy: Data Banks and Dossiers*, in PRIVACY IN A FREE SOCIETY (Final Report of the Chief Justice Earl Warren Conference on Advocacy in the United States) 72, 83 (1974):

> The very real benefits conferred by information technology may opiate our awareness of the price that may be exacted in terms of personal freedom. It thus seems desirable to . . . arouse a greater awareness of the possibility that the computer is precipitating a realignment in the patterns of societal power and is becoming an increasingly important decision-making tool in practically all of our significant governmental and nongovernmental institutions. As society becomes more and more information oriented, the central issue that emerges to challenge us is how to contain the excesses and channel the benefits of this new form of power.

However, Professors Baker and Westin, after studying a variety of computer systems handling personal information, reported:

> In a majority of the organizations we visited, our clear finding is that the content of computerized records about individuals has *not* been increased in scope compared to what was collected in their manual counterparts during the precomputer era. The explanation for this lies in a combination of two factors —managerial intentions and the state of the computer art during the past 15 years.

A. WESTIN & M. BAKER, DATA BANKS IN A FREE SOCIETY 244 (1972) [hereinafter cited as WESTIN & BAKER]. They also concluded that information which is considered most sensitive in an organization tends not to be computerized. *Id.* at 249. They also concluded that precomputer rules and practices tend to persist after an information system is computerized. *Id.* at 253.

subject and the social or organizational interest in the free flow of patient records. Medical data poses this efficiency-privacy dilemma in a particularly acute form: for the great majority of people, records of physical or mental illness are the most sensitive kinds of personal information that will ever be systematically collected, yet widespread access to medical records is vitally important in treatment, in research, in the formation of public policy, and in compensating the victim of accident or disease.

The spread of computers into various specialized fields of medical record-keeping also raises questions about the ability of the legal system to control a technology which tends to ignore geographical and jurisdictional boundaries, blurs the distinction between the public and private sectors, and insulates decisions behind a layer of technical obscurity. The traditional legal doctrines applicable to medical privacy, the physician-patient privilege and the common law right to privacy, are largely irrelevant to questions that arise in automated medical data systems. In place of the old doctrines, new general principles are becoming widely accepted as the basis for protecting informational privacy: there must be no secret data systems; the individual must be able to find out what information about him is recorded, must consent to uses beyond the original purposes for which the data was collected, and must be able to correct erroneous information in his file; and the data collecting organization must assure the reliability of personal data and prevent misuse of it.[5] However, as these principles are adopted and elaborated in legislation like the federal Privacy Act of 1974,[6] it is becoming apparent that the effectiveness and costs of implementing these goals in particular fields such as medical record-keeping remain highly debatable. At most, the recent legislative activity is only a first, cautious step in the search for a workable system of controls for the uses and abuses of sensitive personal data.

I. Medical Records and Record-Keepers

The spread of the computer into medical record-keeping is a relatively recent phenomenon, and one that has been poorly documented. Thus, generalizations about the computer's impact on medicine are

5. *See* HEW, Records, Computers and the Rights of Citizens xx-xxi (Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health, Education and Welfare, July, 1973) [hereinafter cited as HEW Report].

6. *See* text accompanying notes 232-308 *infra.*

hazardous. Nevertheless, a few examples of automated data systems that have been developed or planned in the health care field can illuminate the institutional relationships and imperatives that give rise to computerization of medical records, and the information-handling practices that may pose threats to individual privacy.

In general, medical data systems can be divided into three categories: those that are used in direct support of clinical care; those that are devoted to statistical research and policy planning applications; and those that are employed in the process of providing payment for medical treatment. While these functions are often combined in a single information system, each kind of record-keeping poses sufficiently distinct problems to warrant separate consideration.

A. *Computers in Clinical Medicine*

As the practice of medicine has changed in recent decades, the medical record has become an increasingly important determinant of the quality of health care. A major force affecting the character and use of clinical records has been the "knowledge explosion" in biomedical research, the proliferation of general information relevant to the treatment of a particular illness. Some observers have estimated that the average rate at which new information is being compiled throughout medicine is about 5 percent compounded annually,[7] and in some areas of intensive research the growth rate has been much higher.[8] If this estimate is accurate, the amount of "total clinical knowledge" relevant to medical treatment is now more than eight times larger than it was in 1930.[9]

Medicine has responded to the proliferation of knowledge in part by lengthening the education of doctors. However, this strategy has met obvious limitations of time, cost, and effectiveness: already, some commentators have observed, we have reached the point at which "much of the information [a medical student] acquires is obsolete

---

7. 1 JOINT TASK GROUP OF THE MEDICAL SOCIETY OF THE COUNTY OF ERIE, MEDICAL PRIVACY AND COMPUTER TECHNOLOGY 70 (1974) [hereinafter cited as MEDICAL PRIVACY AND COMPUTER TECHNOLOGY].

8. *E.g., id.*:

> If we take the state-of-the-art of 1930 as a fixed point of comparison, by 1972, our factual knowledge on sickle cell disease has increased 18.2 times. Similar studies in opthalmology (retina detachment), cardiology (subacute bacterial endocarditis), neurology (cord bladder), and hepatology (viral hepatitis) showed similar spectacular growth figures, ranging from 6 to 20 times more specific information today, when compared to the 1930 level of information.

9. *See id.* at 71.

before he completes his residency."[10] Instead, the dominant strategy of the profession has been to fragment the practice of medicine into increasingly narrow specialties and subspecialties, so that the amount of data to be mastered by the physician could be kept within reasonable bounds. But the increasing specialization among physicians means that the individual patient must seek treatment from a wide variety of experts, and often a single episode of illness will require the skills of several different types of medical specialists. As each of these specialists begins treatment, he must bring together relevant information about past treatment and present condition: such record linkage "often increases the meaning of current observations by placing them in time context,"[11] or warns the treating physician of potentially dangerous situations such as drug sensitivities.

The actual records that are needed for diagnosis and treatment will likely be scattered about in different doctors' offices, clinics, laboratories, and hospitals, and often can be obtained only with great difficulty or delay. Indeed, given the extreme mobility of the American people,[12] the records may well be located in different states or foreign countries. Usually, the patient himself is required to perform the necessary record-keeping. The results of using the patient to perform the record-linking function are frequently dismal, since he may never have received sufficiently detailed information about his own condition in the course of previous treatment.[13] Even if he did receive the relevant data, it may have become badly distorted in his memory:

> The diagnostician is often frustrated by the "soft" data and notoriously inaccurate presentation of past medical history. Many patients can recall the post-operative discomfort, the cold food, or the friendliness of a nurse better than the exact reason for or the nature of the surgery performed. Many patients offer a vivid description of the color, size, or taste of their medication, but cannot recall the name and/or dosage of the drug. Besides the notoriously poor quality of historic information presented by many patients, sometimes it is not

10. Austen & Kinney, *The Content of Undergraduate Medical Education,* in THE FUTURE OF MEDICAL EDUCATION 71, 73 (J. Graves ed. 1973).

11. *Id.* at 67.

12. Recent statistics indicate that the average American moves his residence about 14 times in his lifetime; each year some 40 million Americans change their addresses at least once, and more than a third of these move across county or state lines. V. PACKARD, A NATION OF STRANGERS 6-7 (1972).

13. For a discussion of patients' difficulties in getting access to their own records, see Kaiser, *Patients' Right of Access to Their Own Medical Records: The Need for New Law,* 24 BUFFALO L. REV. 317 (1975).

> good medical judgment to burden the patient with his own diagnosis, treatment, or prognosis.[14]

Computer-communications systems are an attractive alternative to the inefficiencies of existing methods for linking and retrieving dispersed patient records. With existing technology,[15] the individual's medical history can be uniformly documented, centrally stored in machine-readable form, quickly accessed, and transmitted nationally or even internationally in seconds via telecommunications channels.[16] Automated data processing systems can also be delegated responsibility for performing a variety of routine hospital and office chores, with potentially lower costs and greater reliability than their human counterparts. Clinical computing systems have been developed or proposed to verify prescriptions against average dosage levels, continuously monitor the patient's condition, remind nurses of medication schedules and check their compliance,[17] and scan large numbers of patient files to identify individuals who may be unusually vulnerable to impending illness.[18] Finally, a different kind of clinical computing system can help

---

14. MEDICAL PRIVACY AND COMPUTER TECHNOLOGY 68. The patient's difficulty in communicating relevant information about his past medical history may be complicated by the record-proliferation that is said to result from "practicing defensive medicine." It has been asserted that fear of malpractice liability induces some physicians to perform more diagnostic tests and procedures than they believe necessary, and to document treatment with great thoroughness, in the belief that these steps can help to avoid or minimize malpractice claims. *See generally* Bernzweig, *Defensive Medicine,* in *Appendix* to REPORT TO THE SECRETARY'S COMMISSION ON MEDICAL MALPRACTICE 38 (U.S. Dept. of Health, Education and Welfare, 1973).

15. For a brief summary of the relevant aspects of computer technology, see Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society,* 67 MICH. L. REV. 1091, 1093-1103 (1969).

16. The capability has been present for some time; for example, in 1967, "a computer in Washington, D.C., analyzed electrocardiograms of patients in France and returned interpretations within thirty seconds." Freed, *Legal Aspects of Computer Use in Medicine,* in MEDICAL PROGRESS AND THE LAW 114 (C. Havighurst ed. 1969). *See also* Irwin, *Washington-Moscow Medical Hotline,* The Buffalo Courier-Express, March 31, 1974 (Parade Magazine), at 16; Freed, *A Legal Structure for a National Medical Data Center,* 49 B.U.L. REV. 79 (1969).

17. *See generally* Freed, *Legal Aspects of Computer Use in Medicine, supra* note 16, at 131, 140.

18. Examples of this capability in a prepaid group health plan serving 20,000 members are provided in Grossman, Barnett, Keopsell, Nesson, Dorsey & Phillips, *An Automated Medical Record System,* 224 J.A.M.A. 1616, 1620 (1973) which states:

> Information can be selected from the computer files concerning any set of patients whose records meet defined criteria. [One such study produced] a list of women whom the physicians wished to contact because they were taking a particular type of sequential birth control pill that had been removed from the market by the Food and Drug Administration. Other special studies included a profile of the welfare-supported population of the plan, and a mailing list of all members who met the Public Health Service's criteria for receiving influenza vaccine.

the treating physician keep current with developing knowledge in his field by providing him with an "external memory" capable of instantly recalling massive bodies of data.[19]

Notwithstanding these many perceived advantages of clinical computing systems, the development of automated patient records has apparently been neither rapid nor extensive.[20] When computers have been used in hospitals and clinics, they have most frequently been employed for routine administrative chores such as admissions, billing or scheduling rather than as part of the treatment process. Several reasons for this reluctance to computerize patient records have been suggested. The number of physicians and related health care professionals who are sufficiently familiar with modern data processing systems to foresee their benefits or feel comfortable in using them is probably small; thus, full acceptance of the technology may have to await broad education or re-education of the medical profession. Moreover, medical records and charts have proven difficult to reduce to machine-readable form at acceptable costs because of the great variety of information that must be stored and retrieved and the lack of generally accepted standard recording formats.[21] Many physicians also may fear that computerization will cause them to lose control over the use and dissemination of their patients' medical records, which they are ethically obliged to keep confidential.

---

19. *See, e.g.*, MEDICAL PRIVACY AND COMPUTER TECHNOLOGY 75 (emphasis removed) which reads:

> Substantial extension of our memory could be accomplished if biomedical knowledge could be deposited in a data bank, in a highly organized fashion, and the clinician could use the external memory in addition to his stored medical knowledge. For instance, if all the less frequent diseases, all the drugs with their indications, risks, and metabolic characteristics could be stored in an easily retrievable fashion, the clinical choice of drugs could be a comparison of clinical data on hand with retrieved information from the biomedical knowledge bank. . . . Such an artificial intelligence support could close the gap between existing knowledge and bedside medicine.

20. *See, e.g.*, WESTIN & BAKER, *supra* note 4, at 204, stating:

> For the most part, the medical community has not yet turned heavily to computerization to solve its medical record-keeping problems. A 1970 survey of hospitals in the U.S. reports that "55 percent of all hospital information processing applications are still performed by hand," and in our national survey only 24 percent of the hospitals in the sample reported computer applications to their patient medical records.

21. *Cf.* WESTIN & BAKER at 204, that reads, "Because the patient's individual medical record is a basically narrative document, it is difficult to reduce it to the kinds of codes and abbreviations which might make computer storage relatively inexpensive; instead, massive storage would be required for any system that was designed to accept the record in narrative form." However, despite the fact that "narrative materials make up much more of the psychiatric patient record than of the average medical or surgical case history," psychiatric records have been successfully computerized. Curran, Laska, Kaplan & Bank, *Protection of Privacy and Confidentiality*, 182 SCIENCE 797 (1973).

Despite the difficulties of computerizing clinical records, some large-scale projects are already being planned. In Massachusetts, a subsidiary of Blue Shield is reportedly developing a computer service called "Blue Streak" which will expand from a simple billing service "to include an automated medical record, tailored [to] the physician's practice, as well as an emergency medical data base . . . for emergency hospital room use."[22] In addition to providing direct links from the hospital emergency room to the patient data base,[23] Blue Streak will make it possible for the diagnosing physician who refers a patient to a specialist to allow the specialist direct access to portions of the patient's computerized file.[24]

Development of a computer system that would be similar in function, but considerably different in organization, has been considered by a multidisciplinary group in Western New York. Instead of a commercial venture, the New York data bank would be an "ethical health data center" subject to a variety of constraints to safeguard the privacy and integrity of patient records.[25] The ethical data center would be a "dedicated system" used exclusively for processing patient records, and structured as a nonprofit corporation or similarly autonomous entity. However, it would also be subject to privacy safeguards resulting from the ethical constraints of the health care professions, oversight by public or quasi-public authorities, and operational guidelines formulated with consumer participation.

A third approach to linking multiple health care providers through computer-communications systems is the Kaiser-Permanente group medical plan described by Professors Westin and Baker.[26] One of the largest and most successful plans providing both insurance and health

---

22. MASSACHUSETTS GOVERNOR'S COMMISSION ON PRIVACY AND PERSONAL DATA, HEALTH AND PRIVACY: PATIENT RECORDS 57 (1974). The data available to emergency care providers will not encompass the patient's entire file, but rather will consist of limited items organized into an "emergency medical bank" consisting of blood type, transplant information, and the like. *Id.* at 61.

23.

> Emergency record files will be stored by patient, number and accessible to 'qualified emergency providers'—namely, hospitals. At the present time, Blue Streak envisions terminals in hospital emergency rooms . . . .

Id. at 61.

24. Apparently input from physicians would be segregated into a "working file" and a "confidential file," with only the former accessible to a physician who subsequently treats the patient. *See id.* at 59-61.

25. *See generally* Computers in Clinical Medicine; Cosgriff, *The Joint Task Force on Computers in Medical Practice of the Medical Society of the County of Erie*, 4 J. CLINICAL COMPUTING 6 (1974).

26. *See* WESTIN & BAKER at 205-14.

care,[27] Kaiser-Permanente has pioneered computerization of clinical records with the objective of developing a data system "that will support the medical data requirements of one million health plan members, one thousand physicians, and a large corps of professional and paramedical contributors to patient care."[28] Since a prepaid plan of this nature attempts to meet all the health care needs of its members, and emphasizes frequent check-ups and preventive care, the amount of data that might be generated by a large-scale data network is potentially enormous. However, the computer system has apparently not yet developed beyond a pilot project confined to the San Francisco area.[29]

While there may be some question as to whether any of these approaches to the computerization of clinical records is technically and economically feasible at the present time,[30] the current level of interest and experimentation suggests that large-scale computerization of primary clinical records will eventually come about. If this does occur, these computing systems may threaten individual privacy for several reasons. First, a data center which attempts to meet a variety of patient needs on a continuing basis will in all likelihood have to be quite comprehensive. At the time patient records enter the system in the process of treatment or a routine check-up, it may well be impossible to determine whether a particular item of data can provide a crucial clue to the diagnosis or cure of a future illness, and consequently the natural tendency of the system operators should be to err on the side of inclusion. It will also be difficult for system operators to establish criteria for "purging" stale or outdated records: a drug reaction or a genetic condition, for example, may not manifest itself for decades or even generations. Thus, the record system most useful for medical treatment will be a complete birth-to-death history of encounters with the health care systems, perhaps cross-referenced to relatives, co-workers and other groups who share medically significant characteristics.

In addition to having a comprehensive data base, an efficient clinical computing system will have to be quickly accessible over a wide

27. "For a set fee, the program—which is both insurer and medical provider—agrees to meet all of the members' health needs, from examinations and innoculations to long-term hospital care." *Id.* at 206.

28. *Id.* at 208.

29. *Id.* at 209. Westin and Baker conclude: "Whether large-scale computerized medical files can provide the kind of reliable and sophisticated service required, or whether the costs of adopting computer systems for medical record-keeping will be too high, are questions still to be answered." *Id.*

30. Development of the Kaiser-Permanente system was subsidized by a grant from the U.S. Department of Health, Education and Welfare. WESTIN & BAKER at 208. Creation of an ethical health data center would undoubtedly require similar support, at least to meet start-up costs.

geographic area if it is to be useful for the treatment of acute illnesses among a mobile populace. To assure that the relevant information will be promptly available in the one emergency room where the accident victim is taken, the data will have to be constantly accessible at all of the facilities where he might need emergency treatment. Achieving this kind of flexibility and quick response, however, may undermine the privacy objective of assuring that sensitive data is disclosed only to those who have legitimate need, and proper authorization, to obtain it.[31]

A third set of problems that will arise from the large-scale computerization of clinical records is economic and institutional pressures to utilize the data base for purposes other than direct patient care. Once medical records are reduced to machine readable form, it will be relatively easy to use them in performing tasks like the biomedical research, policy analysis, and financial accounting functions described in the following sections.[32] The ability to perform these "secondary" data processing functions with records that are compiled for the "primary" purpose of patient care means that those who urge separation of functions on privacy grounds—the use of "dedicated" or single-purpose systems for clinical records—will have to bear a heavy and perhaps insurmountable burden of cost-justification.[33] If the trend of development is toward multiple-purpose systems in which a variety of data users have differing needs for access to different portions of the medical record, the task of safeguarding the data subject's privacy becomes considerably more complex and problematical.

B. *Systems for Health Statistics*

Computerization of medical records has made possible a wide array of statistical programs designed to improve policy decisions at all levels

31. A possible method of reducing this risk is to partition the file so that only a limited amount of data commonly needed for emergency care (*e.g.*, blood type, drug sensitivities) is available to emergency care providers. This is the approach being taken by the Blue Streak system. *See* notes 22-23 *supra* & accompanying text.

32. *See, e.g.*, HEW REPORT, *supra* note 5, at 78.

Many automated personal data systems established primarily for administrative purposes are also used for statistical reporting and research. Since one advantage of computerizing administrative records is the capability thereby acquired for high-speed data retrieval and manipulation, a growing number of administrative data systems will be put to such additional uses.

33. An official of the U.S. Department of Health, Education and Welfare has criticized the "ethical health data center" concept (text accompanying note 25 *supra*), which is based on the separation of clinical records in a dedicated system, on the ground that single-purpose systems would be too costly. Crystal, *Individual, Professional, and Community Concerns With the Health Data Center: Confidentiality Considerations*, 4 J. CLINICAL COMPUTING 37, 41 (1974).

from the administration of a single hospital or clinic to the restructuring of the national health care system. The diversity of health-related statistical functions is illustrated by the Multi-State Information System for Psychiatric Patient Records (MSIS), a single computer system serving a number of public mental health authorities throughout the country.[34] The MSIS system is designed to handle not only "individual [patient] records that could be useful in daily clinical activities," but also "aggregate data for administrative, fiscal, and research purposes":[35]

> Accurate, timely statistics are available on the number of patients served, the types of services rendered, the progress made, and the resources utilized. . . .
>
> Data are also used in determining whether all segments of the population are served adequately and equally by a mental health facility. Statistics on ethnic group, income, age, sex, and so forth are used for planning extensions of existing programs, for developing new programs, and for correcting inequities.
>
> . . . [Within participating institutions], data for the facility as a whole are used for administrative and management purposes—for example, to determine how much food or medication to order. . . .
>
> The system's capabilities continue to expand through the development of data collection and analysis techniques in such areas as patient billings, cost analysis, third-party payers, computer-suggested modes of treatment, automated utilization-review procedures, and program evaluation.[36]

Many of these statistical studies become more valuable if information systems are sufficiently compatible to permit comparative analyses involving different geographical areas or patient populations.[37] How-

34. Curran, Laska, Kaplan & Bank, *Protection of Privacy and Confidentiality,* 182 SCIENCE 797, 798 (1973) describes the program:

> With some $10 million in the [National Institutes of Mental Health] demonstration grant, an effective program of cooperation in data collection and utilization among a group of jurisdictions, some largely urban and some largely rural, ranging from the easternmost to the westernmost state, has been established. At this writing, the participating public mental health authorities are those of the state governments of Connecticut, Hawaii, Massachusetts, New York, Rhode Island, South Carolina, Tennessee, and Vermont; also participating are the public mental health program of the District of Columbia and the psychiatry program of the Universrity of Alabama. The MSIS program is open to additional cooperating jurisdictions and programs.

35. *Id.* at 797.

36. *Id.* at 798.

37. For example, in 1971, the President's Commission on Federal Statistics criticized existing federal statistical programs in the health-care field because they were collected on a national basis, and could not be validly broken down into units smaller than states or large metropolitan areas for statistical purposes. Ullman, *Federal Government Involvement in Data Collection for Subnational Areas,* in 2 PRESIDENT'S COMMISSION ON FEDERAL STATISTICS 121, 160-62 (1971).

ever, compatibility has been lacking because planning for health care delivery has traditionally been decentralized, with most policy-making performed at the state, county or local level.[38] The federal government has recently begun to make health statistics more uniform through a Cooperative Health Statistics System in which federal grants and contracts are used to induce standardization of governmental statistics at all levels.[39] These cooperative efforts, together with the federal government's own statistics-gathering programs,[40] could produce in the health field the functional equivalent of the proposed National Data Center that was abandoned in the mid-1960's because of public and congressional concern about potential invasions of privacy.[41]

The question whether health statistics systems constitute a threat to privacy largely depends upon whether, or to what extent, the records being used for statistical purposes are individually identifiable. In a number of statistical applications, it is clear that the ability to identify particular data subjects contributes to the efficiency and utility of the system. Some health statistics programs have a longitudinal component

---

38. *See id.* at 160.

39. *See* 39 FED. REG. 1458 (1974) (functions of Division of Cooperative Health Statistics System, National Center for Health Statistics). The objectives of the Cooperative System are described as follows in Ullman, *supra* note 37, at 163:

> States will be encouraged to develop strong organizations, spoken of as State Centers for Health Statistics, with the staff and facilities to take on the major part of the data collection and data processing for the system. The federal government will reimburse the states for data provided in machine readable form that meets the federal specifications, and also for a part of the costs of operating the data collection and data processing mechanisms.
>
> . . . This research and development phase will proceed on a project-by-project basis, each project being selected to increase knowledge about how the total system ought to be designed—and to help in the development of the capabilities of a State Center for Health Statistics.

40. The National Center for Health Statistics in the Department of Health, Education and Welfare has several subunits engaged in collecting and analyzing statistics, including the following: Division of Health Interview Statistics, which "[p]lans and administers statistical programs based on a systematic nationwide health interview survey"; Division of Vital Statistics, which "[p]lans and administers statistical programs serving demographic and public health needs of vital statistics" and "develops standards for data collection . . . as the basis for a national cooperative vital statistics system at federal, State, and local levels"; Division of Health Manpower and Facilities Statistics, which "[p]lans and administers statistical programs based on systematic nationwide surveys and inventories of health manpower and facilities"; Division of Health Resources Utilization, which conducts statistical programs based on "a systematic collection of data on the utilization of health resources"; and Division of Health Examination Statistics, which "[p]lans and administers statistical programs based on systematic nationwide health examination surveys of individuals." 39 FED. REG. 1458 (1974). *See also* 1 PRESIDENT'S COMMISSION ON FEDERAL STATISTICS, *supra* note 37, at 25-26; Ullman, *supra* note 37, at 162-63.

41. For a discussion of the National Data Center proposal, and reactions to it, see Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1091, 1129-34 (1969).

that requires tracking the individual over a period of time, either to follow the development of a disease,[42] or to investigate responses to different kinds of treatment, or to find out how certain classes of people utilize health care services.[43] It may also be thought desirable to match different sets of data such as welfare, police, and psychiatric records to see whether the same groups of individuals are making demands upon different public agencies.[44] However, when these kinds of file linkages are permitted, a variety of statistical techniques are available to minimize the risk that data from different files can be aggregated to compile dossiers on identifiable individuals.[45]

Apart from the possibility that statistical data will be improperly used or released in identifiable form, threats to privacy can result from

---

42. *E.g.*, Maryland Department of Mental Hygiene & National Institutes of Mental Health, Maryland Psychiatric Case Register 20 (1967) reads:

> Longitudinal studies on the natural history of mental disorders and their outcome should be possible in a few more years. Since the Register has collected only five years of data, the "payoff" with respect to statistics on the progression from childhood disorders to adult disorders, chronicity and treatment evaluation has not yet been fully realized.

43. *See, e.g., Hearings on Federal Information Systems and Plans Before a Subcomm. of the House Comm. on Government Operations,* 93d Cong., 1st Sess., pt. 2, at 228 (1973) (testimony of Robert A. Knisley, Director, Division of Community Management Systems, Department of Housing and Urban Development).

> At the National Center for Health Statistics . . . data are now collected on the number of visits made to family planning clinics across the country. NCHS is unable to tell, however, the number of women using the clinics. Surely this is inadequate for program planning and evaluation.

Id.

44. *See, e.g.*, Maryland Department of Mental Hygiene & National Institute of Mental Health, *supra* note 42, at 21:

> Record matching studies with [the Maryland Psychiatric Case Register and] police, welfare and other agency records, either on a sample basis or as part of a broader psychosocial register, have not yet been carried out . . . . Studies of the interrelationship of psychiatric cases with other identified cases of deviant behavior are greatly needed. Are these the same or different populations? What is the size of the population with recognized deviant behavior problems and what are its demographic characteristics? What services are provided for these problems?

45. *See generally* D. Campbell, R. Boruch, R. Schwartz & J. Steinberg, Confidentiality-Preserving Modes of Access to Files and to Interfile Exchange for Useful Statistical Analysis (Final Draft of Appendix A to the Final Report of the National Research Council Committee on Federal Agency Evaluation Research, Oct. 1974). Among the techniques discussed are microaggregation "to create many synthetic average persons and to release the data on these rather than on individuals." *Id.* at 9. *See also id.* at 20. Other techniques are "link file brokerage" in which the task of linking the files in question, and stripping off identifiers, can be performed by a neutral third party (*id.* at 22-24); and "mutually insulated file linkage" in which "some types of file linkage can be achieved without merging and in a manner that prevents either file from acquiring individual information from the other file." *Id.* at 4. *See also id.* at 24-32. The authors emphasize that these techniques and others are not absolutely foolproof in all circumstances, but rather are more or less "conservative" (*i.e.*, difficult to penetrate) in various situations.

questionable practices in collecting statistical information. It has been charged that data collectors use the "leverage" inherent in an administrative system, such as welfare benefit determinations, to collect personal information needed solely for statistical purposes,[46] or deliberately foster the mistaken impression that the requested data must be provided under penalty of law,[47] or give respondents assurances of confidentiality that are supported neither by law nor by administrative regulation.[48] Information gatherers may also give data subjects the

46. *See* HEW REPORT at 79-80. The Report recommends that "when 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." *Id.* at 85.

47. *See* 1 PRESIDENT'S COMMISSION ON FEDERAL STATISTICS, *supra* note 37, at 205, which reads:

> Addition of [a] simple statement [that the respondent's voluntary cooperation is solicited] would go far to reduce the range of possible misunderstanding. That it would not completely eliminate misunderstanding is established by the experience of statisticans in several agencies who sometimes get pleading requests from recipients of mailed questionnaires to be excused from responding, despite clear statements in the cover letter that voluntary responses are being sought.

A study of federal agency practices relating to the handling of personally identifiable information which was conducted for the Administrative Conference of the United States in 1973 concluded that "agencies do not, as a rule, give the respondent any information at the time of collection on whether the information is required by statute to be furnished, the precise purpose for which the information is being collected, the uses to which it will be put, or whether other governmental organizations will be given access to the information in individually-identifiable form." The study also found that the failure to disclose was "a calculated practice which was uniformly rationalized by the administrators . . . as a means of obtaining more and fuller responses to demands for information." A. Bell, Interagency Transfers of Information in Individually-Identifiable Form 4-5 (unpublished report prepared for the Committee on Rulemaking and Public Information of the Administrative Conference of the United States, Sept. 10, 1973).

48. 1 PRESIDENT'S COMMISSION ON FEDERAL STATISTICS, *supra* note 37, at 207 reads:

> All who gather information on voluntary basis quickly learn that it is important to promise respondents that data will be held in confidence, but it is not clear exactly what such a promise means when it is made by an agency other than the Bureau of the Census or the National Center for Health Statistics. Data gathered under Title 13 of the U.S. Code, or under Section 305 of the Public Health Service Act are not to be disclosed in such a manner that individuals can be identified, and the data are *immune from legal process.* . . . In some cases, when surveys are administered by researchers on contract or by agency personnel who do not recognize some legal complexities, confidence is promised with no authority whatsoever.

A graphic example of this risk is the experience of the New Jersey Negative Income Tax Experiment, which collected a variety of sensitive personal and financial information from low-income families under pledges of confidentiality. As a result of circumstances which later made the program controversial, the investigators were confronted with subpoenas from a local prosecutor, a grand jury investigation, and congressional inquiries. The investigators discovered that they had little or no legal protection against these attempts to uncover personally identifiable data. *See generally* Kershaw & Small, *Data Confidentiality and Privacy: Lessons from the New Jersey Negative Income Tax Experiment,* 20 PUB. POLICY 257 (Spring, 1972).

erroneous impression that information will be used for surveillance rather than statistical purposes, by failing to provide respondents with an accurate understanding of the nature of the research.[49] Since the right to privacy protects the mental and emotional tranquility of the individual,[50] his belief that he has lost control of sensitive personal information, or that dossiers of embarassing data are being collected about him, can be as harmful as the reality.[51]

C. *The Growth of Third Party Payers*

Although the development of computer systems handling clinical data or health statistics has been significant, it appears that the most rapid and extensive computerization of medical records has taken place in information systems which process data relating to payments for health care services made by parties other than the individual consumers of these services. A variety of institutions and organizations fall within the category of third-party payers: government agencies, nonprofit entities like Blue Cross-Blue Shield,[52] prepaid plans like Kaiser-

49. This risk was recently demonstrated by a Maryland state agency with the Orwellian name of the "Abortion Surveillance Unit." The agency was attacked by civil libertarian and women's rights groups for invading the privacy of women who had had abortions in the state. Much of the protesters' concern arose from the use of a reporting form which required the abortion patient's address; it was feared that this information, along with other identifiers, would permit system users to trace individuals who had had abortions. However, the agency had been collecting this information solely for the purpose of keying the medical data to census tract codes so that health care planners could measure trends in abortion statistics in different geographical areas. After the controversy arose, it was a simple matter for the agency to adjust its practice to assure that identifying details were never fed into the computer, and addresses were blotted out on the reporting forms after use. The Washington Post, Sept. 16, 1974, at C-1, col. 1.

50. *Cf.* Warren & Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 196 (1890):

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

See also notes 338-40 *infra,* & accompanying text.

51. *E.g.,* Miller, *The Right of Privacy: Data Banks and Dossiers,* in PRIVACY IN A FREE SOCIETY, *supra* note 4, at 74:

> Unrestrained governmental recordkeeping poses a serious potential threat to values thought basic to the philosophical fibre of our society. If a citizen knows that his conduct and associations are "on file," and feels that there is some possibility that the information might be used to harass or injure, he may become more concerned about the possible content of the file and less willing to "stick his neck out" in pursuit of constitutional rights.

See also Donner, *Political Intelligence: Cameras, Informers and Files,* in *id.* at 56.

52. For a discussion of the differences between Blue Cross and Blue Shield, and the special regulatory treatment afforded them, see S. LAW, BLUE CROSS: WHAT WENT WRONG?, 5, 7-10 (1974) [hereinafter cited as S. LAW].

Permanente,[53] and commercial health and accident insurers. Together, these third-party payers constitute the dominant source of health care financing. In fiscal year 1973, of the $80 billion spent on personal health care, government paid 38 percent and private insurance accounted for another 26 percent; only about 35 percent was paid directly by the recipient of the services.[54] The dramatic growth in the role of third-party payers[55] seems likely to continue, particularly if some form of national health insurance is enacted.[56]

Regardless of the nature of the organization acting as third-party payer, it will need to process great quantities of medical data in discharging its functions. Statistical analyses must be performed for actuarial and planning purposes, program evaluation, cost and quality control, and the like. In these respects, the third-party payers share many of the characteristics and problems of health statistics systems described above. All third-party payers must also handle personally identifiable information in processing and paying claims. And, if the third-party payer is an insurer which issues individual rather than group policies, it will need some identifiable medical records to accomplish its underwriting task.[57] As the following examples indicate, both underwriting and claims processing have given rise to complex, large-scale computer systems.

1. *Underwriting Information: The Medical Information Bureau.* A commercial insurance company writing health or life insurance policies for individual customers must have some means of determining

---

53. *See* text accompanying notes 26-29 *supra.*

54. STAFF OF THE HOUSE COMMITTEE ON WAYS AND MEANS, NATIONAL HEALTH INSURANCE RESOURCE BOOK 68-69 (1974). *See also id.* at 66-67.

55. *See id.* at 68, where the Committee staff finds:

> The distribution of personal health care expenditures by payment source has changed considerably in the past 20 years. In fiscal 1950, the sources and shares were as follows: Direct payments by patients (68 percent), Federal-State-Local governments (20 percent), private health insurance (9 percent), and philanthropy and others (3 percent).

56. For a summary of major national health insurance bills introduced in the Ninety-Third Congress, *see id.* at 519-74.

57. Because the Blue Cross plans originated as localized "community service organizations" which based their rates on the general health needs of a particular area, they had little need to evaluate the health condition or risk of a particular individual in issuing policies:

> Initially all Blue Cross plans offered hospital insurace to all members of the community at uniform rates, one rate for individuals and one rate for families, while commercial companies offered more favorable rates to those groups and individuals who were actuarially less likely to make claims. Since low income families and the aged tend to utilize hospital services more than the general population, these groups are helped by community rating.

S. LAW at 12.

the likelihood that the events insured against will happen, so that a proper premium can be charged.[58] In modern life insurance practice, this decision requires not only general knowledge about the likelihood of death at a particular age, but also specific data about the health of the individual insurance applicant which would tend to indicate whether he presents a high risk:

> The use of a mortality table, which accurately estimates the longevity of aggregates of people of a given age, is not strictly applicable to an individual, for such a table assumes an average state of health. . . . Despite the certainty of death, variations arise as to when death will occur and the amount of total payments that will be made prior to that eventuality. To ascertain the risk these variations represent, the underwriter must refine the basic longevity estimate provided for by a mortality table for the applicant's age group. These refinements mandate inquiries as to the state of the applicant's health and other non-medical data which could adversely affect his longevity estimate.[59]

Because insurance applicants who are rejected or charged high premiums will sometimes suppress evidence of a medical condition in hopes of obtaining better terms from another insurer, many companies in the industry have long shared underwriting data. Over the years, these information-sharing operations have been institutionalized to create an interlocking network of health data systems.

The focal point of this network is the computerized data bank operated by the Medical Information Bureau (MIB), a trade association of more than 700 life insurance companies.[60] Most of these insurers have computer terminals in their own offices,[61] and for a cost of about 20 cents per inquiry[62] they can directly search the MIB health

---

58. Cf. Stern, *Medical Information Bureau: The Life Insurer's Databank,* 4 RUTGERS J. COMPUTERS & LAW 1, 3-4 (1974). This commentator states:

> The concept of insurance is predicated upon a mutual sharing of the risk of a common hazard, by joint contributions to a common fund. Such a plan is unworkable unless each participant pays into the fund an amount which is proportional to the risk he imposes on the fund. The insurer's function is to set up a schedule of premiums correlating to risks and to place each participant in the correct premium grouping.

Id.

59. *Id.* at 4.

60. *See generally* Stern, *supra* note 58; *Hearings on Commercial Health and Accident Insurance Industry Before the Subcomm. on Antitrust and Monopoly of the Senate Comm. on the Judiciary,* 92d Cong., 2d Sess., pt. 1, at 38 (1972) [hereinafter cited as *Hearings on Commercial Health Insurance*].

61. About 500 of the insurance companies participating in MIB have direct access to the files through remote terminals; the remainder submit inquiries by mail. *Hearings on Commercial Health Insurance* at 105.

62. *Id.* at 39.

files covering more than 12 million individuals.[63] If the insurance applicant has previously sought insurance from a participating company, his file may contain a large body of data arguably relevant to the underwriting decision:

> The coded data may sometimes indicate what type of condition was diagnosed, what parts of the body were affected, how long ago it was present and whether it is present today, how often it has reoccurred . . . , whether it was treated by surgery, and whether the information came from a physician, a hospital, or a sanatorium or clinic.
>
> The official list of potential impairments runs some 22 pages and contains special codes for possible hereditary conditions. One group covers nervous problems, including personality disorders . . ., alcoholism, and drug dependence; codes of sexual deviation and social maladjustments have recently been eliminated.[64]

This comprehensive data base is supplied by the participating insurers who in turn obtain it from a variety of sources, each of which poses some risk that the information will be inaccurate, or that it will be disseminated and used for purposes unknown and unsuspected by the insurance applicant.

The most obvious source of health data is the applicant himself, who is typically asked detailed questions about his medical history. The risks of inaccurate recording at this stage may be substantial: in addition to the applicant's likely difficulties in recalling significant details of his own treatment history[65] and the insurance salesman's lack of expertise in medical matters, distortion may result from the applicant's desire to suppress data that might raise his rates, and the insurance agent's desire to minimize factors that might undermine the transaction and thus jeopardize his commission.[66]

---

63. *Id.* at 114. The number of files is growing at the rate of 3 percent per year. *Id.*

64. Pascoe, *MIB: It Has 12 Million Americans At Its Fingertips,* PRISM, June, 1974, at 29, 30-31.

65. *See* text accompanying notes 13-14 *supra.*

66. *Cf.* Statement of John E. Gregg, Chairman, Policyholders Protective Association International, *Hearings on Fair Credit Reporting Act—1973 Before the Subcomm. on Consumer Credit of the Senate Comm. on Banking, Housing and Urban Affairs,* 93d Cong., 1st Sess., at 586 (1973) [hereinafter cited as *Hearings on FCRA*]. The following is part of the statement by John E. Gregg:

> Based on my experience in selling and supervising salespeople, and from reviewing thousands of photocopied applications attached to policies on which people are paying premiums today, I am convinced that at least 40% of the health information recorded on them is defective and erroneous. Much of it comes from salespeople not sufficiently trained to record the medical informa-

If the insurance company conducts an independent background investigation of the applicant, there may be problems both of inaccuracy and of unauthorized dissemination of sensitive health information. This function is frequently performed by an independent commerical "investigative reporting agency," a field which is dominated by one corporation, the Retail Credit Company.[67] Retail Credit makes some 15 million investigative reports annually, of which 70 percent are "insurance reports."[68]

In a life insurance background investigation, Retail Credit may try to uncover for the insurer information about "the applicant's duties, his finances, his health history, the extent of his use of alcohol, his mode of living, and hazardous avocations."[69] Critics, including the Federal Trade Commission, have charged that the information assembled by Retail Credit is not only frequently wrong as a result of slipshod investigative practices,[70] but that it may be falsely repre-

---

tion properly on application forms. Again, much of what applicants tell salespeople is "doctored" in hopes it will pass and earn a commission . . . .

A staggering amount of information turned in on health insurance applications is out-and-out fiction. Applications are taken from customers and filled out properly in their presence. Later, salespeople, agency office clerks, or other personnel . . . re-write them completely, forging not only the health information, but even customer's signatures.

Id.

67. The Federal Trade Commission has alleged in an antitrust complaint that life and health insurance reporting is a distinct relevant market, and that "Retail Credit has maintained a market share of over 80 percent of this submarket for a number of years." Complaint at paras. 8(c), 9(c), *In re* Retail Credit Co., No. 8920 (F.T.C., March 9, 1973).

68. *Hearings on FCRA* at 61. This figure apparently includes not only life and health insurance investigations, but also other types such as fire and casualty, automobile, etc. It apparently does not include investigations relating to claims made under insurance policies, which Retail Credit also performs. *See id.* at 61-62. The American Life Insurance Association has estimated that nearly 8 million investigative consumer reports were ordered by life insurance companies in 1972 for underwriting purposes.

69. Testimony of W. Lee Burge, President, Retail Credit Co., *Hearings on FCRA* at 105.

70. *E.g.,* note the following testimony of Albert A. Foer before the subcommittee:

I heard sworn testimony by former Retail Credit Co., inspectors . . . that a Retail Credit Co. inspector "on circuit," which means out in the countryside rather than in the city, will report on as many as 50 or 60 individuals a day, and . . . with quantity quotas of this nature it is very difficult to maintain accuracy and fairness, and as a result sometimes inspectors take short cuts and sometimes they do a shoddy job of reporting.

. . . .

. . . The Inspection bureaus say that they don't have quotas for protective [*i.e.,* derogatory] information, they have norms but the way it works out in practice, these norms are quotas.

Id. at 676-77. *See also* A. MILLER, THE ASSAULT ON PRIVACY 70 (1971), where Miller states:

Given interrogation practices designed to provoke gossip, it is not surprising that files produced during several congressional hearings contained comments

sented to purchasers of the report as objective data based on personal observation of the applicant or in-person interviews with his friends, neighbors and co-workers.[71] If derogatory "protective information," whether accurate or inaccurate, does turn up in a Retail Credit insurance investigation, its damaging effects may not be limited to the 700 life insurers who can obtain it through the MIB computers.[72] Retail Credit Co. has been described as "a personal information department store"[73] which, either directly or through subsidiaries, sells data about individuals in a variety of information submarkets, including local and national credit reporting, fire and casualty insurance reporting, and personnel reports requested by prospective employers.[74] Health information gathered for life insurance underwriting may later prove useful for these other purposes and, according to a Federal Trade Commission complaint, Retail Credit retains a copy of the applicant's insurance data in their own files for subsequent sale or use.[75] If this is so, the medical data may then move into a new information system, and find even further uses and markets; at the same time, medical

---

from unidentified sources such as "peculiar," "scatterbrained," "neurotic," "psychotic," and "has . . . a persecution complex." None of these remarks appears to have had any medical or psychiatric basis. Other files included remarks about the subject's drinking, aggressiveness, associations, health, hobbies, and activities.

71. This allegation is contained in a Federal Trade Commission complaint charging the company with deceptive practices and violations of the Fair Credit Reporting Act. Complaint at paras. 9-10, *In re* Retail Credit Co., No. 8954 (F.T.C., Feb. 21, 1974).

72. The Executive Director of the MIB estimated in 1973 that 14 percent of the MIB data came from investigative reporting companies like Retail Credit, through member life insurance companies. *Hearings on FCRA* at 443. Pascoe reports that since May of 1974 member companies may supply personal and financial data to MIB only if it comes from the applicant himself; "[i]nformation about these areas obtained by investigative agencies hired by carriers or company snooping by its own investigators is now inadmissible." Pascoe, *supra* note 64, at 32. Of course, the rule is an effective safeguard for the data subject only if it is adequately enforced. *Cf.* note 86 *infra* & accompanying text.

73. *Hearings on FCRA* at 685.

74. The market descriptions are taken from the Federal Trade Commission's antitrust Complaint at paras. 8-9, *In re* Retail Credit Co., No. 8920 (F.T.C., Mar. 9, 1973). *See also* testimony of W. Lee Burge, President, Retail Credit Co., *Hearings on FCRA* at 57.

75. The FTC's deceptive practices complaint against Retail Credit, *supra* note 48, at para. 5, alleges that contrary to the impression given interviewees by Retail Credit's investigators:

> The information furnished by the consumer or others during an interview, will not be used exclusively by the company to which the consumer has applied for a benefit. The information is added to respondent's files for future reference in connection with any subsequent requests by other customers for reports on the consumer, who is the subject of the interview.

Retail Credit has denied that it "indiscriminately makes such reports available to its field representatives for use in consumer reports that might be ordered at a later date." *Hearings on FCRA* at 117.

and related information generated for these other operations, or purchased from other data systems, may be useful for life insurance underwriting.[76]

Two other sources of medical data for the MIB system, physical examinations by insurance company physicians and reports by doctors or institutions who have treated the applicant in the past, may seem at first glance to be less susceptible to error or to diversion of the data into improper uses. However, some serious questions have been raised. Personal physicians and health care providers apparently have diverse policies for dealing with insurance investigators, ranging from relatively unsupervised access to raw files[77] to deliberate falsification of reports[78]—either of which can produce an erroneous file entry. Family physicians are also frequently slow to provide the requested information, and this delay can be costly to the insurer, particularly if the applicant changes his mind about purchasing insurance in the interim. Transforming this problem into an opportunity, Retail Credit developed an Underwriting Medical History service which offers to expedite the transmission of the physicians' statements from the appli-

---

76. One such possibility is suggested by the following description of Retail Credit's relationship with one state's motor vehicle department:

> [A]ny individual or organization for a 50 cent charge can purchase [from the New York State Department of Motor Vehicles] the print out of a specific license or registration record. Information such as motorist accident reports (which in many states are confidential) can also be purchased in New York for $3.50. . . . [T]he Retail Credit Company, a leading investigative service for the insurance industry, buys approximately 1 million print outs a year, primarily for use in its automobile and life-insurance reports. The insurance industry itself buys upwards of 100,000 print outs per month. . . .
>
> In recognition of the volume of this trade, the department is currently considering the request by the Retail Credit Company and some insurance companies to have on-line terminals installed connecting their offices with the department.

WESTIN & BAKER at 74.

77. Holton, *An Alert to Physicians About Photocopying Patient Records*, PRISM, June, 1974. In his article, Holton states:

> In 1973, AMA's Council on Medical Services expressed concern over the apparently increasing frequency with which insurance companies are sending their employees or agents into physicians' offices to photograph medical records.
>
> In some cases, although photographing of records is not involved, company representatives are offering to look through patient records "to save the doctor time and effort."

Id. at 32.

78. *See, e.g., Caveat Shrink*, TRIAL, July/August 1974, at 10 which reads:

> A survey of 247 psychiatrists in Massachusetts revealed that many psychiatrists have lied about patients' conditions or advised patients to lie because of insurance companies' inability to properly evaluate the conditions of psychiatric patients. The psychiatrists claimed that insurance companies regard all patients, regardless of the severity of the disorder, as such potential risks that many cannot get, or afford, life insurance.

cant's doctor to the insurance underwriter.[79] In the process, Retail Credit reportedly takes care to deposit a copy of the physician's statement in its files, for use in future investigations.[80] Retail Credit has also attempted to become the processor of medical data generated when the applicant is examined by an insurance company doctor, by establishing a chain of service centers "staffed by technicians trained to receive medical history, perform certain laboratory tests and take the physical measurements of applicants."[81] These paramedical examination centers may reduce costs by conserving expensive physicians' time, but they also create a new fund of medical data which may be useful to Retail Credit for a variety of purposes,[82] and which is outside the control of both the consumer and the medical profession.

Aside from the possibility that Retail Credit or a similar organization can divert to its own uses part of the stream of data flowing into the MIB, there remains the question of whether medical data is likely to be misused after it enters the Bureau's computers. One possibility frequently mentioned by critics is that participating insurance companies will use information that was obtained in processing the life insurance application for other purposes. Since many of the life insurers who participate in MIB also sell health or accident insurance in which the insured's physical condition is relevant to the underwriting decision,[83] there is at least a temptation to use the data for multiple purposes. Another problem is underwriters' reliance on possibly wrong or misleading MIB data in deciding whether to insure the applicant or to assign him to a special high-risk category. The internal rules governing the MIB system prohibit reliance on file information with-

79. Testimony of Albert A. Foer, *Hearings on FCRA* at 685. *See also id.* at 723, where it is reported that Retail Credit handled over 26,000 such reports in the month of June, 1972.

80. *Id.*

81. 1971 Retail Credit Co. Annual Report, in *Hearings on FCRA* at 685.

82. *See Hearings on FCRA* at 722. File integration seems common at Retail Credit; the FTC's deceptive practices complaint against the company, *supra* note 71, at paragraph 28, charges:

> [R]espondent retains file copies of the information contained in the consumer reports and claims reports which it prepares for its customers. Respondent incorporates all of said information into the same filing system, making no attempt to segregate the consumer report information from the claims information. In the preparation of subsequent consumer reports, respondent uses all of its file information interchangeably . . . .

83. In the 1973 hearings on the Fair Credit Reporting Act, for example, Senator Kennedy asserted that 87 percent of all health and accident insurance coverage in the country is sold by life insurance companies. *Hearing on FCRA* at 432.

out independent verification,[84] but corroborating a suspicious item may be costly and burdensome for the insurer:

> Since MIB reports never reveal the reporting company [that put the data in the system], if after filing the initial request for MIB information the requesting company seeks greater detail, it must file a second request with the MIB. The MIB forwards this request to the reporting company for it to deal with at its discretion. A requesting company may be discouraged from taking such action for the number of requests which it is allowed is limited. Furthermore, due to competition between insurers, the information may not be forthcoming.[85]

Member companies might be prevented from violating the MIB's consumer protection rules through a vigorous self-policing and sanctioning policy; however, the magnitude of MIB's commitment to enforcement of its rules has not been impressive in the past.[86]

Beyond the details of ways in which personal medical records can be used or misused in life insurance underwriting, the MIB experience seems suggestive of general problems that are likely to arise in attempts to control commercial uses of sensitive information. When extensive files of personal information are a major asset for a business organization,[87] the data base is likely to be relatively costly in time or money to collect, particularly if accuracy is important and the information sought is more judgmental than the bare facts of a retail transaction. Once this fixed cost is met, however, the low cost of supplying the information to subsequent users may make it attractive to

---

84. *See, e.g.*, statement of Joseph C. Wilberding, Executive Director and General Counsel, Medical Information Bureau, part of which reads as follows:

> Members are not permitted to underwrite risks on the basis of the information received from MIB. They may not rate or decline an application on the basis of such information. When alerted of an MIB record, the member company, under MIB rules, is required to make its own independent investigation. Its ultimate decision on the application must then be based on the results of such investigation.

Id. at 458-59.

85. Stern, *supra* note 58, at 9-10.

86. In 1973 congressional hearings, the Executive Director of MIB revealed that the Bureau's staff to spot check the insurers' compliance with its rules consisted of one man who "spends a great deal of his time on it." *Hearings on FCRA* at 447. By mid-1974, it was reported that MIB had two full-time investigators checking on compliance. Pascoe, *supra* note 64, at 48. *See also* Stern, *supra* note 58, at 30-31.

87. This would not be the case where the demand was for new information rather than historical file data—for example, in the "classic" divorce situation where one partner retains an investigator to substantiate suspicions about the other partner's current liasons. For this type of operation, capital requirements are low and barriers to entry fairly minimal. *See* Foer, The Personal Information Market, in *Hearings on FCRA* at 695, 740. Even in this commercial setting, "old information" from the files might confer a competitive advantage, by suggesting leads for further investigation. *Cf. id.* at 743.

find multiple markets for the data base.[88] Some kinds of personal information—unfortunately including medical records—seem commercially useful for a variety of purposes. Knowledge that a person had been diagnosed as having cancer would be relevant to employers making hiring or promotion decisions, enterprises considering loans or other commercial transactions involving the individual, and insurers in the life, health, accident, and possibly automobile markets; perhaps even a mailing list composed of cancer patients would be salable.

Against these kinds of incentives, there appear to be few barriers impeding the widespread, repetitive dissemination of sensitive data. Personal information is a commodity that is not necessarily depleted or altered through repeated use; consequently, the possibilities for commercial exploitation are as expansive as the problems of controlling information once it has been disclosed.[89] Moreover, the boundaries of systems and organizations seem easy to cross under existing law and custom. In the life insurance context, a simple authorization from the insurance applicant, easily extracted and uninformedly given,[90] is sufficient to remove most practical obstacles and permit the

88. Precise information about these relationships is, not surprisingly, hard to find. Foer, *supra* note 87, at 729, found that the re-investigation of a disputed item by an organization like Retail Credit could cost up to $100, and that in the highly competitive Chicago market the average rate for "open-ended" (*i.e.*, nonstandardized) investigations was $10.50 per hour in 1972. By contrast, the cost of supplying a report from MIB's computers at about the same time was, as previously mentioned, about 20 cents. *See* text accompanying note 62 *supra*.

89. An illustration of the difficulties of imposing restraints on the use of personal information can be found in the 1973 hearings on the Fair Credit Reporting Act. Senator Kennedy testified, presumably on the basis of information given him by the agency, that "if [an] insurance company, on behalf of an individual applying for health or life insurance, requests medical information from the Veterans Administration, the VA will supply it but does not permit the company to pass that information on to the Medical Information Bureau [MIB]." *Hearings on FCRA* at 429. However, the MIB later informed the committee that "about ½ of 1 percent of the total MIB codes [*i.e.*, items of information relevant to the underwriting decision] came from the V.A." *Id.* at 512.

90. Prior to recent criticism of the MIB in the press and the Congress, most insurance application authorizations for investigation did not even alert the applicant to the existence of the MIB, much less the role it would play in processing his medical records. *See* Pascoe, *supra* note 64, at 31. COMPUTERWORLD, Aug. 28, 1974, at 1, spoke to this issue in the following:

> Effective Jan. 1, the Medical Information Bureau (MIB) will no longer be able to collect and store confidential health information on insurance applicants without their knowledge or access as a result of pressure brought by the state insurance commissioners of Pennsylvania and Massachusetts.
>
> . . . .
>
> The new policies specify that insurance applicants be "prenotified" in writing that health data they supply will be transmitted to the MIB for storage in a computerized data bank where there is a possibility the information may be shared among the various member insurance companies.

Id. at 1. For a more complete discussion of the consent problem, see text accompanying notes 151-59 *infra*.

data to flow freely from the doctor's and hospital's record systems to those of MIB and Retail Credit, and thus perhaps on to still other systems. This atmosphere of cooperation rather than competition regarding sources and files of personal information, which may be common in a variety of commercial settings beyond the insurance industry, indicates the range of incentives and institutional relationships that need to be taken into account in evaluating proposals to control commercial uses of personal information. Simple abolition of highly visible computer targets like the MIB, as some have urged,[91] would in all likelihood simply lead to re-creation of the same information-sharing functions in a different guise, possibly with higher costs and undesirable side effects.[92]

2. *Claims processing: the Medicare program.* Despite MIB's image as an information goliath feeding on millions of files, it is really a small-time operation compared to data systems that have been developed to process medical claims in the major government health care programs. A brief look at the information flows within one of these federal programs, Medicare, may suggest both the magnitude and the complexity of data systems used in claims processing.

Medicare, a health care program for the aged using an insurance model, was a major but nevertheless limited step by the federal government into the field of health care financing. Its limits fall into two general categories which would also be present to a greater or lesser degree in many private health insurance systems: (1) prescriptions on the classes of people who are entitled to coverage and the services they can receive (which in Medicare included ceilings on the benefits each covered individual could receive for each "spell of illness");[93] and (2) controls on the amounts paid out for covered services (specifically, some assurance that the treatment was medically necessary and that the costs to be reimbursed were within established norms).[94] The Social

91. *See, e.g.*, statement of Sidney M. Wolfe, M.D., Health Research Group, *Hearings on FCRA* at 434-36.

92. The MIB has argued that simple abolition of its information system would result in a competitive advantage to large insurance companies, accompanied by a risk that small or medium sized companies would be driven out of the market and competition reduced. This would come about because the large companies would agree to share data accumulated in their own files; the small companies, lacking a sufficiently comprehensive data base to entice larger companies to share with them, would be squeezed out. *Hearings on FCRA* at 472. If this is a realistic evaluation, the result would be that a simple control strategy—abolition of the offending information system—would quickly raise much more complex questions about what government should do, and what level of government should do it, to offset or avoid these anticompetitive consequences.

93. *See* text accompanying notes 95-98 *infra*.

94. Of course, health insurance payment schedules could be based on principles other than cost reimbursement. For a brief discussion of the political factors that led to adoption

Security Administration (SSA), as the agency operating the government's retirement, survivors and disability benefits programs, was a logical candidate for taking over the administration of Medicare, but it was not given the entire job; instead, the private sector, predominantly the insurance industry, was given a role in claims processing. As these shared responsibilities are reflected in information systems, SSA has primary control over eligibility information, while nonfederal "carriers" and "intermediaries" perform most of the collection and analysis of cost data, and make the initial determinations to pay or reject claims.

The Social Security Administration maintains at its computer center some 20 million "health insurance master records which contain information about individuals' entitlement to Medicare benefits and a record of their utilization of covered services,"[95] together with additional file systems containing the personal information needed for other programs administered by SSA.[96] The 130 carriers and intermediaries participating in the Medicare program, who need eligibility information in deciding whether to pay claims, can obtain direct access to the health insurance master records through telecommunications links, and they in turn update the individual beneficiary's "utilization record" on the master file when they pay a claim.[97] The central files are also accessible to the more than 1,000 district and branch offices which SSA maintains around the country to answer inquiries

---

of the cost reimbursement principle in Medicare, and criticism of its effects, see Hodgson, *The Politics of American Health Care,* THE ATLANTIC, October, 1973, at 45, 52-53.

95. *Hearings of Federal Information Systems and Plans Before a Subcomm. of the House Comm. on Government Operations,* 93d Cong., 1st Sess., pt. 2, at 280 (1973) [hereinafter cited as *Hearings on Federal Information Systems*]. *See also id.* at 271.

96. The other major files maintained by SSA at its central computer complex were described as follows in the 1973 hearings:

1) Master earnings record, for making entitlement decisions under Social Security old age disability and similiar programs—207 million accounts with 343 million earnings items posted annually;
2) Master beneficiary record of those who are currently entitled to receive benefits—33 million individuals;
3) Supplemental Security Income master file relating to income maintenance for eligible aged, blind and disabled individuals, estimated to contain 5.3 million persons when the program became fully operable.

These statistics apparently do not include records used for smaller programs administered by SSA, such as the black lung program which paid benefits to some 250,000 people. Testimony of Richard D. Shepherd, Director, Division of Systems Coordination and Planning, Office of Administration, Social Security Administration, *Hearings on Federal Information Systems,* pt. 2, at 271.

97. *See id.* at 274.

from the public, assist individuals in applying for benefits, correct records, and the like.[98]

The second general part of the claims processing function under Medicare, determining the appropriate amount of reimbursement for treatment rendered to eligible beneficiaries, is complicated by the existence of two different kinds of delivery systems for health services: institutions such as hospitals or nursing homes, and individual physicians. This distinction has been acknowledged in the statute and in administrative practice by significantly different approaches to cost determinations; both "Part A" and "Part B," however, require substantial quantities of individual medical records.[99]

Part A, dealing with reimbursement to hospitals and other institutional providers, works through a system of "fiscal intermediaries" or entities designated by the providers[100] to make reimbursement determinations, disburse funds, audit the providers, and generally serve as a conduit of information between SSA and the participating institutions.[101] When a Medicare patient is hospitalized, the hospital forwards information about the treatment and the bill for services rendered to the intermediary which, after obtaining eligibility information from SSA, decides how much of the claim should be paid.[102] From the

---

98. *Id.* at 271. Portions of master records are also physically available on microform in the district offices.

> Each district and branch office has as the backbone of its information system a file of the master records in clear language for all Social Security Administration beneficiaries living within the State. This file is in alphabetic order and is on microfiche . . . . The file is completely reissued every 6 months and contains not only active master beneficiary records but [also] records of disallowances, railroad retirement eligibility, and entitlement to black lung benefits. With this file, a social security employee is able to answer many questions while the individual is on the telephone or at the office.

Id. at 285.

99. It should be noted that the following descriptions focus only on aspects of the Medicare program which require substantial quantities of individuals' records, and even within this limited scope many of the details are overlooked. For a more thorough discussion of the administration of Part A, see S. LAW.

100. The fiscal intermediary may be a private organization or a public entity, and the provider's choice of intermediary will be approved by the Secretary of Health, Education and Welfare unless the Secretary can make a finding that this would not be consistent with efficient and effective operation of the program. 42 U.S.C. § 1395h(a) (1970). *See also* S. LAW at 33.

101. *Hearings on Administration of Federal Health Benefit Programs Before a Subcomm. of the House Comm. on Government Operations,* 91st Cong., 2d Sess., pt. 1, at 88 (1970). *See also* S. LAW at 33. The intermediaries may also have some less important responsibilities, such as conducting management studies and participating in statistical research. *Id. See also* Homer & Platten, *Medicare Provider Reimbursement Disputes: An Analysis of the Administrative Hearing Procedures,* 63 GEO. L.J. 107 (1974).

102. A more detailed step-by-step description of the information exchanges involved in this kind of transaction may be found in *Hearings on Federal Information Systems,* pt. 2, at 287-88.

beginning of the Medicare program, the overwhelmingly dominant intermediary has been the Blue Cross Association,[103] a national trade association of local Blue Cross plans which had already developed its own wire communications network to serve its policyholders.[104] The Blue Cross Association, as prime contractor, has subcontracted or redelegated most of the administrative functions to its constituent local Blue Cross plans, and these plans in turn may further subcontract auditing, data processing or other functions to private firms.[105] Thus, Part A claims processing centers around two interconnected data networks: the BCA headquarters, fed by its local plans and their subcontractors, and the SSA computer center, interacting with its branch offices. These linked systems have further "interfaces"—whether manual or electronic—with other data systems for both input (for example, billing information from a hospital administrative data system)[106]

---

103. In 1970, for example, Blue Cross was fiscal intermediary for 93 per cent of the participating hospitals, and 53 percent of the extended care facilities. Testimony of Robert Mayne, Assistant Bureau Director, Division of Intermediary Operations, Social Security Administration, *Hearings on Administration of Federal Health Benefit Programs, supra* note 101, pt. 1, at 89.

104. Evolution of the wire network has been attributed to the mobility of Blue Cross policyholders:

> When the Blue Cross system identified the need for out-of-area benefits, a program called the interplan service bank was developed, meaning if a person insured under a plan in California got sick in New York, arrangements were made between the plans to cover the benefits . . . .
>
> In addition, as . . . society becomes more mobile, [the Blue Cross system] found people began to move, and they wanted to carry their Blue Cross benefits from one area to another, and [the Blue Cross Association] set up an interplan transfer program . . . .
>
> Because of these operating responsibilities, [the Blue Cross Association] developed a vast wire telecommunications network to facilitate the operation.

Testimony of Bernard R. Tresnowski, Senior Vice President, Blue Cross Association, *id.* pt. 2, at 222-23. The dominant role of BCA among intermediaries has been attributed not only to its organizational structure and wire communications facility, but also to the Association's "lobbying" among hospitals to be designated as intermediary. *See* S. LAW at 41.

105. S. LAW at 41-42.

106. The provider apparently has little control or discretion in deciding what kinds of medical record data may properly be released to an intermediary. *See, e.g.,* MASSACHUSETTS GOVERNOR'S COMMISSION ON PRIVACY AND PERSONAL DATA, HEALTH AND PRIVACY: A REPORT OF CURRENT PRACTICES (Nov. 1974), part of which reads:

> Most carriers, private and Blue Cross, and governmental reimbursement systems—Medicaid and Medicare—provide their own forms to hospitals. There is little discretion left to the hospital in completing the form, because if the hospital wants to be reimbursed, it must provide the information requested. On the other hand, most claim forms, even Medicare, provide for patient authorization for release of information pertinent to the processing of the claim. The authorizations are peremptory, and somewhere open-ended, but arguably they serve the purpose, at least, of alerting the patient to the fact that some portion of medical information about him will be released.

Id. at 8.

and output (for example, requests from SSA to the Treasury Department to issue checks for reimbursement).[107]

Development of data processing systems for handling payments to individual physicians under Part B of Medicare has been more difficult than the evolution of systems under Part A, perhaps because of the greater number and more decentralized nature of the Part B providers.[108] In addition, Part B has a higher volume of claims because eligible beneficiaries are treated by physicians more frequently than they are admitted to hospitals or extended care facilities.[109] The reimbursement formula for Part B also contributed to administrative problems because it is a complex calculus which requires collection and analysis of large bodies of data relating to prevailing rates for similar services in the relevant locality:

> [T]he program is to pay 80 percent of reasonable charges after the deductible has been met, but in determining the reasonable charge, the carrier must take into consideration the customary charge of the individual physician to all of his patients for similar service and then screen that against the prevailing charge for similar services made by other doctors in the community, and then screen that further against what it would pay under a program of its own which was similar in scope and nature.
>
> In addition to this, medicare for the first time put a good deal of emphasis on the medical necessity of the service . . . and it put responsibility on the carrier for determining patterns of utilization, and for establishing parameters which would identify any aberrant patterns of utilization by individual physicians.[110]

Finally, the private insurance "carriers" administering payments—who are the Part B equivalents of the Part A intermediaries[111]—did not have adequate electronic data processing facilities or expertise to handle the enormous numbers of claims generated by Part B.[112] Gradually,

---

107. *Cf. Hearings on Federal Information Systems* at 274. If an intermediary is not a member of the Blue Cross Association network, it may use the SSA district office network for its claims processing work. *Id.* at 287.

108. Part B involves reimbursement for 200,000 private physicians, in contrast to the 10,000 institutional providers covered by Part A. S. LAW at 5.

109. In fiscal year 1973, over 19 million bills from hospitals and other facilities were processed under Medicare, while over 58 million bills for physician services were processed during the same period. NATIONAL HEALTH INSURANCE RESOURCE BOOK, *supra* note 54, at 429.

110. *Hearings on Administration of Federal Health Benefit Programs, supra* note 101, pt. 3, at 5.

111. *See* 42 U.S.C. § 1395u (1970).

112. *Hearings on Administration of Federal Health Benefit Programs, supra* note 101, pt. 3, at 260. The result was that "a huge backlog of claims" had accumulated under Part B by 1967. *Id.* at 5.

private data processing companies have taken on the information-handling requirements of Part B through subcontracts with the carriers. The dominant firm in the market, Electronic Data Systems,[113] operates on a national basis and offers carriers a complete data processing service that includes work related not only to Medicare beneficiaries but also to the carriers' private policyholders.[114]

More recently, another layer of cost control (and therefore of medical record processing) has been added to Medicare by legislation creating Professional Standards Review Organizations (PSRO's).[115] The PSRO's generally will be groups of physicians whose main functions are monitoring the necessity and quality of medical services and establishing professional norms of practice within their geographic areas.[116] To perform these duties, the PSRO's, like the Part B carriers, will require a large statistical data base against which to screen particular case histories.[117] Because of economies of scale, these data

113. *See id.* at 22-23, where it is reported that the total cost for electronic data processing under Part B was $48 million in FY 1971; of this amount, $23 million was subcontracted, and $20.7 million worth of these subcontracts were held by EDS.

114. The Social Security System contracted in 1968 for the development of a "model" data processing system for Part B claims. *See id.* at 5. But the more diversified services offered by EDS were apparently more attractive to the carriers:

> One feature of their system which is quite different from the Pilot, or Model system, for example, is that EDS is in a position to go in and take over, not only the medicare data processing phase of an organization's operations, but also their own business operations. In other words, they can do a whole job for them. They move in their own people. It was a problem for many carriers just to get qualified EDP personnel, and EDS has been successful in securing a number of contracts.

Testimony of Thomas M. Tierney, Director, Bureau of Health Insurance, Social Security Administration, *id.* at 5-6.

115. *See generally* 86 Stat. 1429-45 (1972).

116. Office of Professional Standards Review of U.S. Department of Health, Education and Welfare, PSRO's and Medical Information—Safeguards to Privacy 10 (unpublished. July 22, 1974; copy available in the files of the Buffalo Law Review) [hereinafter cited as PSRO's and Medical Information]. Prior to the PSRO legislation, the primary safeguard to assure that hospitalization was medically necessary under Part A of Medicare was the attending physician's certification of need for treatment. *See* 42 U.S.C. § 1395f(a)(3) (1970). In addition, there was a requirement that participating hospitals establish their own "utilization review committees" to determine the need for hospitalization and the quality of the care provided. *See* 42 U.S.C. §§ 1395x(e)(2), (j)(8), (k)(1970); S. LAW at 119-21. For a discussion of the problems with this system that gave rise to the PSRO approach, see Note, *Federally-Imposed Self-Regulation of Medical Practice: A Critique of the Professional Standards Review Organization,* 42 GEO. WASH. L. REV. 822 (1971); PSRO's and Medical Information at 10. Hospital utilization review committees may be retained under the new system, but PSRO is responsible for the effectiveness of their review. *See* Note, *supra,* at 825-26.

117. The statute gives PSRO's broad authority to gather information relevant to their duties. 42 U.S.C. § 1320e-4(f)(1)(B) (Supp. 1973). At the same time it requires them to utilize "to the greatest extent practical" coding methods which "provide maximum confidentiality as to patient identity." 42 U.S.C. §§ 1320c-4(a)(4), c-15 (Supp. 1973). The HEW report, PSRO's and Medical Information, at 10, notes, "For

bases will probably be stored in a series of compatible regional computer centers, each collecting information from a number of local PSRO's.[118] Thus, a new national data network for handling medical information may be in its formative stages.[119]

As massive as the Medicare program is, it constitutes only a part of the maze of federal health care programs, each of which varies in size, complexity and approach. Medicaid, for example, paralleled Medicare by providing federal support for health care to the poor,[120] thereby giving rise to extensive data-sharing relationships between state and federal welfare agencies,[121] and frequently with private con-

---

the setting of norms based upon the 'typical patterns of practice in the region where the PSRO is located' . . . an enormous amount of data will have to be collected to determine what practice is typical with respect to care, diagnosis and treatment."

118. The possibility of integrating PSRO, Medicare, and National Health Insurance into a single system is prominently mentioned in a document prepared by a Department of Health, Education and Welfare Task Force on PSRO Information Systems Model(s), Nov. 15, 1974, at 3:

> As one alternative, consideration was given to appending the PSRO data and processing to the existing Medicare and Medicaid payment systems. A prototypical model was developed reflecting an achievable and desirable concept which would require major changes in existing agency functions. Should National Health Insurance be enacted this model may be the optimum approach to the information system. The urgency of the PSRO information needs and the problems associated with modifications of the Medicare and Medicaid billing systems strongly indicates that an "interim" PSRO information processing system should be established.

It should be noted that sharing of data processing facilities would not necessarily involve sharing of data. In discussing the establishment of "group processors" to provide groups of PSRO's with data processing services, this report states:

> The data acquired and processed at the group processor will be organized and maintained on a local PSRO basis. No further aggregation of this data is expected at this point.

Id. at 5. *See also Hearings on Administration of Federal Health Benefit Programs Before a Subcomm. of the House Comm. on Government Operations,* 92d Cong., 1st Sess., pt. 3, at 168 (1971).

119. Because a large part of the data handled by PSRO's is statistical in nature, it may be possible to delete or obscure identifying information and thereby minimize threats to individual privacy. In the absence of specific rules governing the details of data processing procedures, it seems rather premature to assert, as the Director of the ACLU's Project on Privacy and Data Collection has done, that the PSRO legislation marks "the incipient stages of yet another massive system of databanks, a system whose fodder will include some of the most sensitive information extant on millions of Americans." PSRO's and Medical Information at 27.

120. *See generally* Stevens & Stevens, *Medicaid: Anatomy of a Dilemma,* 35 LAW & CONTEMP. PROB. 348 (1970).

121. Federal-state information sharing extends beyond the health care field to other categories of public assistance. *See, e.g.,* the following statement by Richard D. Shepherd, Director, Division of Systems Coordination and Planning, Office of Administration, Social Security Administration:

> The BENDEX [beneficiary data exchange] system was devised jointly by the Social Security Administration and the Social and Rehabilitation Service (SRS) to provide State public assistance agencies with social security benefit information and an automatic notification to the States of any material change

tractors as well.[122] Medical aid programs for more narrowly defined social problems, such as alcoholism or drug abuse, also contribute to the collection and sharing of medical information, and often these programs interact with the record-keeping systems of other bureaucracies.[123] Only rarely has there been a serious public examination of the privacy implications of these various data systems, and efforts at comprehensive analysis of personal information flows associated with

---

in the beneficiary/recipients social security status. . . . The system is effective in all States except Pennsylvania and for all categories of grants-in-aid. . . .

. . . .

. . . The individual States will decide whether to pay their own supplement to the supplemental security income benefit amounts and the scope of their medicaid program after January 1, 1974, and whether they want Federal administration of either or both of these optional provisions. Regardless of a State's options, information from the supplemental security record will be of use to the States. For instance, the Social Security Administration will have the record of resources available to the individual, mailing addresses, representative payee involvement, etc., and via data exchange with States on a timely basis, much redundancy can be avoided in establishing eligibility for State social service, or State administered supplementation and/or medicaid.

Hearings on Federal Information Systems, pt. 2, at 290.

122. *Cf. Hearings on National Health Insurance Before the House Comm. on Ways and Means,* 93d Cong., 2d Sess., vol. 7, at 3127 (1974). The following statement was made by Margaret Ewine, National Health Law Program, Los Angeles, California, before the committee:

Although [the statute] . . . makes no express provision for the use of fiscal intermediaries in the administration of the Medicaid program, many Blue Cross and Blue Shield plans sought out and received roles in the program's administration through negotiations with participating State agencies. . . . Blue Cross [is involved] . . . in the administration of Medicaid in at least half the states.

Id. The Blues are not the only organizations from the private sector involved in administration of Medicaid; according to newspaper reports, the state of North Carolina

has awarded a $405 million, 26-month contract to Health Application Systems (HAS), a subsidiary of the California-based Bergen-Brunswick Corp., a health products and services company. HAS has agreed to pay, out of the $405 million, all valid [Medicaid] claims [by State residents], and hopes to run the operation so efficiently that some will be left over as a profit.

The Washington Post, July 11, 1975, at A2, col. 1.

123. A brief history of the confidentiality provisions relating to drug abuse and alcohol abuse patient records is set forth in the proposed rules issued by the Department of Health, Education and Welfare and the Special Action Office for Drug Abuse Prevention. 39 Fed. Reg. 30426, 30427-28 (1974). An example of the ways in which state law or policy can frustrate federal confidentiality policies is provided by news reports of a woman on probation for a state crime who was sent to a federally funded drug treatment program, and told her counselor in the treatment program that she had used marijuana after she had been placed on probation. The counselor, in accord with the program's policies, informed the woman's probation officer, the probation officer informed the sentencing court, and the judge ordered a probation revocation hearing. Officials in the federal funding agency were reportedly redrafting the regulations on confidentiality of treatment records to deal with such problems. The Washington Post, April 3, 1975, at C1, col. 5.

third-party payment for medical services appear to be virtually nonexistent.[124]

Notwithstanding the complexities and gaps in knowledge, several general tendencies affecting personal privacy do seem to emerge from federal third-party payment programs like Medicare. A striking characteristic of the evolution of Medicare and related programs is the frequency with which information-processing tasks resulting from newly legislated programs are added on to existing data systems. Medicare, Medicaid, and later health-related programs were built into existing data nets like the Blue Cross wire system and the Social Security beneficiary records, and a national health insurance program would quite likely be planned around some existing data processing facility.[125] A variety of factors seem to contribute to this centralization or sharing of data systems. Legislators or administrators developing new benefits may be attracted to the model of a similar, functioning program, and decide to incorporate the new into the old. By the same token, officials who are responsible for administering a newly-enacted program may be under political pressure to get it functioning quickly. Expansion of an existing computer system, rather than development of a completely new one, may make it possible to realize economies of scale, or contribute to administrators' empire-building tendencies by providing an occasion to upgrade facilities for other programs,[126] or to justify larger budgets.[127]

---

124. A notable exception is the report of the MASSACHUSETTS GOVERNOR'S COMMISSION ON PRIVACY AND PERSONAL DATA, *supra* note 106, which surveys health-related record-keeping in the State of Massachusetts. This report is sometimes difficult to follow, which doubtless is more a function of the complexity of the subject matter being described than of the style of the author.

125. *See, e.g.*, note 118 *supra.*

126. For example, the Social Security Administration's upgrading of its data processing and telecommunications facilities under the acronym SSADARS (Social Security Administration Data Acquisition and Response System) was justified by the additional data processing demands associated with the enactment of the supplemental security income program; however, the system improvements will affect the operation of other benefit programs administered by SSA. *See generally* testimony of Richard D. Shepherd, Director, Division of Systems Coordination and Planning, Office of Administration, Social Security Administration, *Hearings on Federal Information Systems,* pt. 2, at 270-73, 281-84.

127. This was reportedly one of the attractive features of the Multi-State Information System in psychiatric patient records, described in text accompanying notes 21-24 *supra.*

> One of the strongest arguments for developing [MSIS] was the opportunity of eliminating the inefficiencies that plague existing state psychiatric record-keeping programs. The majority of non-MSIS states, even now, are only in the earliest, most primitive stages of developing data processing methods to handle psychiatric material. Principally a manual operation in most states until the last few years, these programs are typically the stepsisters of statewide data process-

The greater size of systems and data bases resulting from this apparent trend toward centralization may not be perceived as a risk to individual privacy interests, at least as they are traditionally defined. Although the effect is to make the individual's record accessible to more people and institutions, there still may be little risk that sensitive personal information will "leak" from the system and find its way back to the data subject's circle of relatives and acquaintances. Ironically, the risk that this kind of leakage will occur may be increased if the data-processing organization attempts to be open and responsive to its clientele rather than bureaucratic and remote. Recent congressional testimony by an SSA official indicates both the dilemma facing the agency, and the way in which it is likely to be resolved:

> We are kind of in the middle between the need to efficiently serve the people, which is our basic function, and the need to protect the privacy and confidentiality of our records.
>
> In taking 4, 5, or 6 million claims a year and processing 18 million postentitlement earnings and posting 343 million earnings items, when you are talking about this kind of operation, then we must set up systems and operations so that the district office personnel can get the information readily and efficiently.
>
> Now if we put too many restrictions on obtaining it, then we would have to get too much [identification or authorization] information from people [who are requesting information about their entitlement status], or so much information that it would be difficult to respond to our mission.[128]

In addition, the more comprehensive, accurate and sensitive a data base is, the greater will be the temptation to utilize it for a variety of purposes, ranging from law enforcement to commercial gain to basic or applied social science research. As the Social Security Administration has discovered, the basic threat here seems to arise not so much from illegal intruders and wiretappers as from perfectly legitimate organizations and interests which are able to obtain access through

---

ing organizations, their data often being processed after data from such agencies as the departments of taxation and motor vehicles. Many states feel the need for efficient, automated, psychiatric reporting methods in order that large budgets for mental health departments may be justified, the use of such funds may be monitored, and appropriate care for the patient may be assured.

Curran, Laska, Kaplan & Bank, *Protection of Privacy and Confidentiality*, SCIENCE, Nov. 23, 1973, at 797.

128. Testimony of Richard D. Shepherd, Director, Division of Systems Coordination and Planning, Office of Administration, Social Security Administration, *Hearings on Federal Information Systems*, pt. 2, at 324.

political or legal means.[129] And even if large centralized stores of personal data can be effectively protected against improper or unnecessary access, the popular perception of size and power may remain significant: a widespread belief or suspicion that SSA used its computers as a giant universal surveillance system would doubtless affect the relationship between citizen and government in much the same way that an actual surveillance system would.

A second significant trend that seems apparent in the evolution of third-party payment systems is the pervasive interpenetration of public and private sectors, and of federal and state levels of government, in administering the programs. Undoubtedly, there have been both practical and political reasons for creating a mixed system of carriers, intermediaries, contractors, subcontractors, and federal and state agencies to pay for health care services. Potentially greater resources and expertise can be brought to bear on health care problems than any one sector or level of government could provide acting alone;[130] the

---

129. An official of the Social Security Administration has described some of the demands made on that agency in the following terms:

> [V]arious kinds of requests and demands are received by the Social Security Administration in large numbers daily, and millions are responded to yearly. Attorneys seek information helpful to their clients and frequently try to obtain it by subpoena where the individual concerned refuses to authorize disclosure. Missing persons bureaus and skip-tracer organizations try to get information about persons who have disappeared or have moved leaving no address. Business firms seek data about the size or business or wage patterns of competitors. Organizations request listings of names and addresses for a variety of reasons. Pension fund administrators request wage information. Political organizations and public officials seek information for political advantages.
>
> Law enforcement agencies, naturally are interested in the potential that exists for locating persons.

W. Rubenstein, Confidentiality Under the Social Security Act 8-9 (unpublished, undated; copy available in the files of the Buffalo Law Review). A recent example of a successful attempt to gain access to SSA records is the congressionally-created "parent locator system" which allows welfare officials access to SSA and other federal data systems for the purpose of tracking down parents who have defaulted on their obligation to support minor children. *See id.* at 21; The Washington Post, June 26, 1975, at A3, col. 6.

130. *Cf. Hearings on National Health Insurance Before the House Comm. on Ways and Means,* 93d Cong., 2d Sess., vol. 7, at 2771-72 (1974). The following is part of a statement by Wilbur J. Cohen, of the American Public Welfare Association:

> There is considerable difference of opinion as to the respective roles of the public and private sectors in health financing, organization, delivery, cost containment, and preventive services. . . . The arguments given for utilizing the private sector in these areas usually overstate the case as to what the competitive market forces can contribute to increased efficiency, effectiveness, and access to an improved delivery system. Similarly, the arguments that recourse to the public sector, whether federal or state, can simply, easily or promptly solve the monumental problems facing the health system is clearly overconfidence in our present capacity.
>
> A more realistic appraisal of the situation we face is that we must utilize both the private and public sectors in the management of a nationwide health

power flowing from payment of public monies, collection of personal information, and other aspects of welfare is arguably decentralized to a degree; and organizations working in the health care payment field are given new business rather than being forced out by a federal takeover.[131] Legally, there are simple mechanisms available to extend constraints on the misuse of identifiable records to all of the public and private entities involved in administering the programs.[132] Yet, there may still be some risks in this tendency. As more organizations take part in running or using the systems, lines of authority may become attenuated or blurred, and responsibility difficult to pinpoint. Despite the unity of formal requirements, different organizations may have different perspectives on what information practices are permissible or desirable, and different kinds of interests to protect. And symbiotic relationships between government agencies and private contractors may be unusually threatening in this area because of the large amounts of personal information involved. Recent charges that one of the major data processing contractors for Medicare Part B used improper influence to obtain contracts, made illegal political campaign contributions, and engaged in generally slipshod performance of data processing operations,[133] are merely suggestive of the kinds of advantages a corrupt

---

> system; we must utilize federal, state, and local agencies; we must seek and obtain full and appropriate participation of all providers of services and the consumers of services . . . .

Id.

131. Wilbur Cohen, who was a high-ranking official in the Department of Health, Education and Welfare at the time the original Medicare legislation was passed, described the kind of compromises that were necessary in recent congressional testimony:

> We are using 80 intermediaries now in the program. If you will recall, Mr. Chairman, I had to promise you and Mr. Watts in the executive session in 1965 that I would, as the administrator of the program, fairly utilize a wide variety of fiscal intermediaries. . . .
>
> Now, after 7 or 8 years, we don't need 80 intermediaries to run the program. We could run it with the 9 or 10 who are most efficient.

Hearings on National Health Insurance Before the House Comm. on Ways and Means, 93d Cong., 2d Sess., vol. 7, at 2765 (1974).

132. The Office of General Counsel of the Department of Health, Education and Welfare has taken the position that the statutes and regulations governing confidentiality of personal information are applicable to nonfederal instrumentalities involved in the administration of these programs. In addition, the Department has a standard clause in its contracts which requires subcontractors to agree to abide by the applicable regulations. *Hearings on Federal Information Systems,* pt. 2, at 306-07 (letter from Gerald C. Altman, Jr., Acting Assistant General Counsel, Department of Health, Education and Welfare, to William S. Moorhead, Chairman, Subcomm. on Foreign Operations and Government Information, House Comm. on Government Operations). *See also* W. Rubinstein, *supra* note 129.

133. *See generally* Kelly, *It May Not Be Illegal . . . But Is It Professional,* COMPUTERWORLD, Aug. 22, 1973, at 11; Tracy, *The Poverty Billionaire Comes Calling on Rocky,* The Village Voice, July 12, 1973, at 1, col. 4; *Hearings on Administration of*

contractor could seek by exploiting its unique position and its massive store of personal records.

A final clear trend in third-party payment is the steady expansion of benefits and beneficiaries resulting from the growing governmental presence in the health care field. Apart from the simple growth in medical data processing systems that this expansion implies, there is also the possibility that it could produce widespread changes in official attitudes toward the privacy of medical information. As publicly funded health care becomes ubiquitous, everyone becomes a kind of welfare recipient—and thus joins a group whose privacy has traditionally been readily sacrificed to administrative convenience and pressures for public accountability.[134] As computer-assisted techniques are developed to improve accountability in the government-financed programs—by automatically screening patient records to find patterns and instances of abnormal costs, or unnecessary or unsuccessful treatments, or aberrant patterns of utilization—it becomes apparent that these devices can also be applied to the diminishing segment of health care which is privately financed. Thus, some commentators have argued that licensing of physicians and other health care providers should be supplanted by a system of "output monitoring" patterned on the quality control approaches developed for public health care programs, and built upon a large-scale computer network.[135]

Although public funding inevitably implies some form of public accountability to minimize waste or misappropriation, it remains unclear how much of this function can be achieved with unidentifiable statistical aggregates rather than identified patient records. Conceivably, development of a more universal system of public funding might ease some of the pressures to collect identifiable records. When health benefits are narrowly limited or "targeted"—to particular groups, to certain types of providers, to given levels of cost, or even to specified diseases—it becomes necessary to gather and evaluate sufficient medical, financial and personal data to assure that the complex eligibility

---

Federal Health Benefit Programs Before a Subcomm. of the House Comm. on Government Operations, 92d Cong., 1st & 2d Sess., pts. 3-4 (1971-72).

134. *See generally* Handler & Rosenheim, *Privacy in Welfare: Public Assistance and Juvenile Justice*, 31 LAW & CONTEMP. PROB. 377 (1966); *cf.* Handler & Hollingsworth, *Stigma, Privacy and Other Attitudes of Welfare Recipients*, 22 STAN. L. REV. 1 (1969).

135. Tancredi & Woods, *The Social Control of Medical Practice: Licensure Versus Output Monitoring*, 50 MILLBANK MEMORIAL FUND Q. 99 (1972).

136. *Cf. Hearings on Administration of Federal Health Benefit Programs Before a Subcomm. of the House Comm. on Government Operations*, 92d Cong., 1st Sess., pt. 3, at 169 (1971). The following is testimony of Robert Mayne, Deputy Director of Pro-

criteria have been met. Simplified eligibility standards could make it possible to reduce this data collecton burden.[136] Similarly, replacement of the present patchwork of separate and parallel programs with a unified apparatus for dispensing benefits could reduce the pressure to use computers as surveillance devices which can track down individuals who are "overutilizing" the health care system.[137] However, efforts to make such large-scale structural changes in health care delivery systems inevitably raise a host of controversial practical and political issues, and it seems unlikely that privacy considerations could play more than a marginal role in shaping public funding programs. Perhaps for this reason, efforts to protect medical privacy have tended to focus on legal and administrative devices to control the behavior of those who operate the systems, rather than the underlying justifications for collecting the data in the first place.

II. Privilege and Privacy: The Established Legal Controls

Traditionally, legal controls for the confidentiality of medical information can be divided into two conceptual categories: evidentiary privileges for communications between doctor and patient, and tort actions for invasion of privacy. In theory these two areas of law are

---

gram Operations, Bureau of Health Insurance, Social Security Administration before the Subcommittee:

> The point of the system to be employed is . . . an everchanging consideration dependent upon changes in the law. What is required of the system, now under the medicare law as a primary part of the operation, is the reasonable charge determination, because of the requirements on how reasonable charge is to be made. A simple change in the law, if Congress were to do this, would make a complete difference in the system. It would wipe out two-thirds of the EDP system operation as such.

Id.

137. *See, e.g.*, The Washington Post, Aug. 12, 1974, at C-1, col. 3, where it reads:

> District [of Columbia] and Maryland welfare officials, under federal pressure to reduce welfare cheating, are discussing an agreement under which they would exchange information telling welfare authorities about outside income being received improperly and secretly from out of state by persons on public assistance.
>
> . . . .
>
> "One of the most important causes of error in maryland [sic] is unreported earnings," [a state official] said . . . . "A lot is attributable to unreported earnings in the District" . . . .
>
> . . . .
>
> "Basically," he said, the exchange of information entails "cross referencing social security numbers" of welfare recipients against earning statements filed by employers in the two jurisdictions and then against unemployment compensation records.

complementary, since privilege statutes are designed to govern disclosures in some official forum such as a court or legislature, while privacy actions are designed to deal with disclosures to the general public. In practice, however, privacy and privilege doctrines are largely irrelevant to the problems posed by modern computerized medical information systems, and they are both subject to abuse by organizations that are bent on collecting and using identifiable medical records.

At the threshold, traditional privacy and privilege doctrines suffer from the common disability of being creatures of diverse state statutory or common law provisions rather than uniform national standards. As a result, they are extremely difficult to apply to a technology that frequently is part of multistate or multinational communications networks. A medical information system like the MIB or MSIS that transmits personal data across state lines for storage or processing, and then moves it back to the point of origin or to some other destination for end use or retransmission, poses obvious problems as to which state's law should apply when there is a challenge to the propriety of a particular use or disclosure. In addition to these relatively straightforward conflicts, gaps, and inconsistencies, there remain difficult problems of federalism when the record system reflects a mix of federal, state and private interests. If a medical information system is owned and operated by the federal government and is integral to the functioning of a health care program that is wholly supported by federal funds, it seems reasonable enough to make the federal statutes and regulations relating to confidentiality preemptive of state law. If, on the other hand, the federal government requires a proportional funding contribution from the State of New York to support a health care program for New York citizens which is administered by a private carrier that is located in Illinois but has a data processing subcontract with a Texas corporation whose computers are continually in communication with federal computers in Maryland, it is difficult to say, as a general matter, whether federal or state interests are predominant, or indeed which states' interests ought to be taken into account. Beyond these systemic difficulties, however, the existing state-created laws of privacy and privilege have substantive shortcomings which can make them more effective as a shield for system operators than as a safeguard for data subjects.

A. *The Doctor-Patient Privilege*

The rule that confidential communications from a patient to his doctor during the course of treatment are inadmissible in judicial

proceedings did not exist at common law, and does not exist today in a significant minority of states where there is no statute creating the privilege.[138] The doctor-patient privilege has been repeatedly criticized by leading commentators on the law of evidence, on the ground that it interferes unduly with the truth-seeking functions of courts and other tribunals, and attempts to expand the privilege frequently encounter strong opposition for this reason.[139]

Even when a doctor-patient privilege does exist, it may be so narrowly confined as to be of little value to an individual seeking to prevent disclosure of his medical records. If the body seeking the records is legislative or administrative rather than judicial, the patient may not be protected at all by the privilege statute:

> The status of the privilege in proceedings before state legislative and administrative committees is uncertain. Several statutes are, in terms, limited to judicial proceedings, while the others contain language prohibiting certain disclosures without defining the locus in which the prohibition is to take effect. . . .
>
> . . . .
>
> As in the case of Congressional committees, there is apparently no way of forcing federal administrative agencies to recognize the privilege.[140]

Once it is established that there is a privilege statute applicable to the forum where a controversy is pending,[141] the party asserting the

---

138. *See, e.g.*, J. WALTZ & F. INBAU, MEDICAL JURISPRUDENCE 256 (1971) [hereinafter cited as J. WALTZ & F. INBAU].

139. *See, e.g.*, Chafee, *Privileged Communications: Is Justice Served Or Obstructed by Closing the Doctor's Mouth on the Witness Stand?*, 52 YALE L. J. 607 (1943); Morgan, *Suggested Remedy for Obstruction to Expert Testimony by Rules of Evidence*, 10 U. CHI. L. REV. 285, 290-92 (1943). J. WALTZ & F. INBAU at 253 conclude:

> A death knell for the general physician-patient privilege has been sounded. The law is on the verge of letting medical truth—and all of it—be known in the courtroom . . . .

140. Note, *Legal Protection of the Confidential Nature of the Physician-Patient Relationship*, 52 COLUM. L. REV. 384, 388-90 (1952).

A case that is frequently cited for the proposition that state legislative committees are subject to the privilege is New York City Council v. Goldwater, 284 N.Y. 296, 31 N.E.2d 31 (1940). There, the court relied upon a privilege statute to deny enforcement of a subpoena duces tecum which sought access to hospital patient records as part of a City Council investigation of negligence and maladministration in the treatment of patients. However, the holding may be limited to the particular factual setting. *See* Note, *supra*, at 389.

141. It remains an open question whether federal courts are constitutionally required under the *Erie* doctrine to follow the privilege rules of the states. The new Federal Rules of Evidence as approved by the Supreme Court would have created federal rules of privilege, but this aspect of the Rules was changed by the Congress. *See gen-*

privilege will still have to meet the conditions specified by the statute. Four kinds of requirements are common in privilege legislation: the professional status of the party testifying; the existence of a physician-patient relationship; the nature of the communication or information in question; and the necessity of the communication to treatment.[142] Each of these conditions may cause problems in the context of contemporary medical practice.

Often privilege statutes apply only to physicians, surgeons and other narrowly defined categories of medical personnel. Thus, if medical data are gathered by someone whose title does not fit the statutory categories, such as a member of a hospital administrative staff or a welfare intake worker, the privilege may not be effective in some states.[143] Similarly, communications made in the course of treatment by "helping professionals" other than physicians—psychologists, social workers, family counselors, and the like—may be unprivileged,[144] even though the mental or emotional problems being treated generate far more sensitive information than routine medical care. The existence of a privilege may also be questionable when information generated by a treating physician is placed in the hands of third-party custodians such as hospital record administrators or independent data systems like the MSIS.[145] Since these categories of record-keepers are unlikely to be mentioned in the privilege statute, the issue of disclosure may turn on whether the record custodian can be termed an agent of the doctor under relevant state law.

---

erally Anderton, *The Constitutional and Erie Implications for Federal Diversity Cases of the Privilege Provisions of the Proposed Federal Rules of Evidence,* 8 LINCOLN L. REV. 151 (1973); Santarelli, *The Supreme Court's Proposed Federal Rules of Evidence: The Authority and Necessity for Codification in Retrospect,* 32 FED. BAR J. 257, 264-69 (1973); Pub. L. No. 93-595, Rule 501 (Jan. 2, 1975).

142. Note, *supra* note 140, at 390-91.

143. *See* J. WALTZ & F. INBAU at 243, where they state:

> To the extent that hospital records include confidential information supplied by a patient to his physician and the physician's diagnostic findings, they too are privileged. Some courts, believing that privilege statutes should be narrowly construed because of their truth-frustrating attributes, do not extend the privilege to information obtained and recorded by someone other than a physician.

144. *See, e.g.,* Note, *Functional Overlap Between the Lawyer and Other Professionals: Its Implication for the Privileged Communications Doctrine,* 71 YALE L. J. 1226, 1254-1260 (1962). A few states have enacted psychotherapist-patient privileges. *See, e.g.,* CAL. EVID. CODE §§ 1010-1026 (West 1966).

145. During the development of the Multistate Information System for Psychiatric Patient Records, discussed in note 34 *supra,* doubts about the applicability of the privilege were resolved by enactment of a special statute in New York, the state where the computer files were kept, providing that records in MSIS. were immune from subpoena. Curran, Laska, Kaplan & Bank, *Protection of Privacy and Confidentiality,* SCIENCE, Nov. 23 1973, at 797, 799-800.

Other technical defects sufficient to defeat the privilege occasionally arise from a failure to establish a true doctor-patient relationship, or from the fact that the information in question was not deemed necessary for medical treatment. Thus, it has been held that "since the relation between a patient committed to a mental institution and the official in charge of that institution is not the professional relation contemplated by statute," the privilege was not applicable.[146] "Treatment purposes" may be defined to exclude many common situations in which sensitive data is collected, such as pre-employment or pre-insurance medical examinations,[147] as well as less normal occurrences like attempts to obtain narcotics or other treatment illegally.[148] Finally, the patient can waive the protections of the privilege, and frequently is forced to do so either by an express contract clause in insurance policies[149] or by implication when he brings an action to recover for personal injuries.[150] Since waiver verges into the problem of the consent defense to an invasion of privacy claim, the two principles will be discussed together in the following section. As will be seen, the easy potential for abuse of the waiver principle, like other doctrinal shortcomings in the doctor-patient privilege, is in large measure attributable to the law's implicit assumption that the dominant mode for delivering medical services will be the individual physician or the small clinic. Consequently, the doctrines fail to take account of the ways in which the recent bureaucratization has affected medical record-keeping. Trends toward the paraprofessionalization of health care, the separation of record-keeping from the doctor's direct control and supervision, the growing utility of medical records for purposes beyond treatment of the data subject, and the individual's powerlessness and unequal bargaining power in comparison to the large, impersonal institutions which make demands for access to his records, all tend to shift the

146. Munzer v. Blaisdell, 183 Misc. 773, 776, 49 N.Y.S.2d 915, 918 (Sup. Ct. 1944). It may be significant that the data subject in this case was trying to recover damages from the superintendent of the state hospital for the mentally ill for disclosing privileged records, rather than simply asserting the privilege to block testimony. J. Waltz & F. Inbau note that "the majority of jurisdictions hold that the fact that the afflicted person is a patient in a public institution, such as a hospital for the insane or mentally ill, does not strip him of the physician-patient privilege." J. WALTZ & F. INBAU at 241.

147. J. WALTZ & F. INBAU at 239.

148. *Id.* at 242. As further examples, the authors state: "The privilege would undoubtedly be held inapplicable to a fugitive who sought to have a police-inflicted gunshot wound treated or to have his appearance altered through plastic surgery." *Id.*

149. "Except in a minority of states, Michigan being the most important, the courts give effect to an express waiver of the doctor-patient privilege contained in applications for health or life insurance or in the policy itself." *Id.* at 245-46.

150. *See id.* at 247, 249.

focus away from the traditional courtroom confrontation in which the patient can rely on relatively clear legal principles and the medical profession's strong ethical tradition of confidentiality to block damaging disclosures.

B. *Invasion of Privacy Actions*

Unlike the doctor-patient privilege, statutory or common-law causes of action for invasion of privacy were not formulated with the specific objective of regulating disclosures of medical information. As a result, the relevance of the legal principles to the realities of medical record use and abuse frequently is rather tenuous. Among the four general categories of common-law actions for invasion of privacy,[151] only one, public disclosure of private facts, seems reasonably applicable to the abuses that are likely to arise in modern medical record systems.[152] "Public disclosure" generally has meant widespread dissemination of the information, if not mass media publicity,[153] and the few reported cases involving medical information seem to arise out of sensationalized reports of freakish maladies,[154] or medical case history studies in which the researcher has failed to conceal the subject's identity.[155] In contrast to these unusual situations, the threatening

151. The four categories are intrusion upon an individual's seclusion, appropriation of a person's name or likeness, unreasonable publicity for private facts, and publicity which places the individual in a "false light" in the public eye. *See generally* RESTATEMENT (SECOND) OF TORTS § 652A (1965); W. PROSSER, TORTS, § 112 (4th ed. 1971); Prosser, *Privacy*, 48 CALIF. L. REV. 383, 392-93 (1960).

152. *Cf.* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089, 1156-58 (1969).

153. *Id.* at 1157:

> [B]efore an injured party can recover for a public disclosure of private facts . . . he must show that the private information was given "publicity," or that it was communicated to the public at large. By way of contrast, a plaintiff in an action for defamation need show only that the derogatory statement in question was "published"—that the defendant communicated it to a third party. A few exceptions to the mass publication requirement for privacy actions have been recognized, most of them involving instances in which "the information was gained by wrongful prying or . . . its communication involves a breach of confidence or the violation of an independent duty."

154. *See, e.g.*, Barber v. Time, Inc., 348 Mo. 1199, 159 S.W.2d 291 (1942); Bazemore v. Savannah Hosp., 171 Ga. 257, 155 S.E. 194 (1930).

155. *E.g.*, Griffin v. Medical Society of the State of New York, 7 Misc. 2d 549, 11 N.Y.S.2d 109 (Sup. Ct. 1939). An unusual recent example of the failure to conceal the identity of a patient in a medical history report is Doe v. Roe, 42 App. Div. 2d 559, 345 N.Y.S.2d 560 (1st Dep't), *aff'd*, 33 N.Y.2d 902, 307 N.E.2d 823, 352 N.Y.S.2d 626, *motion to amend remittitur granted*, 34 N.Y.2d 562, 310 N.E.2d 539, 354 N.Y.S.2d 941 (1973), *cert. dismissed as improvidently granted*, 95 S. Ct. 1154 (1975). There, a psychotherapist published a book about a patient and her family, based on intimate revelations made during seven years of psychotherapy. Plaintiff claimed that anyone who knew the family could easily identify them in the book.

disclosures in modern medical record-keeping are likely to be low-visibility transactions—transferring identifiable records from one computer operator to another under the "buddy system,"[156] or permitting an investigator to search the files without proper authorization,[157] or releasing information to an employer, credit grantor, or acquaintance of the data subject.[158] In these situations, the concerns for first amendment freedom of the press that have dominated the "public disclosure of private fact" cases are largely absent; the interest in promoting debate or issues of public importance is at least tangential when the

---

156. Professors Westin and Baker, after studying a number of computer systems handling personal information, concluded that "computerization has not halted the informal or 'buddy system' exchanges that existed in the manual era, and may even have increased their volume in some cases." WESTIN & BAKER at 255. A survey of the practices of selected federal agencies relating to sharing of personal information concluded:

> The "common law" of interagency transfers of information that obtains in agencies that have no regulations governing their information—and indeed, in a fair number of agencies that do—seems to be that if a "responsible" member of one agency makes a request—preferably, but not invariably, in writing—for particular information about an individual or business entity to a person in another agency who has access to the information, and if the party who requests the information states his reasons for needing it—often no more than a bare statement that he wants it for undisclosed "official purposes"—then the transfer of information will be made with no further ado. Generally no inquiry is made into the authority of the requesting agency to gather the information sought, and none is cited beyond perhaps a bare statement of "need." The requesting agency usually does not inquire and is not told about the confidentiality restrictions, if any, under which the information is held . . . .

A. Bell, Interagency Transfers of Information in Individually Identifiable Form 17 (Report prepared for the Committee on Rulemaking and Public Information of the Administrative Conference of the United States, Sept. 10, 1973).

157. *Cf.* Miller, *supra* note 152, at 1149; WESTIN & BAKER at 148.

158. *See, e.g.,* E. SPRINGER, AUTOMATED MEDICAL RECORDS AND THE LAW 14-15 (1971), which reads:

> There is the story of a young career woman employed by a . . . company which gave all its key employees free annual medical examinations. During her routine physical examination she mentioned in passing that she had been undergoing psychoanalysis for several years. The woman refused to discuss the matter further but was badgered into accounting all the details because the examining physician insisted that it was impossible for him to complete his medical examination without this information. She was assured that the information would, of course, be kept private. Within two weeks, her immediate supervisor knew of the details and within three, all of her co-workers.
>
> . . . .
>
> Other companies have major medical plans which reimburse the employee for medical and prescription drug bills. However, it is usually necessary to obtain complete statements of all visits to physicians and all pharmaceutical bills. . . . These are not filed with the insurance company, but rather with the corporations themselves which in turn forward the claims. Token pretense is made of information privacy by mailing the forms in sealed envelopes.

See also Joint Hearings on Privacy Before the Ad Hoc Subcomm. on Privacy and Information Systems of the Senate Comm. on Government Operations and the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 93d Cong., 2d Sess., pt. 2, at 1039-40 (1974); Note 188 *infra.*

information is dispersed through an elite rather than a mass medium, and the data is of little or no general interest.[159]

The difficulty of fitting many kinds of medical data disclosures into the traditional privacy categories may have given rise to the miscellany of alternative theories that occasionaly appear when invasion-of-privacy claims are brought against doctors. Damage actions have been based upon an obligation to be silent that is implied in the contract between physician and patient,[160] a fiduciary duty imposed on the doctor as a result of his power over the patient,[161] and implied rights of private action under licensing or testimonial privilege statutes.[162] More ingenious litigants have ranged farther afield, basing actions for unauthorized disclosure of medical records on the theory that the disclosure was a commercial exploitation of the patient's name or likeness,[163] or a prima facie tort,[164] or malpractice.[165] Commentators have added to the confusion by suggesting that a new breach of privacy

---

159. Due to the Supreme Court's dismissal of certiorari in the *Roe v. Doe* case, the question of what constitutional standards are applicable to a "public disclosure of private facts" case involving medical records remains open. *Cf.* Gertz v. Welch, 94 S. Ct. 2997 (1974) (defamation action by private individual); Time, Inc. v. Hill, 385 U.S. 374 (1967) ("false light" invasion of privacy).

160. *E.g.*, Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793 (N.D. Ohio 1965). In *Hammonds*, the court states the following:

> Doctor and patient enter into a simple contract, the patient hoping he will be cured and the doctor optimistically assuming that he will be compensated. As an implied condition of that contract, this Court is of the opinion that the doctor warrants that any confidential information gained through the relationship will not be released without the patient's permission. Almost every member of the public is aware of the promise of discretion contained in the Hippocratic Oath, and every patient has a right to rely upon this warranty of silence. The promise of secrecy is as much an express warranty as the advertisement of a commercial entrepreneur. Consequently, when a doctor breaches his duty of secrecy, he is in violation of part of his obligations under the contract.

Id. at 801. *See also* Hague v. Williams, 37 N.J. 328, 181 A.2d 345 (1962).

161. *Cf.* Alexander v. Knight, 197 Pa. Super. 79, 177 A.2d 142 (1962).

162. *Cf.* Clark v. Geraci, 29 Misc. 2d 791, 208 N.Y.S.2d 564, 567 (Sup. Ct. 1960); Berry v. Moench, 8 Utah 2d 191, 331 P.2d 814 (1958).

163. In Griffin v. Medical Society of the State of New York, 7 Misc. 2d 549, 11 N.Y.S.2d 109 (Sup. Ct. 1939), plaintiff's physician took pictures of him before and after treatment, and published them without consent in a medical journal article on "The Saddle Nose." Plaintiff brought his action under the New York statutory provision which prohibits appropriation of a person's name or likeness for commercial purposes. N.Y. Civ. Rights Law §§ 50-51 (McKinney 1948). The court reasoned that the medical journal article might well be a form of commercial exploitation:

> An article, even in a scientific publication, may be nothing more than someone's advertisement in disguise. . . . Publicity of a kind which is tantamount to concealed or subtle advertising is sometimes freely given, or exchanged for some immediate or remote benefit anticipated by the publisher.

7 Misc. 2d at 550, 11 N.Y.S.2d at 110.

164. *E.g.*, Felis v. Greenberg, 51 Misc. 2d 441, 273 N.Y.S.2d 288 (Sup. Ct. 1966); Clark v. Geraci, 29 Misc. 2d 791, 208 N.Y.S.2d 564 (Sup. Ct. 1960).

165. Clark v. Geraci, 29 Misc. 2d 791, 208 N.Y.S.2d 564 (Sup. Ct. 1960).

tort be added to the established common-law categories: an action for "breach of confidence" which "would be a recognition of the special characteristics of secrecy in the physician-patient relationship."[166]

Once a plaintiff succeeds in finding a plausible theory to fit his claim, he still may find his recovery barred by one of the affirmative defenses (confusingly refered to as "privileges") that have developed in the law of privacy.[167] Courts have recognized that other health-care professionals have a qualified right[168] to disclose sensitive information to individuals and organizations having a reasonable "need to know": those who might be infected by the data subject's contagious disease,[169] or the patient's spouse,[170] or the staff of a school where the patient is enrolled,[171] or those who need the information to protect the national security.[172] In addition, the patient's consent, whether explicitly given

166. Note, *Action for Breach of Medical Secrecy Outside the Courtroom,* 36 U. CIN. L. REV. 103, 108 (1967).

167. *See generally* Miller, *supra* note 152, at 1160-62.

168. The qualified privilege can be lost if it is exercised unreasonably or in bad faith. *See id.* In the present context, the privilege will generally be referred to as an affirmative defense in order to avoid confusion with the doctor-patient testimonial privilege.

169. *E.g.,* Simonsen v. Swenson, 104 Neb. 224, 177 N.W. 831 (1920) (physician told patient's landlady that he had a contagious disease, and that she should disinfect his bedclothes; court held that patient could not recover under statute providing that "betrayal of a professional secret to the detriment of a patient" was unprofessional conduct).

170. In Curry v. Corn, 52 Misc. 2d 1035, 277 N.Y.S.2d 470 (Sup. Ct. 1966), the wife brought an action against her doctor for revealing information to her husband "with the intent and expectation" that the husband would use this information against her in a pending divorce action. The court held that such a disclosure was not actionable: "As a prospective husband or wife is entitled to know before marriage whether his or her future spouse is suffering from a diseased condition . . . it would appear to follow that during marriage each has the right to know the existence of any disease which may have a bearing on the marital relation." 52 Misc. 2d at 1037, 277 N.Y.S.2d at 471; *cf.* Berry v. Moench, 8 Utah 2d 191, 331 P.2d 814 (1958).

171. Iverson v. Frandsen, 237 F.2d 898 (10th Cir. 1956), was brought as a defamation action rather than an invasion of privacy claim, but it illustrates the serious abuses that can be immunized by this kind of affirmative defense. The plaintiff, a young child, was treated at a state mental hospital for claustrophobia, and while under treatment she was given a standard test by a staff psychologist which was interpreted as indicating that she was "at the high-grade moron level of general ability." 237 F.2d at 900. Subsequently the psychologist's report was forwarded to the guidance counsellor at her school, and "[i]t was from this source that embarrassing rumors apparently emanated concerning the mental condition of appellant." *Id.* The court held that the plaintiff had failed to show actual malice on the part of the psychologist, which was necessary to defeat the qualified privilege. "It was a professional report made by a public servant in good faith representing his best judgment, and therefore could not be maliciously false." *Id.*

172. Clark v. Geraci, 29 Misc. 2d 791, 793, 208 N.Y.S.2d 564, 567 (Sup. Ct. 1960) (dictum).

or implied from the factual circumstances,[173] is generally regarded as a valid defense to an invasion of privacy claim.[174] Since the reported medical privacy cases have little useful discussion of the consent principle, commentators often rely on the analogous body of doctrine developed to deal with the question of whether a patient has given informed consent to medical treatment.[175]

Despite some contentions that the concept of "informed consent" to treatment is confusing and lacks content,[176] it is widely understood that the patient's valid consent must be premised on two factors: sufficient information about risks and benefits to permit an intelligent choice, and freedom to choose without coercion.[177] Recent cases and commentaries suggest a growing skepticism as to whether either of these two conditions is usually satisfied in the routine transactions that comprise the doctor-patient relationship. The duty to disclose risks, which traditionally was based upon deference to the physician's discretion and the prevailing standard of practice within the medical community,[178] has been recast in a few recent decisions to require dis-

---

173. *See, e.g.,* Note, *Medical Practice and the Right to Privacy,* 43 MINN. L. REV. 943, 952-53 (1959), which reads:

> [C]onsent will be implied to any privacy invasion that the patient can reasonably expect to be necessary for proper diagnosis or treatment of his case. For example, by consulting a doctor, the patient impliedly consents to the doctor's keeping ordinary medical records of the patient's case, and to the customary and foreseeable use of these records.

174. *See generally* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information Oriented Society,* 67 MICH. L. REV. 1089, 1170-73 (1969).

175. *E.g.,* J. WALTZ & F. INBAU at 278 (principles relating to informed consent to therapy are "broadly applicable" to consent to invasion of privacy); *cf.* Note, *Medical Practice and the Right to Privacy,* 43 MINN. L. REV. 943, 952-53 (1959).

176. *See, e.g.,* J. WALTZ & F. INBAU at 152 (informed consent is "another of those expressions, current in the medical-legal lexicon, that may possess more felicity than content"); Plante, *An Analysis of "Informed Consent,"* 36 FORDHAM L. REV. 639 (1968) (informed consent an "unfortunate journalistic expression [which] has caused confusion"). Part of this confusion undoubtedly resulted from frequent failure to make the distinction between the two major theories of recovery for unauthorized treatment, malpractice and battery, and to this extent the confusion would not be cause for concern in the privacy context. *See generally* Plante, *supra.*

177. J. WALTZ & F. INBAU at 156.

178. *See, e.g.,* Salgo v. Leland Stanford Jr. University Board of Trustees, 154 Cal. App. 2d 560, 578, 317 P.2d 170, 181 (1957); Kesserick & Mankin, *Medical Malpractice: The Right To Be Informed,* 8 U. SAN FRANCISCO L. REV. 261, 267-68 (1973); Plante, *supra* note 151, at 658. This policy was premised on the belief that "much of the risk [is] of a technical nature beyond the patient's understanding." Roberts v. Wood, 206 F. Supp. 579, 583 (S.D. Ala. 1962). It was also premised on the belief that disclosure of all risks, however remote, "may well result in unduly alarming the patient, who is already apprehensive, fearful and dejected." Oppenheim, *Informed Consent to Medical Treatment,* 11 CLEV.-MAR. L. REV. 249, 251 (1962). Patient fear, in turn, might "actually increas[e] the risks by reason of the physiological results of the apprehension itself." 154 Cal. App. 2d at 578, 317 P.2d at 181 (1957). Consequently, "good medical practice,"

closure of "all information relevant to a meaningful decisional process."[179] The rationale of these recent decisions—the fact that the patient's reliance on the doctor for relevant information is "well-nigh abject,"[180] and the likelihood that a standard based on prevailing medical practices would provide little or no protection for the patient[181]—seems equally applicable to privacy questions. At the same time, full disclosure of privacy risks associated with possible uses of his medical records should pose no threat to the patient's well-being. As a practical matter, however, it is doubtful whether the full-disclosure-of-risks notion is a useful approach to privacy questions. When patient data is collected, privacy-threatening future uses may be unforeseen or unforeseeable; the doctor or paraprofessional who deals with the patient may be so little involved in the details of record-keeping or the privacy issue that he would not be aware of even the obvious risks; and the patient faced with a serious health problem will generally not be able to mobilize much attention for privacy problems. More important, it is difficult to imagine many situations in which a patient really has much of a choice as to whether he should give out or authorize later disclosures of particular items of information.

The general rule, at least in the consent-to-treatment situation, is that individuals who are of sound mind and sufficient age are rebuttably presumed to be qualified to give or withhold consent.[182] Yet, there is some empirical evidence that, even in the best of circumstances,[183] pa-

---

measured by a professional community standard, was the test for disclosure of risks. *See* Kessenick & Mankin, *supra*, at 267-70.

179. Cobbs v. Grant, 8 Cal. 3d 229, 242, 502 P.2d 1, 10, 104 Cal. Rptr. 505, 513 (1972) (en banc).

180. Canterbury v. Spence, 464 F.2d 772, 782 (D.C. Cir. 1972). Because of this dependent position of the patient, the court reasoned, the law "exacted obligations beyond those associated with arms-length transactions." *Id.* The court left open the possibility that "sound medical judgment" would justify nondisclosure of risks in particular situations. *Id.* at 789. But the general tenor of the opinion suggests that such claims would be carefully and skeptically scrutinized. *See also* Berkey v. Anderson, 1 Cal. App. 3d 790, 82 Cal. Rptr. 67 (1969).

181. *See Canterbury v. Spence*, where the court stated:

> [T]o bind the disclosure to medical usage is to arrogate the decision on revelation to the physician alone. Respect for the patient's right of self-determination on particular therapy demands a standard set by law for physicians rather than one which physicians may or may not impose upon themselves.

464 F.2d at 784.

182. J. WALTZ & F. INBAU at 169. The authors note that the presumption "falls away in the face of evidence that the person was delirious or comatose, intoxicated, under the influence of drugs, or otherwise incapable of exercising rational judgement." *Id.*

183. The study that highlighted these problems of the voluntariness of informed consent took place in a major university medical center, with peer review committees to assure that proper consent procedures were followed. Bradford H. Gray, Human Ex-

tients' freedom of choice will be overborne by their emotional need to place absolute reliance on their doctors' recommendations,[184] or their reluctance to question the judgment of a high-status professional.[185] In one recent study, researchers concluded that about half of the members of a group of women who had volunteered to take an experimental drug during childbirth had not given full and free consent.[186] If patients are unable to exercise independent judgment on matters that so directly and immediately affect their physical well-being, there seems to be little chance that they could act autonomously regarding collateral matters of information use.

Frequently, of course, the patient will also be under overwhelming economic pressure to give whatever consent might be requested. In the field of third-party payment, the general practice seems to favor use of broadly-worded authorizations that provide maximum convenience for the paying organization, and virtually no protection for the patient. A claim form used in the New York statewide employees' health insurance program requires the claimant to sign a statement saying "I hereby authorize any Insurance Company, Organization, Employer, Hospital, Physician, Surgeon, or Pharmacist to release any information requested with respect to this claim and the attached bills."[187] The standard form reportedly used in the New York no-fault program is at least as broad, providing that "[t]his authorization, *or photocopy hereof,* will authorize you to furnish all information you may have regarding my condition

---

perimentation in Medical Research: A Sociological Study 37 (unpublished Ph. D. dissertation, Yale University, 1973, now published as HUMAN SUBJECTS IN MEDICAL EXPERIMENTATION: A SOCIOLOGICAL STUDY OF THE CONDUCT AND REGULATION OF CLINICAL RESEARCH (1975)). The experimenters required a written consent, and they "believed in the ethical validity of the principle of informed consent." *Id.* at 232.

184. *See id.* at 129, where it was noted that "the striking thing about subjects' responses was the extent to which they reflected faith and trust in physicians, even to the point where assumptions of no risk were made when apparently no knowledge was present." One inference drawn from these findings was that "many people apparently cannot conceive of a physician in a nontherapeutic role" and consequently they will assume that anything a physician wants them to do is for their own benefit. *Id.* at 228. *See also id.* at 234.

185. The indigent clinic patients included in the study group, who were treated by different doctors at various times and had not established a personal relationship with any physician, were unwilling to question what they thought was the doctor's recommendation that they participate in the experiment because they were apparently intimidated by the "wide status gulf between them and the physicians." *Id.* at 243-44.

186. Of the patients participating in the experiments, 39 percent did not understand that they were taking part in an experiment; 8 percent felt that they had been coerced into participating; and another 6 percent were indifferent to their own involvement in the experiment or gave no reason other than the belief that their doctors wanted them to take the drug. *Id.* at 142.

187. Copy available in the files of the Buffalo Law Review.

which under your observation or treatment, including the history obtained, x-ray and physical findings, diagnosis and prognosis."[188]

With this type of open-ended consent, the only realistic safeguard for the patient seems to be the third-party payer's good faith or possible lack of interest in irrelevant data.[189] For most people, foregoing coverage and personally absorbing the cost of a major episode of illness is simply not a plausible alternative. And it is not only the private insurers, but government agencies as well, that have sought protection or justification in the consent principle. As a Department of Health, Education and Welfare document puts it,

> Social Security Act beneficiaries, by analogy to a contractual waiver of the physician-patient privilege, have agreed to a waiver within the limited confines of the Social Security Act. Accordingly, Medicare, Medicaid, and Maternal and Child Health beneficiaries have permitted a waiver of the privilege for the purposes of peer, utilization, carrier, and PSRO review of their medical records, not to mention Social Security audits of those records.[190]

To be sure, there is nothing unreasonable in requiring a beneficiary of a public or private health care program to provide sufficient data to demonstrate that he is properly entitled to compensation. The problem is that the leverage resulting from the patient's economic dependency can easily be used to extract unduly broad authorizations which purport to immunize any collection, storage or disclosure practices that the third-party payer may decide to adopt. When the consent principle is used in

---

188. Copy available in the files of the Buffalo Law Review (emphasis added).

189. In some situations, notably work-related health insurance programs, there have been reports of widespread abuse. *See* M. Grossman, Factors Concerning Consent Form Authorizing Release of Medical Information for Insurance Reports (1974) (unpublished background paper for the Conference on Confidentiality of Health Records; copy available in the files of the Buffalo Law Review). This paper states:

> Numerous . . . patients, not being told of their official diagnosis for one reason or another, get word of it through outside channels. In most cases, it is from fellow employees who receive the information from personnel office employees, after the insurance company sent the information back to the employer. In other cases, the employees themselves have been told by the employers . . . . In some cases, they received information about this when credit bureau investigators began asking neighbors what they know about the patient-claimant's treatment or hospitalization. In one case, the insurance company assigned the consent form to a credit bureau to act as their agent in reviewing a physician's records.

Id. at 1.

190. Office of Professional Standards Review of U.S. Department of Health, Education and Welfare, PSRO's and Medical Information—Safeguards to Privacy 2 (undated).

this fashion, it becomes little more than a device "to place responsibility for invasions of privacy on the victim."[191]

C. *Public Law and Medical Privacy*

The obvious artificiality of applying consent principles based on an implicit model of arm's-length bargaining between relatively equal parties to relationships between welfare recipients and the massive HEW bureaucracy suggests that public law approaches may be more appropriate for many privacy issues. Unfortunately, the general trend of relevant legal doctrine seems to have been legitimation of government's growing appetite for personal medical records, with fairly minimal safeguards or opportunities for public participation in relevant agency decisions. Only recently have there been serious efforts to re-examine and improve the laws affecting government information practices.

As direct government involvement in health care and disease prevention grew, the developing public law absorbed the private law notion that doctors should be protected in divulging confidential medical information to those directly concerned, such as individuals who were exposed to contagious diseases.[192] Early statutes, following this rationale, carved out exceptions to the doctor-patient privilege by requiring physicians to report to public health authorities simple matters such as communicable diseases or vital statistics relating to births and deaths.[193] Gradually reporting requirements were expanded to require reporting of a great variety of medical conditions that are of interest to public health authorities, such as cancer,[194] blindness,[195] gunshot or knife wounds,[196] injuries inflicted with a deadly weapon,[197] suspected cases of child abuse,[198] prescriptions of drugs and narcotics,[199] disorders that may

191. Miller, *supra* note 173, at 1172; *cf.* Tunkl v. Regents of the Univ. of Cal., 60 Cal. 2d 92, 303 P.2d 441, 32 Cal. Rptr. 33 (1963) (en banc).

192. *See* text accompanying notes 167-68 *supra.*

193. *See* J. WALTZ & F. INBAU at 312.

194. *E.g.,* N.Y. PUB. HEALTH LAW § 2401 (McKinney 1971); E. SPRINGER, *supra* note 157, at 52.

195. N.Y. UNCONSOL. LAWS § 8704 (McKinney 1974).

196. *E.g.,* N.Y. PENAL LAW § 265.25 (McKinney 1971).

197. CAL. PENAL CODE § 11161 (West 1970).

198. *See generally* Paulsen, *Child Abuse Reporting Laws: The Shape of the Legislation,* 67 COLUM. L. REV. 1 (1967). Child abuse reporting laws frequently extend beyond physicians and health care professionals to include people with little or no medical training such as teachers or school administrators, welfare or social workers, or even "any person." *See id.* at 7. Obviously, the high risk of inaccuracy and stigma associated with such reports would make them extremely dangerous to data subjects if improperly released.

199. *See* J. WALTZ & F. INBAU at 312.

cause lapses of consciousness resulting in hazard to other motorists,[200] hearing impairments in children,[201] and job-related injuries.[202] In addition to these provisions for government collection of medical records from private-sector health care providers,[203] government is increasingly involved in creating medical records directly. Welfare programs and public clinics or hospitals are the most obvious government functions that may generate medical data, but they do not complete the list: mandatory screening programs, exemplified by the New York statute which empowers public health officials to compel persons suspected of having venereal disease to undergo a physical examination,[204] or the genetic screening programs which seek to identify children who have hereditary diseases like sickle-cell anemia,[205] are increasingly common. Once identifiable medical records have passed into government hands, whether state or federal, the privacy of data subjects has usually depended upon a maze of ad hoc statutes and administrative regulations which seem to be consistent only with respect to the broad discretion that they give the recordkeepers to decide who will have access, and on what terms.[206]

---

200. CAL. HEALTH & SAFETY CODE § 410 (West 1970).

201. *See* J. WALTZ & F. INBAU at 319.

202. CAL. LABOR CODE § 6407 (West 1971).

203. In addition to narrowly-drawn reporting requirements, there may be broad grants of information-gathering authority to public health officials which would theoretically enable them to collect private medical records in bulk. *See, e.g.,* Curran, Stearns & Kaplan, *Privacy, Confidentiality and Other Legal Considerations in the Establishment of a Centralized Health-Data System,* 281 NEW ENGLAND J. MED. 241 (1969), where a state statute governing disclosure of hospital records is characterized as "a classic example of obscure, overly complex legal drafting destroying all clarity in the law." *Id.* at 242-43:

> The provision can be read to give to the courts and to the department head (presumably, the Commissioner of Public Health) an unlimited power to "order" inspection of hospital patient records. We cannot find evidence of the use of this power by Commissioners of Public Health, present or past. . . . If the provision is read liberally, however, it would allow the Commissioner to order inspection of otherwise confidential patient records by anyone he designates and for any purpose he deems proper. For example, under such an interpretation, the Commissioner could possibly order every hospital in the state to allow inspection of its patient records and to allow copies to be made of them. These copies might then be entered into a central health-data system. to allow inspection of its patient records and to allow copies to be made of them. There is nothing in the statute that would provide for confidentiality of the data once released.

204. N.Y. PUB. HEALTH LAW § 2300 (McKinney 1971).

205. *See generally* Waltz & Thigpen, *Genetic Screening and Counseling: The Legal and Ethical Issues,* 68 NW. U. L. REV. 696, 703-05 (1973).

206. *E.g.,* Meldman, *Centralized Information Systems and the Legal Right to Privacy,* 52 MARQ. L. REV. 335 (1969). In his article Meldman indicates the following:

> Almost all states have statutory provisions for the accessibility of official records. These provisions are usually scattered throughout the statutes, . . . As each governmental department or agency is created, provisions for the neces-

One possible means of rationalizing and controlling government policies for handling sensitive personal information is development of constitutional doctrines imposing minimum standards on government information practices. However, the evolution of constitutional principles dealing with collection and dissemination of medical records or similar personal data has been slow and cautious. Supreme Court decisions recognizing a constitutional privacy right to be free from government interference in the areas of birth control[207] and abortion[208] raised the possibility that a general right to privacy for matters relating to medical treatment might emerge,[209] and restrict government power to gather medical records. As yet this possibility remains largely unrealized, as illustrated by two subsequent lower court cases in which attempts to extract medical information were challenged on constitutional grounds.

In the first case, *Merriken v. Cressman*,[210] the challengers succeeded

---

sary record-gathering or bookkeeping are generally enacted at the same time. The laws pertaining to access of these records therefore widely vary among the different sets of records kept within a state. Most official records are established as "public," which usually means that anyone may have access to them, but certain more sensitive information, such as tax or health records, is defined as "confidential." Various levels of confidentiality exist. Some information may be available to any governmental body or to certain governmental bodies upon a showing of a good reason for obtaining the information, or it may be unavailable to anyone outside the original record-gathering body. Quite often, however, the accessibility of records is unclear in the statutory provisions, and questions of accessibility are left up to the discretion of the keeper of the records.

Id. at 343. The 1973 survey of federal statutes and regulations discussed in A. Bell, *supra* note 156, reached similar conclusions. As might be imagined, problems can arise in cooperative federal-state welfare programs when the rules of the two jurisdictions treat the same information differently. *See, e.g.*, The Washington Post, July 11, 1975, at A7, col. 1 (U.S. Department of Health, Education and Welfare regulations requiring states to keep confidential records identifying parents who have deserted their families in conflict with state statutes making the records public documents).

207. Griswold v. Connecticut, 381 U.S. 479 (1965).

208. Roe v. Wade, 410 U.S. 113 (1973); Doe v. Bolton, 410 U.S. 179 (1973).

209. Perhaps the strongest statement in the Supreme Court opinions were the comments in Justice Douglas' concurrence in *Doe v. Bolton*, relating to a state requirement that a prospective abortion patient had to be examined by doctors other than her personal physician:

> The right of privacy has no more conspicuous place than in the physician-patient relationship, unless it be in the priest-penitent relationship.
>
> It is one thing for a patient to agree that her physician may consult with another physician about her case. It is quite a different matter for the State compulsorily to impose on that physician-patient relationship another layer or, as in this case, still a third layer of physicians. The right of privacy—the right to care for one's health and person and to seek out a physician of one's own choice protected by the Fourteenth Amendment—becomes only a matter of theory, not a reality, when a multiple-physician-approval system is mandated by the State.

410 U.S. at 219.

210. 364 F. Supp. 913 (E.D. Pa. 1973).

in blocking a school program which used psychological testing to identify eighth grade students who were "potential drug abusers," and compulsory counseling to modify the behavior of those who were placed in the high-risk group. As described by the court, the program seemed almost designed to trample the privacy interests of the students: the scientific validity of the theories on which the program was based was questionable;[211] the qualifications of the people running the program were dubious;[212] the procedures used to obtain parental consent were coercive and misleading;[213] and the program designers were admittedly compiling a "massive data bank" that would be generally accessible throughout the school bureaucracy.[214] Although the program was held unconstitutional, the grounds relied on by the court are sufficiently narrow that the decision probably would not be a substantial restraint on planners contemplating similar programs, much less programs which involve different kinds of medical information. Instead of focusing on the medical nature of the intimate data being extracted from the students, the court emphasized that the items on the questionnaire probing family relationships violated a constitutionally protected family privacy interest.[215] Thus, the decision may not be applicable to government data-gathering activities that do not directly affect a family interest.[216] Moreover, the court found that this interest was threatened primarily because the parental consent was invalid—and in the process suggested that the conventional consent-to-medical-treatment standards were constitutionally sufficient.[217] Thus, slightly

211. *See id.* at 915-16.

212. *Id.* at 915.

213. In addition to a general overemphasis on benefits and failure to mention risks, the disclosures made to parents offered assurances of confidentiality when in fact there was "absolutely no assurance that the materials which have been gathered would be free from access by outside authorities in the community who have subpoena power." *Id.* at 916. Coercion arose from a "negative option" scheme in which parents who did not want their children to participate had to take affirmative action to release them from the testing. *Id.* at 914. It arose as well from stigmatizing of the student plaintiff "in which fellow students accused him of being a drug user because his mother does not want him to participate . . . ." *Id.* at 915.

214. *Id.* at 916. Identified data was to be disseminated to "various school personnel, including superintendents, principals, guidance counselors, athletic coaches, social workers, PTA officers, and school board members." *Id.*

215. *Id.* at 918.

216. *See* Recent Case, *Constitutional Law—Right of Privacy—Personality Test Used by a School to Identify Potential Drug Users Without Informed Consent of Parents Violates Student's and Parents' Right of Privacy*, 27 VAND. L. REV. 372, 379 (1974).

217. 364 F. Supp. at 920. The court endorsed use of the consent-to-treatment approach despite its earlier observation that "[t]he Supreme Court has indicated that in civil cases as well as criminal cases the Court should indulge in every reasonable pre-

better consent procedures, or statutory authority to extract data by compulsory process, might protect a program from constitutional challenge.

The willingness of many courts to defer to legislative or administrative justifications for collecting personal information is illustrated by the second recent privacy case, *Schulman v. New York City Health & Hosp. Corp.*[218] There, doctors and patients failed in an attempt to strike down a city ordinance which required that abortion patients' names and addresses be reported on a "termination of pregnancy" certificate which was put into a central filing registry. After first concluding that a challenge based on violation of the doctor-patient privilege was insubstantial because the privilege was already riddled with exceptions for hospital, welfare, insurance, and public health purposes,[219] the court held that the constitutional privacy claim must fail because there was a "compelling state interest" in requiring the identity of the abortion patients. Among the rationales that the court found "compelling" were the government's desire "to provide statistical information, presently unavailable, as to the effect of multiple abortions on the same woman and any other adverse effects that may occur due to abortion," and the government's purpose "to offer public health counseling on adequate preventive family planning measures as an alternative measure to repeated abortions as a means of birth control."[220]

If statistical or advisory functions like these can be considered a "compelling state interest" sufficient to overbalance the patients' privacy rights,[221] then the constitutional check on government collection of medical records seems minimal indeed. While the Supreme Court's recent decisions have not been as closely on point for medical records collection programs as these lower court cases, the opinions in the 1974

---

sumption against waiver of procedural due process and an individual's Constitutional rights." *Id.* at 919.

218. 44 App. Div. 2d 482, 355 N.Y.S.2d 781 (1st Dep't 1974).

219. *Id.* at 483-85, 355 N.Y.S.2d at 783-84. The court also emphasized that the New York City Health Code contained confidentiality provisions which limited disclosure of the data. *Id.*

220. *Id.* at 485, 355 N.Y.S.2d at 784. Other "persuasive reasons" mentioned by the court were:

> to allow follow-up where complications or coma ensues; to enable public health authorities to determine whether improper or unorthodox procedures were used in an out-patient facility and whether further investigation or regulation is required; . . . and to insure that women who test positive for an Rh negative factor, venereal disease, sickle cell anemia and other factors which may affect the health of future children receive proper counseling and treatment.

221. It is possible to argue that, even under the *Schulman* decision, these government interests standing alone would not be considered compelling. The relevant portion of the opinion pulls together a variety of justifications advanced by the government. *See* note 220 *supra.* It also makes no attempt to indicate what the relative weight of each of these interests might be.

California Bankers case,[222] involving government access to private financial records, suggest that some members of the present court are quite willing to avoid these kinds of constitutional issues, and defer to the judgments of other branches of government regarding data-collection needs, at least when a plausible law-enforcement justification can be made.

Constitutional controls on the use of personal data after it has been collected seem to be even more rudimentary. Apart from a few cases in the District of Columbia Circuit dealing with criminal justice records,[223] courts have been extremely reluctant to find that agency practices for handling personal data created a cognizable injury to constitutional rights,[224] unless the personal information was used to support an agency determination about entitlement to benefits or liability to sanctions.[225] While it is possible that due process principles could be extended on a case-by-case basis to deal with a great variety of government information-handling practices, experience in a related area—development of constitutional doctrines to protect free speech interests that might be

---

222. California Bankers' Ass'n v. Schultz, 416 U.S. 21 (1974). The substance of the decision is summarized as follows in Miller, *supra* note 4, at 72, 81:

> [Justice Rehnquist, author of the plurality opinion] concluded that the recordkeeping requirements did not create an unreasonable burden on the banks so as to violate due process; that the obligation to maintain the records, as opposed to a requirement to turn them over to the government, was not an invasion of the prohibition against unreasonable searches and seizures; that the banks, having no privilege against self-incrimination, could not raise that objection; that the assertion the recordkeeping might be used by governmental investigators to identify members of organizations in violation of the First Amendment right of freedom of association was premature; that the Fourth Amendment challenges to the reporting requirements failed because the statutory purposes were reasonable and the depositor plaintiffs lacked standing to challenge the domestic reporting regulations; that the banks could not challenge the reporting requirements on the ground of self-incrimination and that the depositor plaintiffs' similar attack on the reporting requirements was premature; and, finally, that the ACLU's claim that its associational freedom under the First Amendment was violated was premature. . . .
>
> Mr. Justice Powell and Mr. Justice Blackmun interposed a short concurring opinion suggesting that they might not have joined in the result if the Treasury Department's regulations had applied to all banking transactions.

223. *See* Chastain v. Saxbe, 510 F.2d 1232 (D.C. Cir. 1975); Tarlton v. Saxbe, 507 F.2d 1116 (D.C. Cir. 1974); Menard v. Saxbe, 498 F.2d 1017 (D.C. Cir. 1974). Even in these cases, the courts' analysis has dealt primarily with the agencies' statutory authority to keep and disseminate the records, with constitutional discussions largely consigned to dictum.

224. *E.g.*, Laird v. Tatum, 408 U.S. 1 (1972); Finley v. Hampton, 473 F.2d 180 (D.C. Cir. 1972).

225. *See generally* Finley v. Hampton, 473 F.2d 180, 185 (D.C. Cir. 1972); Freedman, *Summary Action by Administrative Agencies*, 40 U. CHI. L. REV. 1 (1972); Gellhorn, *Adverse Publicity by Administrative Agencies*, 86 HARV. L. REV. 1380 (1973).

compromised by privacy protections—indicates how slow and uncertain the process of constitutional litigation can be.[226]

As these shortcomings in traditional privacy law have become apparent, the focus of reform efforts has shifted toward development of legislation which could quickly and comprehensively prescribe standards to protect individuals' informational privacy.[227] A few statutes have been enacted at the state[228] or local[229] level, and interest groups have been organized to develop and promote uniform state laws in specialized areas like medical records.[230] However, by far the greatest concentration of legislative activity on behalf of personal privacy has taken place at the federal level.[231] In the closing days of the Ninety-Third Congress, this activity culminated in passage of the Privacy Act of 1974,[232] a statute that seems sure to become the new model for legal protection of informational privacy.

III. The New Legal Controls: The Privacy Act of 1974

As might be expected in Congress' first attempt to deal with informational privacy problems generically,[233] the Privacy Act reflects a

226. *See* notes 155, 159 *supra* & accompanying text. As the cases there cited indicate, the question of what first amendment standards should be applied to privacy actions brought by individuals who are not "public figures" has remained in doubt for nearly ten years.

227. *See generally* Kane, Book Review, 24 Buffalo L. Rev. 331, 340-43 (1975); Miller, *supra* note 174, at 1114-19; Westin & Baker at 15-17.

228. *See, e.g.,* Minnesota Stat. 1974, H.F. 1316, Computer Law Service App. 5-2b.

229. *See, e.g.,* Berkeley, Cal. Ordinance 4732-NS, Oct. 29, 1974 (copy available in the files of the Buffalo Law Review) requiring a "social impact statement" before funds are expended to change any automated city personal data system.

230. *See, e.g.,* Barton, *Should a National Commission for the Preservation of Confidentiality of Health Records Be Formed?,* 12 Psychiatric Opinion 15 (January, 1975); Council of State Governments News Release, Dec. 26, 1975 (state and local government officials cooperating in development of state privacy legislation).

231. The Library of Congress Congressional Research Service reports that "upwards of 200 bills pertaining to privacy" were introduced in the Ninety-Third Congress. L. Becker, Privacy; Information Technology Implications 3, March 21, 1975 (mimeograph, Issue Brief No. IB 74105).

232. 88 Stat. 1897 (1974) [hereinafter cited as Privacy Act]. Privacy Act § 3, *amends* 5 U.S.C.A. § 552 (Supp. I, 1975) by adding to it § 552a (Supp I, 1975) [hereinafter cited as 5 U.S.C.A. § 552a]. The haste with which the legislation was enacted is reflected in the fact that the bills passed by the House and Senate did not even go to a conference committee; instead, committee staff members in the two houses worked out a compromise, and it was adopted through floor action. *See generally* 120 Cong. Rec. 12,243 (daily ed. Dec. 18, 1974) (remarks of Rep. Morehead). In place of a conference committee report, there is a staff "Analysis of House and Senate Compromise Amendments to the Federal Privacy Act." *Id.* at 12,243-246 [hereinafter cited as Staff Analysis].

233. The major legislative precursor to the Privacy Act, the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-81(t) (1970), differs in this respect by virtue of its limitation

relatively cautious approach to the kinds of information systems that are covered, and the control mechanisms that are employed. In contrast to some of the privacy bills considered by Congress, the Act does not deal directly with data systems operated by private organizations or state and local governments. Instead, it applies only to information systems[234] which are either operated by federal agencies, or used by government contractors performing an "agency function,"[235] a rather fuzzy jurisdictional boundary which has been interpreted to include nonfederal intermediaries and carriers in programs like Medicare.[236] Moreover, the Act rejected proposals for "strong" regulatory controls such as a requirement that computer systems handling personal records

to data that affects credit-granting decisions. Similarly, the "Buckley Amendments," Pub. L. No. 93-380, § 315 (1974), dealt only with the privacy of student records; even so, problems in implementing these provisions resulted in early amendment. *See* Pub. L. No. 93-568, § 2 (1974).

234. The Act applies to both manual and machine record systems. A "record" for purposes of the Act is defined to include "any *item,* collection, or grouping of information about an indivilual . . . including, but not limited to, his education, financial transactions, *medical history,* and criminal or employment history and that contains" some identifying particular like the individual's name. 5 U.S.C.A. § 552a(a)(4) (emphasis added). Thus, identifiable records are distinguished from statistical records. *See id.* at § 552a(a)6. But the level at which many of the Act's provisions operate is the "system of records," defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some . . . identifying particular . . . ." 5 U.S.C.A. § 552a(a)(5). The Office of Management and Budget Guidelines for implementation of the Act, 40 Fed. Reg. 28949, 28952 (1975) [hereinafter cited as OMB Guidelines] emphasize two limitations implicit in this definition: (1) it is not sufficient that the agency merely have the capability of accessing records by the individual's name or identifier, but rather it must actually access the records in this manner; and (2) the record system must be official records of the agency rather than personal records of agency employees such as personal telephone lists or "[u]ncirculated personal notes, papers and records which are retained or discarded at the author's discretion." *Id.* The OMB Guidelines take the position that agencies have broad discretion in determining what groupings of records constitute separate "systems" for purposes of the Act. *See id.* at 28962-63. Whether these interpretations develop into serious "loopholes" in the Act's coverage remains to be seen; however, it does seem that they are broadly consistent with the Privacy Act's general philosophy of trying to remedy large scale, serious threats to privacy rather than dealing exhaustively with every possible abuse of personal information.

235. 5 U.S.C.A. § 552a(m) provides in part: "When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system."

236. HEW concluded that "intermediaries and carriers are agents of the Department (as well as contractors) in carrying out Medicare functions." 40 Fed. Reg. 47406 (1975). The OMB Guidelines generally interpret the "contractor provision" to restrict its coverage. *See, e.g.,* OMB Guidelines which read:

> The qualifying phrase "to accomplish an agency function" limits the applicability of subsection (m) to these systems directly related to the performance of Federal agency functions by excluding from its coverage systems which are financed, in whole-or in part, with Federal funds but which are managed by state or local governments for the benefit of state or local governments.

40 Fed. Reg. at 28951. *See also id.* at 28975-76.

be licensed by an administrative agency[237] or even creation of the "non-regulatory commission" with investigative powers that was included in the Senate-passed version of the Privacy Act.[238] Instead, the Congress chose to rely on public disclosure and rulemaking by existing agencies, supplemented with private judicial and administrative remedies to cure specific abuses. A temporary Study Commission was also provided to evaluate the functioning of the Act, and report back to Congress.[239] Thus, in significant ways the Privacy Act is a modest, tentative step toward evolution of a comprehensive system of legal safeguards for personal information; even so, however, it is unquestionably a sweeping innovation in prior law and practice.

Many provisions of the Privacy Act reflect approaches that were developed in the Fair Credit Reporting Act,[240] and then expanded and refined by the HEW Advisory Committee Report, Records Computers and the Rights of Citizens.[241] In accord with the HEW Report, the Act seeks to attain four basic types of objectives in regulating personal information systems: public accountability of system operators, limits on who can obtain access to identifiable records, accuracy of the data, and

---

237. *See generally* HEW REPORT, *supra* note 5, at 170-71; H.R. 9786, 93d Cong., 1st Sess. (1973); H.R. 10610, 93d Cong., 1st Sess. (1973). Variations on the licensing theme include proposals for occupational licensing of personnel who are engaged in handling personal data (*Cf.* H.R. 2620, 93d Cong., 1st Sess. (1973)), which proposed licensing of consumer credit investigators by a federal agency. Also proposed were bills that would create an agency empowered to issue rules defining "fair information practices" and then adjudicate complaints of violations. *See, e.g.*, H.R. 12207, 93d Cong., 2d Sess. (1974); H.R. 12880, 93d Cong., 2d Sess. (1974); H.R. 13304, 93d Cong., 2d Sess. (1974); S. REP. No. 1183, 93d Cong., 2d Sess. 25 (1974).

238. *See generally* 120 CONG. REC. 19,835 (daily ed. Nov. 21, 1974) (remarks of Senator Ervin); *id.* at 19,858-62. The investigative commission approach seems functionally similar to an ombudsman model, which was rejected by the HEW REPORT at 42:

> [The] ombudsman concept is basically remedial and will, therefore, work best in the context of established rights and procedures. Furthermore, the function is not well understood or widely accepted in America, and some observers feel that it has severe limitations in the context of American legal, political and administrative traditions.

239. The Privacy Protection Study Commission established by section 5 of the Privacy Act is a tripartite advisory committee consisting of seven members, three appointed by the President and two each by the Speaker of the House and the President of the Senate. *Id.* § 5(a)(1). Among the topics that the Commission is authorized to investigate are medical and insurance activities involving personal information. *Id.* § 5(c)(2)(A). The Commission is required to make its final report and recommendations to Congress and the President within two years of the date on which all Commissioners have been appointed. *Id.* § 5(g). This is true even though this amount of time may be an unreasonably short time in which to assess operational experience under the Act.

240. *See* note 233 *supra.*

241. HEW REPORT.

fairness to individuals who may be adversely affected when decisions are based on identifiable records.[242]

The Act's basic tool to assure public accountability and prevent the growth of secret data systems is Federal Register publication of notices describing the general characteristics of covered data systems.[243] These general notices must be published annually,[244] and if the agency proposes a "new use" of data— presumably one not described in a prior notice—it must publish the proposal and give interested persons an opportunity to comment at least 30 days before the regular annual notice.[245] Similarly, establishment of a new personal information system, or alteration of an existing system, must be preceded by "adequate advance notice" to Congress and the Office of Management and Budget.[246] Paralleling these public notice provisions is a directive to the agencies to promulgate detailed rules under the Administrative Procedure Act's notice-and-comment rulemaking procedure implementing the public

242. The articulation of these goals in the HEW REPORT at xx-xxi was somewhat more elaborate:

> 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 about him that was 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 precautions to prevent misuse of the data.

243. 5 U.S.C.A. § 552a(e)(4). Among the matters required to be contained in the published notice are the categories of records in the system, the categories of individuals on whom records are maintained, the routine uses of the records, and the procedures for obtaining access. *Id.* The Office of Federal Register is required to publish an annual directory of agency data systems and rules relating to storage of personal data "in a form available to the public at low cost." *Id.* § 552a(f); *cf.* HEW REPORT at xxx-xxxi.

244. 5 U.S.C.A. § 552a(e)(4).

245. *Id.* § 552a(e)(11). The OMB Guidelines summarize the effect of the Act's provisions requiring public notice of system changes as follows:

> Generally, any change in a system which has the effect of expanding the categories of records maintained, the categories of individuals on whom records are maintained, or the potential recipients of the information, will require the publication of a revised public notice before the change is put into effect. In addition, any modification that alters the procedures by which individuals exercise their rights under the Act (e.g. for gaining access) will require the publication of a revised notice before that change becomes effective.

40 Fed. Reg. at 28963.

246. 5 U.S.C.A. § 552a(o). This section provides that the purpose of the advance submission is "to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers." *Id.*

access rights conferred by the Act.[247] Finally, notice to individual data subjects is required at the time when the agency attempts to collect personal information. The notice must specify the source of the agency's authority to collect the information, the uses that will be made of it, and the consequences to the data subject if he refuses to supply the requested data.[248]

The extent to which this notice-and-opportunity-to-object approach will be effective in curbing or eliminating improper agency practices may be largely dependent on the participation of well organized interest groups who are able to provide timely criticism and suggest reasonable alternatives.[249] In the field of medical records, the major candidates to fill this role are consumer and provider groups—welfare rights organizations, public interest groups involved in health care issues, veterans' organizations, medical societies concerned about government intrusions on the doctor-patient relationship, or professional associations of medical record librarians and other administrative personnel. For all of these kinds of organizations, it may be difficult to mobilize either expertise about information systems and technology, or constituency support and financial resources sufficient to maintain effective participation. It is, of course, possible that organizational priorities will shift, or new activist groups will emerge to represent the interest of medical privacy; however, it seems more likely that most of the effective public input will come from data users rather than data subjects.

Public disclosure and accountability goals are also implicit in the portions of the Privacy Act dealing with access to personal records stored in covered systems. While the statutory provisions are complex and subject to exceptions,[250] the underlying philosophy is straightfor-

247. *Id.* § 552a(f).

248. *Id.* § 552a(e)(3).

249. *Cf.* Cramton, *The Why, Where and How of Broadened Public Participation in the Administrative Process*, 60 GEO. L.J. 525, 529 (1972), which states:

> [Our] governmental institutions are highly responsive. But responsive to what? . . . They are responsive to the inputs they receive, including the feedback that greets their actions.
>
> The cardinal fact that underlies the demand for broadened public participation is that governmental agencies rarely respond to interests that are not represented in their proceedings. And they are exposed, with rare and somewhat insignificant exceptions, only to the view of those who have a sufficient economic stake in a proceeding or succession of proceedings to warrant the substantial expense of hiring lawyers and expert witnesses to make a case for them.

250. 5 U.S.C.A. §§ 552a(j), (k) establish "general" and "specific" exemptions to certain provisions of the Act. Since the kinds of records covered by these exemptions—*e.g.*, criminal justice information and Central Intelligence Agency files—will not typically contain large quantities of medical information, they are not discussed in detail here. *See generally* OMB Guidelines at 28971-74.

ward: identifiable records can be used or disclosed either pursuant to general rules publicly established, or with the specific consent of the data subject. The Act itself provides some general standards defining proper disclosures. Personal information can be released without obtaining the data subject's consent to personnel of the agency maintaining the records who need to use the records in performing their official duties,[251] to members of the public seeking records that must be disclosed under the Freedom of Information Act,[252] to Congress or the Comptroller General,[253] to statistical users and the National Archives,[254] to a government instrumentality for civil or criminal law enforcement purposes,[255] and to any person if the disclosure is pursuant to court order[256] or is based upon a showing of "compelling circumstances affecting the health or safety of an individual."[257] In addition to these

251. 5 U.S.C.A. § 552a(b)(1). The OMB Guidelines at 28954 interpret the legislative history as reflecting Congress' intention that there be constraints on the use of records within the agency:

> Minimally, the recipient officer or employee must have an official "need to know." The language would also seem to imply that the use should be generally related to the purpose for which the record is maintained.

Id.

252. 5 U.S.C.A. § 552a(b)(2). Exemption (6) of the Freedom of Information Act, 5 U.S.C. § 552(b)(6)(1970), authorizes agencies to withhold from the public "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." The 1974 amendments to the Freedom of Information Act, Pub. L. No. 93-502, also added a privacy provision to exemption (7): agencies may now refuse to disclose investigatory files only to the extent that disclosure would, *inter alia*, "constitute an unwarranted invasion of personal privacy." The OMB Guidelines at 28954 interpret the Privacy Act exception as applying only to disclosures that are mandatory under the Freedom of Information Act; discretionary disclosures, without the data subject's consent, would be prohibited unless this type of disclosure had been published as a "routine use." *See text* accompanying notes 258-61 *infra*.

253. 5 U.S.C.A. § 552a(b)(9)-(10).

254. *Id.* §§ 552a(b)(4) (Bureau of the Census); § 552a(b)(6) (National Archives); § 552a(b)(5) ("to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable").

255. *Id.* § 552a(b)(7). Disclosure under this section can be made only if the law enforcement activity "is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the records specifying the particular portion desired and the law enforcement activity for which the record is sought." If the law enforcement agency had not requested the records in question, the record-keeping agency still might disclose them as a routine use. OMB Guidelines at 28955.

256. 5 U.S.C.A. § 552a(b)(11). Section 552a(e)(8) of the Act requires agencies to "make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record."

257. *Id.* § 552a(b)(8). The OMB Guidelines at 28955 note that "[t]he individual pertaining to whom the record are disclosed [*sic*] need not necessarily be the individual whose health or safety is at peril; *e.g.*, release of dental records on several individuals in order to identify an individual who was injured in an accident."

statutorily-approved disclosures, the agency maintaining the system can provide further exceptions to the consent requirement after appropriate public notice[258] under the "routine use" standard. A "routine use" is one which is "compatible with the purpose for which [the record] was collected."[259] Apparently this would include uses beyond the "explicit and expressed purposes for which [the data] was collected,"[260] including some which lie outside the jurisdiction of the collecting agency or have only tangential relevance to the disclosing agency's statutory mandate. The example given during floor debate by Senator Ervin, a principal sponsor of the bill, demonstrates that "compatibility" can be quite broadly defined to legitimize a great variety of current data-sharing relationships:

> [T]he [Internal Revenue Service] sends to State, and local, tax agencies the Federal tax returns of individuals who live in the State so the State agency can check to see if the individual has reported the same income and deductions on his Federal and State, or local, tax returns. . . . [T]he States rely on this information in enforcing their own tax laws. Also, this information may be sent to a State before it conducts a tax investigation on its own.
>
> Under the bill, it is intended that this would be a routine use for a purpose compatible with the purpose for which the information is collected so the IRS can continue to send tax information to State and local tax agencies in this way.[261]

Under this rationale, it seems clear that most of the arrangements between the Social Security Administration and the states to share medical records would meet the "compatibility" criterion, and could be continued unchanged under the Privacy Act if proper notice was given.

Obviously, these basic access limitations are not very onerous standards to meet. The vagueness of some of the operative terms like "civil or criminal law enforcement activity,"[262] the possibility that data subject

---

258. 5 U.S.C.A. §§ 552a(b)(3), (e)(4)(D).

259. *Id.* § 552a(a)(7). *See also id.* § 552a(b)(3).

260. OMB Guidelines at 28953.

> The term "routine use" was introduced to recognize the practical limitations of restricting use of information to explicit and expressed purposes for which it was collected. It recognizes that there are appropriate and corollary purposes . . . that are appropriate and necessary for the efficient conduct of government and in the best interest of the individual and the public.

Id.

261. 120 CONG. REC. 21815 (daily ed. Dec. 17, 1974).

262. 5 U.S.C.A. § 552a(b)(7). Neither the legislative history nor the OMB Guidelines seems to provide much guidance as to what actions, taken by an agency within its powers, would *not* be a "civil or criminal law enforcement activity."

consent may be abused even if none of the exceptions is invoked,[263] and the broad discretion that agencies seem to have in defining "routine uses," all suggest that the access controls may function simply as a mechanism to compel agencies to devote some systematic thought to their disclosure policies, rather than as a set of firm, definite limitations on the sharing of personal records.[264] Similar vagueness of statutory language and implementing regulations may dilute the effectiveness of two other Privacy Act provisions designed to protect against unauthorized or improper disclosure: the requirements that agencies "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records" in order to protect data subjects from harm or embarassment,[265] and the directive that agencies establish rules of conduct for information-handlers.[266] Undoubtedly the need to take account of unique data system features or particular agency programs, as well as the generally undeveloped state of knowledge in the fields of technical security and administrative controls,[267] were the

263. *See* text accompanying notes 173-91 *supra*. The OMB Guidelines at 28954 show some awareness of the coerced consent problem:

> [C]are must be exercised to assure that the language of the request [for consent] is not coercive and that any consequences of refusing to consent are made clear. . . .
>
> The consent provision of this subsection was not intended to permit a blanket or openended consent clause: *i.e.*, one which would permit an agency to disclose a record without limit. At a minimum, the consent clause should state the general purposes for, or types of recipients, to which disclosure may be made.

264. This limited purpose of the Act is explicitly endorsed in the congressional Staff Analysis adopted in lieu of a Conference Committee Report. *See* note 232 *supra*. Part of the Analysis reads:

> The compromise definition should serve as a caution to agencies to think out in advance what uses it [*sic*] will make of information. This act is not intended to impose undue burdens on the transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or intraagency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to other persons or agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.

Id. at 12244.

265. 5 U.S.C.A. § 552a(e)(10). *See also* OMB Guidelines at 28966.

266. 5 U.S.C.A. § 552a(e)(9). In addition to promulgating the rules, the agency is required to "instruct each such person [involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record] with respect to such rules and the requirements of this section." *Id. See also* OMB Guidelines at 28965-66.

267. The OMB Guidelines at 28966 on the technical security requirements emphasize these kinds of problems:

> The development of appropriate administrative, technical, and physical safeguards will, necessarily, have to be tailored to the requirements of each system of records and other related requirements for security and confidentiality.

principal reasons why more detailed standards have not been written. But it is also clear that the lack of articulated general principles in these areas means that development of effective privacy protection criteria and techniques will depend primarily upon the discretion and good faith of the data collecting agencies, and to a lesser extent on the willingness of the courts to give enforceable content to the vague statutory standards in any civil action that may be brought.[268]

Another major device which the Privacy Act uses to control dissemination of personal records, the "accounting of certain disclosures"[269] or "access log," should be more easily enforceable.[270] The purpose of the accounting is to provide a record of all significant disclosures[271] affecting each data subject's file, and to make this record available to the data subject so that he can discover who has been using his personal data and for what purposes.[272] Since the "routine use" and other disclosure provisions of the Act previously discussed make it relatively easy for agencies to legitimize data sharing arrangements, the accounting device probably will not uncover a great number of unauthorized dis-

---

The need to assure the integrity of and to prevent unauthorized access to, systems of records will be determined not only by the requirements of this Act but also by other factors like the requirement for continuity of agency operations, the need to protect proprietary data, applicable access restrictions to protect the national security, and the need for accuracy and reliability of agency information.

While the technology of system security (both for computer-based and other systems of records) is well developed as it relates to materials classified for reasons of national defense or foreign policy, few standards currently exist to guide a "civil" agency in this area.

See also text accompanying notes 299-308 *infra.*

268. *See* text accompanying note 264 *supra.*

269. 5 U.S.C.A. § 552a(c).

270. Enforcement of the "accounting of disclosures" could, however, be completely frustrated if agency personnel were able to falsify or conceal portions of the accounting. *Cf.* Ralph Nader's charge that agencies have deliberately given deceptive responses, or concealed documents, in acting upon requests for records under the Freedom of Information Act. Nader, *Freedom From Information: The Act and the Agencies,* 5 HARV. CIV. RIGHTS—CIV. LIB. L. REV. 1, 10-13 (1970). The Privacy Act's criminal penalties provisions, 5 U.S.C.A. § 552a(i), apparently would not prohibit willful alteration of the accounting of disclosures.

271. The accounting requirement does not apply to disclosures required by the Freedom of Information Act, or to uses of the record by personnel of the agency maintaining the record system in the performance of their official duties. 5 U.S.C.A. § 552a(c)(1).

272. Although an accounting must include disclosures made to law enforcement agencies, this aspect of the accounting is not available to the data subject. 5 U.S.C.A. § 552a(c)(3). The accounting must include "the date, nature, and purpose of each disclosure of a record to any person or to another agency" and the name and address of the data recipient. *Id.* § 552a(c)(1)(A)-(B). It must also be retained "for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made." *Id.* § 552a(c)(2).

closures. Rather, its main utility in limiting access to personal records[273] may be as a notice device to support public participation in rulemaking by highlighting particular data disclosure practices that threaten groups or individuals who are potential participants.

In addition to the foregoing access controls that are addressed to potential transferor agencies, the Act also contains a limit on potential transferee agencies: they must "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs."[274] This requirement effectively reverses the prior practice of encouraging the agencies to share data bases when the exchange would reduce the burden on respondents,[275] and its effects obviously hinge on the content that will be given to the word "practicable." In an effort to structure agency discretion in this area, the Office of Management and Budget guidelines for implementation of the Privacy Act suggest several factors for an agency to consider in determining whether direct collection is practicable:[276] "the nature of the program"[277]; the risk that erroneous information would adversely affect the data subject; the relative costs of direct and third-party data collection; the need to assure the accuracy of information supplied by an individual by verifying it with a third party; and, conversely, the posssibility of verifying third-party information with the individual before using it to make particularized determinations of his liabilities or entitlement to benefits. Although they are an improvement over the open-ended statutory language, these criteria still leave the agencies considerable latitude to

273. The accounting of disclosures should be more effective in assuring accuracy and fairness under the provision of the Privacy Act which requires agencies that have corrected a disputed record to send copies of the correction to prior recipients of the record. *See* text accompanying notes 295-97 *infra.*

274. 5 U.S.C.A. § 552(a)(e)(2).

275. OMB Guidelines at 28961. *See also* A. MILLER, THE ASSAULT ON PRIVACY 141-45 (1971).

276. OMB Guidelines at 28961.

277. The example given in the OMB Guidelines is not very helpful in interpreting this criterion: "[I]t may well be that the kind of information needed can only be obtained from a third party such as investigations of possible criminal misconduct; . . ." *Id.* The impracticability of going to a criminal suspect is obvious, but it is not apparent whether there are other circumstances in which the "nature of the progarm" would argue in favor of gathering data from a third party. Perhaps what is meant is that agencies should consider whether the nature of the function they are performing would induce people to report erroneous information about themselves—either because they fear sanctions, or because they may become eligible for a benefit. If the principle is this broad, it would seem to argue in favor of third-party collection in most of the major federal programs involving use of personal information, and certainly in the major health care programs.

justify data-sharing. The relative cost consideration, without a strong presumption in favor of privacy that seems lacking in the guidelines, will frequently weigh heavily in favor of getting the records from a third party; and the Guideline's emphasis on accuracy considerations—the need to verify information by obtaining it from multiple sources—provides a convenient rationale for maintaning existing data-sharing relationships. In the medical records field, it will always be possible to argue that diagnostic or prognostic information is too poorly understood by patients to make direct collection from the data subject "practicable."

The Privacy Act's fairness and accuracy safeguards are contained in three sets of provisions which are designed to give the individual data subject some right to control the ways in which his personal records are used. The standards contained in the first set of provisions are designed to assure that the data subject will not be adversely affected by wrong or irrelevant or incomplete data.[278] Thus, the agency using identifiable records is directed to "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose . . . required to be accomplished by statute or executive order,"[279] and at the same time is instructed to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual in the determination."[280] At first impression these two provisions, read together, may seem to impose an impossibly high standard on the agencies: as the OMB Guidelines point out, the personal information must be not only relevant but *necessary* as well,[281] which means that personal data used in informal agency action may be subject to more stringent tests of "admissibility" than similar evidence introduced in trial-type hearings.[282] Nevertheless, concepts like "timeliness," "completeness" and

278. In addition to the provisions discussed in the text, 5 U.S.C.A. § 552a(e)(6) directs the data-collecting agency "prior to disseminating any record about an individual to any person other than an agency . . . [unless the dissemination is required by the Freedom of Information Act, to] make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes; . . ." *See also id.* at § 552a(e)(7) (agencies prohibited from maintaining records about exercise of first amendment rights "unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity").

279. 5 U.S.C.A. § 552a(e)(1).

280. *Id.* § 552a(e)(5).

281. OMB Guidelines at 28960.

282. *Id.* at 28961:

> It should be noted that subsection (e) [of the Privacy Act] is not intended to interfere with the presentation of evidence by the parties before a quasi-

"necessity" can be interpreted as conferring a reasonable amount of agency discretion,[283] and, more importantly, they seem susceptible to more detailed elaboration of standards.[284] If the courts adjudicating civil remedy actions[285] become involved in the process of developing more detailed standards, and compel the agencies to justify their data-gathering in detail, the "accuracy, relevance, timeliness and completeness" requirement may become one of the stronger protections of the Privacy Act.

The second major set of fairness and accuracy provisions in the Act gives the data subject a right, modeled on the Fair Credit Reporting Act,[286] to find out whether an agency has information about him,[287] to gain access to his record,[288] and to obtain a copy.[289] This access right extends to medical or psychiatric records as well, in contrast to the prevailing law and the custom among members of the medical profession.[290]

---

judicial or quasi-legislative body. For example, a quasi-judicial board or commission need not reject otherwise admissible evidence because it is offered by a part[y] other than the individual to whom it relates or because it is not "necessary" to the decision or is not "complete." The normal rules of evidence would [continue] to govern in such situations.

283. *See id.* at 28960, 28964-65.

284. For example, the OMB Guidelines suggest a number of factors that bear on the determination of whether the data is "necessary," including the following:

> Could the need be met through the use of information that is not in individually identifiable form?
>
> Does the information need to be collected on every individual who is the subject of a record in the system or would a sampling procedure suffice?
>
> At what point will the information have satisfied the purpose for which it was collected, *i.e.*, how long is it necessary to retain the information? . . .
>
> . . . .
>
> Is the information, while generally relevant and necessary to accomplish a statutory purpose, specifically relevant and necessary only in certain cases? For example in establishing financial need as part of assessing eligibility for a program for which need is a legitimate criterion, parental income may be relevant only for certain applicants.

Id. at 28960.

285. *See* text accompanying notes 299-308 *infra.* Subsection 552a (g)(1)(C) of the Privacy Act specifically provides for a court action if an agency "fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual."

286. *See* 15 U.S.C. §§ 1681-1681t (1970).

287. 5 U.S.C.A. § 552a(f)(1).

288. *Id.* § 552a(d)(1). The data subject may have "a person of his own choosing to accompany him," but in this situation the agency may require a written statement authorizing the agency to discuss the data in the accompanying person's presence. *Id.*

289. *Id.* Agencies may charge for copies of records furnished to data subjects, but they may not charge them for the agency's cost of searching and reviewing the records. *Id.* § 552a(f)(5).

290. *See generally* Kaiser, *Patients' Rights of Access to Their Own Medical Records: The Need for New Law,* 24 BUFFALO L. REV. 317 (1975).

However, when medical records are sought the agencies may by rule establish "special procedures"[291] such as disclosing to a physician chosen by the data subject rather than directly to the data subject himself.[292] Apart from these special procedures, however, the Act does not attempt to deal with the risk that organizations with economic leverage or other forms of power over the individual data subject will use this advantage to compel the individual to obtain copies of his records and submit them with applications for benefits.[293] Since medical records often are relevant to employment or credit granting decisions, and since government agencies ranging from the military to the Medicare program collect large quantities of medical information, this risk may not be insubstantial.

The final type of procedure created by the Privacy Act to promote accuracy and fairness in government information use is the right to contest inaccurate or incomplete data, and to compel a correction. The mechanism is similar to that of the Fair Credit Reporting Act.[294] When a data subject disputes the accuracy of material in his file, he can obtain review of the question within the agency. If the agency ultimately refuses to make the requested correction, the data subject may file a "concise statement of disagreement" to be incorporated in his file.[295] The dispute must be noted in the file in any subsequent disclosures,[296] and a correction or notation of the dispute must also be sent to all persons who previously received the data if there is an "accounting of disclosures."[297] Finally, a data subject who is dissatisfied with agency performance in correcting records or implementing other safeguards established by the Act may bring a suit in federal court seeking civil remedies.[298]

---

291. 5 U.S.C.A. § 552a(f)(3).

292. OMB Guidelines at 28957. The Guidelines also indicate that agencies should use "far more stringent measures" to validate the identity of the person seeking access "when the records sought to be accessed are medical or other sensitive records." *Id.*

293. Indeed, the OMB Guidelines state that under the Act, the agencies may not even ask why the data subject wants his record: "The granting of access may not be conditioned upon any requirement to state a reason or otherwise justify the need to gain access." *Id.* at 28957.

294. *See* 15 U.S.C. § 1681i (1970).

295. 5 U.S.C.A. § 552a(d)(2)-(3).

296. *Id.* § 552a(d)(4).

297. *Id.* § 552a(c)(4).

298. The Act also provides criminal penalties for limited categories of violations. Under 5 U.S.C.A. § 552a(i), wrongful disclosure of agency records containing individually identifiable information, willful maintenance of a record system without meeting statutory notice requirements, and requesting or obtaining identifiable records under false pretenses are misdemeanors punishable by a fine of $5,000.

It seems unlikely that criminal penalties will play a significant role in administration of the Act. In addition to the low priority such crimes would receive from prose-

The Privacy Act creates four different kinds of actions for civil remedies. If an agency refuses a data subject's request for access to his records, he can bring an action to compel production, and the burden is on the agency to sustain its refusal.[299] Similarly, if the agency refuses to amend a record in response to a contention that it is inaccurate, the data subject can obtain a trial de novo and the court may order the agency to amend the record.[300] For other types of violations, the data subject can obtain damages rather than injunctive relief. When the individual suffers an injury because of the agency's failure to maintain records "with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness,"[301] or he is adversely affected by an agency's failure to comply with any other provision of the Act or its implementing rules,[302] he can recover "actual damages" together with costs and attorney's fees[303] if he can show that the agency action was "intentional or willful."[304]

---

cutors and the difficulty of showing criminal intent in many bureaucratic data-gathering activities, the Senate Report on the Privacy Act pointed out another problem:

> As introduced, the original bill contained strong criminal penalties for employees and others who violated or contributed to the violation of the Act. These penalties were deleted in Committee for two main reasons: the difficulties of effective enforcement through such criminal prosecutions and the possibility that the threat of prosecution may preclude that "Whistleblowing" and disclosure of wrongdoing to Congress and the press which helps to promote "open government."

S. REP. No. 1183, 93d Cong., 2d Sess. 27-28 (1974).

299. 5 U.S.C.A. §§ 552a(g)(1)(B), 552a(g)(3)(A).

300. *Id.* §§ 552a(g)(1)(A), 552a(g)(2)(A).

301. *Id.* § 552a(g)(1)(C).

302. *Id.* § 552a(g)(1)(D).

303. *Id.* § 552a(g)(4). This section further stipulates that "in no case shall a person entitled to recovery receive less than the sum of $1,000." *Id.* The Privacy Act also uses the term "general damages." *See* § 5(c)(2)(B)(iii). But there does not appear to be any explanation in the legislative history of a possible distinction between these two terms.

304. 5 U.S.C.A. § 552a(g)(4). According to the Staff Analysis on the compromise bill, this formulation was intended to reflect a standard of conduct falling between "gross negligence" and "willful, arbitrary and capricious." Staff Analysis, *supra* note 232, at 12245. This appears to be a rather confusing combination of tort doctrines and administrative law standards for judicial review of agency action. In tort law, questions of intent have generally dealt with the actor's certainty that the prohibited result would occur:

> [W]here a reasonable man in the defendant's position would believe that a particular result was substantially certain to follow, he will be dealt with . . . as though he had intended it. . . .
>
> On the other hand, the mere knowledge and appreciation of the risk, short of substantial certainty, is not the equivalent of intent. The defendant who acts in the belief or consciousness that he is causing an appreciable risk of harm to another may be negligent, and if the risk is great his conduct may be characterized as reckless or wanton, but it is not classed as an intentional wrong.

W. PROSSER, LAW OF TORTS § 8, at 32 (4th ed. 1971) (footnote omitted).

Since personal information provides the basis for many agency decisions, particularly those relating to individual entitlement to disability compensation or other benefits, judicial examination of agency information practices under the Privacy Act's civil remedies will sometimes be functionally similar to judicial review of the merits of agency action.[305] Thus, litigants may attempt to raise Privacy Act violations as a ground for invalidating agency action in existing statutory or nonstatutory review proceedings,[306] or instead may try to use the Privacy Act to seek review of administrative action when other routes to the courts are unavailable or unsatisfactory. While Privacy Act review would present some additional obstacles to the litigant,[307] it could also

---

305. This seems to be particularly true with regard to questions of the "accuracy, relevance, timeliness and completeness" of the agency's information. *See* text accompanying notes 278-84 *supra*. On a related point, the OMB Guidelines at 28958 assert, without citing any support in the legislative history, that:

> These provisions for amending records are not intended to permit the alteration of evidence presented in the course of judicial, quasi-judicial or quasi-legislative proceedings. Any changes in such records should be made only through the established procedures consistent with the adversary process. These provisions are not designed to permit collateral attack upon that which has already been the subject of a judicial or quasi-judicial action.

Perhaps so, but one wonders whether the result could be predicted so confidently if (a) the agency determination was an informal action taken without any trial-type or rulemaking proceedings; or (b) the trial-type proceedings were available only at the initiative of the data subject, and he elected to use the Privacy Act; or (c) quasi-judicial proceedings were available at the agency's initiative, but the Privacy Act suit was filed well before the agency decided whether to issue a complaint or otherwise go forward with the action.

306. The OMB Guidelines suggest that the Privacy Act does not preclude judicial review of violations of its provisions in other forms of action, including judicial review of administrative action under the Administrative Procedure Act, *id.* at 28968. Elsewhere however, the Guidelines argue that at least some violations of the Privacy Act would not be sufficient ground for setting aside agency action. In discussing the Act's requirement that individuals be informed at the point of data collection why the personal information is being sought and what the consequences of refusal to provide it may be, the Guidelines say:

> It was not the intent of this subsection [of the Act] to create a right the nonobservance of which would preclude the use of the information or void an action taken on the basis of that information. For example, a failure to comply with this section, in collecting crop yield data from a farmer, was not intended to vitiate a crop import quota based, in part, upon such information. However, such an individual may have grounds for civil action under [the Privacy Act] . . . if he can show harm as a result of that determination.

OMB Guidelines at 28961-62.

However, at least in the situation where the only interests at stake are the data subject's entitlement to a particular benefit (*e.g.*., a government disability compensation payment), the Privacy Act's actual damages may be functionally equivalent to a reversal of an administrative denial on conventional review.

307. The most obvious difficulty in using the Privacy Act is proving the necessary intent for violations which can bring civil penalties. *See* note 304 *supra* & accompanying text. Also, when the party seeking review is other than the data subject of the records in question, it may be difficult to establish standing under the Privacy Act.

have some clear advantages over more conventional judicial review of administrative action: trial de novo rather than the more limited review of facts that would be available under the traditional substantial evidence test,[308] a possible means of avoiding doctrines like ripeness, finality and exhaustion of administrative remedies that can frustrate or delay other forms of review, and a subsidy for successful litigants through the Act's award of reasonable costs and attorneys' fees for parties who "substantially prevail," in addition to money damages for many violations. Since neither the legislative history of the Privacy Act nor the OMB guidelines discuss these issues in any great detail, it will undoubtedly require some years of litigation before the relationships between the Act's remedies and other forms of review are fully established.

IV. Beyond the Privacy Act

Although the Privacy Act of 1974 is the most recent innovation in the ongoing evolution of legal responses to the privacy issue, it is already clear that the Act raises or leaves unresolved many questions about the shape of future efforts to safeguard medical records or other personal information. In general, these questions seem to fall into two broad categories: problems concerning the technical effectiveness of the Act's provisions, and more basic questions about the nature of the values that the Act is trying to serve.

One technical question that is explicitly reserved for later decision by the Privacy Act[309] is whether it makes sense to end the Act's coverage with federal agencies and their contractors, rather than extending it to all information systems.[310] In the medical records field, and particu-

308. *See* 5 U.S.C. § 706(2)(E) (1970).

309. The Privacy Protection Study Commission, *supra* note 239, is explicitly directed to make a recommendation to the President and the Congress regarding "the extent, if any, to which the requirements and principles of [the Act] . . . should be applied to the information practices of [governmental, regional and private] organizations by legislation, administrative action, or voluntary adoption. . . ." Privacy Act § 5(b)(2). *See also* H.R. 1984, 94th Cong., 1st Sess. (1975).

310. *Cf.* S. Rep. No. 1183, *supra* note 298, at 17-19, which describes the process by which the Senate-passed version of the Act was limited to federal data systems:

> As introduced, S.3418 applied to all governmental and private organizations which maintained a personal information system, under supervision of a strong regulatory body, with provision for delegating power to State instrumentalities. . . .
>
> . . . .
>
> Despite calls by . . . witnesses for total or partial coverage, the Committee was persuaded to delay a decision on total application by considerations of time and investigative resources for developing a full hearing record and for drafting the needed complex legislative solution for information abuses in the private sector . . . .

larly in the area of third-party payments, the institutional relationships that have developed make the line drawn by the Act seem artificial and unworkable. Within the major categories of medical record use—clinical care, statistical research and planning, and payment for services—the trend seems to be toward collaborative, large-scale information systems, with little regard to whether the organizations participating are state or federal, public or private. More basically, the economies of scale that argue in favor of large, often multistate systems,[311] together with the ease of transmitting data over national communications networks,[312] will undoubtedly lead to development of more regional and national systems that are effectively beyond the control of any one state; and, in any event, the states have shown little ability or interest in providing comprehensive protection for personal information.

If the coverage of the Privacy Act seems too narrowly confined in its limitation to federal systems, it may be that at the same time it sweeps too broadly by providing uniform safeguards for systems handling different kinds of information. Some commentators have urged that control provisions should be tailored to the nature of the data systems, with separate legislation for criminal justice systems, credit reporting organizations, medical record systems, and so on.[313] However,

---

311. *See* text accompanying notes 125-29 *supra*. *See also Report to the Committee on Scientific and Technical Information of the Federal Council on Science and Technology from the Panel on Legal Aspects of Information Systems*, 7 HONEYWELL COMPUTER J. No. 1, at I-1, II-9 (1973), which reads:

> [S]torage costs [for computerized information] may be expected to decrease rapidly with time and, in fact, will approach or be lower than that available with other media today, specifically including paper and microfilm. . . .
>
> . . . The extremely low costs are inevitably associated with very large volumes of information. Such extremely low costs do not appear to be achieveable in computerized systems if the quantities of information to be stored are small. Thus the economy is truly one of scale—the costs of storage are still substantial, but the volume of storage is so enormous that the cost per unit of information is very low.

312. *Cf. Report, supra* note 311, which states:

> Future communications costs . . . must be regarded with care, since today's experience will not carry over directly. The fundamental communications system we are using today (the telephone system) was designed for voice service. Its use for carrying data is an afterthought and, as a result, the system is limited in capacity. . . . The common carrier companies are beginning to put in place communication systems especially designed for data communications, whose costs for data transfer will be dramatically lower.

Id. See also id. at II-10 to II-11.

313. *See, e.g.*, WESTIN & BAKER at 350-51:

> [I]t appears clear to us that no single law, constitutional amendment, or court decision can cope with the tremendous diversity of issues and settings, and the uneven readiness for corrective action, that make up the current databank problem. Such total solutions are not worth pursuing.

Of similar effect is the distinction sometimes made between "primary" or clinical medical

the institutional relationships and data flows evidence a practical disrespect for these kinds of conceptual boundaries that makes it frequently difficult, and sometimes pointless, to categorize a particular system or item of information. If an investigative reporting agency preparing an insurance claim report obtains hospital records showing that a particular data subject was treated for a mild heart attack, and then incorporates this information in its own files so that it may later be used in response to queries from other insurers, or credit grantors, or potential employers, does the information change from a "medical record" to an "insurance record" to "credit" or "employment" data, and thereby require differential safeguards? The problem is that the sensitivity of a given item of information is partly contextual or use-related and partly inherent,[314] so that classification schemes based wholly on either dimension are in some measure unsatisfactory. Given the general lack of experience in implementing privacy controls, and the multiple uses made of medical records and other personal information, perhaps the most reasonable approach for the present is the Privacy Act's adoption of across-the-board controls, accompanied by rather generous escape hatches to permit adjustments where unique circumstances warrant.

Another major technical question about the Privacy Act is whether its remedial provisions will be effective in achieving their intended purposes. Both of the major enforcement devices provided by the Act, public notice and private litigation, have inherent weaknesses that may undermine the statute's safeguards. The public notice and opportunity to comment controls which govern the important issues of system structure, content and access policy reflect the philosophy that "sunlight is the best disinfectant," but in this context the maxim may be better rhetoric than policy. Ultimately, the effectiveness of notice-and-comment approaches depends primarily upon the ability of affected interests to articulate their concerns forcefully and persuasively before entities that can bring power to bear on the proposal in question—the proposing agency itself, the Congress, the courts, or the media.[315] The ability of pro-privacy interests to mobilize and deploy the necessary resources

---

records and "secondary" or statistical-administrative records. *See, e.g.*, Jackson, *Consideration of the "Active Working Record" Versus the "Permanent Record,"* 12 PSYCHIATRIC OPINION 29 (Jan., 1975).

314. *Cf.* Miller, *supra* note 174, at 1170-73.

315. *Cf.* S. LAZARUS, THE GENTEEL POPULISTS, 28 (1974):

> These three items—wealth, organization, and persuasion—comprise the elements of influence in democratic politics. If everyone can participate by right in the political process, then, inevitably, those who are best able to amass and deploy the ingredients of influence will participate most effectively.

See also note 249 *supra* & accompanying text.

seems questionable, at least in comparison to the planners, administrators and other data users who will generally advocate intensive data collection and free access to records.

For the Privacy Act's judicial controls to be effective, a sufficient number of parties must be willing to use them, and the issues in litigation must be framed so that the courts can exercise meaningful oversight of agency practices. Here, also, there are questions as to whether the necessary conditions can be met. The Senate-passed version of the Privacy Act concluded that private judicial enforcement would be inadequate to assure compliance, and that a separate, independent administrative agency should be created to enforce the Act's requirements.[316] Some of the factors that may deter potential litigants include the low visibility of many information misuses, with the result that the individual may not be able to link a denial of benefit or other harm to a violation of the statute;[317] the fact that the information practice objected to may have already been immunized under the "routine use" provision or some other exception; and the difficulty of proving the requisite intent[318] or sufficient actual damages to make the burdens of suing worthwhile.[319] If factors like these prove to be serious obstacles to judicial enforcement of the Privacy Act, or conversely if the Act's civil remedies work so well that data users feel the need for regulation in order to

316. S. REP. No. 1183, *supra* note 298, at 16:
Contrary to the views of Administration spokesmen it is not enough to tell agencies to gather and keep only data which is reliable . . . for whatever they determine is their intended use, and then to pit the individual against government, armed only with a power to inspect his file, and a right to challenge it in court if he has the resources and the will to do so. To leave the situation there is to shirk the duty of Congress to protect freedom from . . . incursions by the arbitrary exercise of the power of government and to provide for the fair and responsible use of that power. . . . For this reason, the establishment of the Privacy Commission is essential as an aid to enforcement and oversight.

317. Apart from the notice of intended uses at the point of data collection *(see* text accompanying note 248 *supra*), the data subject must take the initiative by (a) inquiring whether the agency has any records relating to him, (b) requesting access to his record, and (c) requesting the "accounting of disclosures" indicating who has had access to his record. Alternatives to this system, such as automatically providing all data subjects with periodic reports on the contents of their records and the disclosures that have been made, generally have been rejected as too costly. *See* HEW REPORT at 62. There is a middle ground that seems not to have been considered. For example, a random sample of data subjects could be given periodic automatic reports, which if carefully done should be adequate to expose patterns of error or abuse.

318. *See* note 304 *supra.*

319. 5 U.S.C.A. § 552a(g)(4)(A) sets a bottom limit of $1,000 on the amount of actual damages recoverable in a civil remedy action. While this will ease the problem of measuring damages in doubtful cases, it still may be a rather inadequate inducement to bear the burdens of litigation.

assure their access to data bases,[320] the proposals to establish a permanent Privacy Agency may be revived.

The second aspect of judicial remedies under the Act, the form in which questions will be presented to the courts, seems highly variable among different provisions of the Act. The access-to-records procedures are spelled out in detail, and implementation of these rights should be rather straightforward. Other sections of the Privacy Act, such as the "timeliness-relevance-accuracy-completeness" standard,[321] seem sufficiently analogous to functions that the courts already perform in passing on questions of evidence or legality of administrative action that the standards should be manageable, although doubtless some judges will be reluctant to second-guess administrative practices in detail.[322] Some of the provisions, however, embody little more than congressional hope that complex, difficult problems can be solved, and it seems unlikely

---

320. The idea is probably not as farfetched as it may sound. *See, e.g., Report, supra* note 311, at II-5, which reads:

> It may be the case, with respect to certain fields of knowledge, that the necessity of safeguards becomes more urgent as the consequences of a denial of access assume greater magnitude; it may be desirable, e.g., that unique knowledge banks serving such disciplines as medicine or political science are more likely candidates for the imposition of government regulation designed to achieve reasonable conditions of access than are comparable utilities dealing with literature or with other disciplines where a knowledge bank's uniqueness is not so pronounced. On the other hand, in some instances a concept of universal access, albeit not necessarily gratis, may be appropriate.

321. *See* text accompanying notes 279-85 *supra.*

322. *Cf.* Tarlton v. Saxbe, 507 F.2d 1116, 1122 (D.C. Cir. 1974), where the majority concluded that constitutional and statutory principles supported judicial review of the Federal Bureau of Investigation's handling of arrest records to determine whether they had exercised "such reasonable care as the FBI is able to afford to avoid injury to innocent citizens through dissemination of inaccurate information." Judge Wilkey, dissenting, argued that this kind of inquiry was beyond the competence of the courts:

> The breadth of the inquiry which the District Judge is directed to make . . . clearly shows the legislative nature of the task entrusted to him. . . . The inquiry involved is the type which a Congressional committee is supposed to make, taking into account data on a nationwide basis from all interested parties, before drafting and enacting legislation. This court thrusts on one District Judge sitting in the District of Columbia a task of national scope.

507 F.2d at 1132. The courts may also find that computer operators' notions of accuracy are quite different from lawyers'. *Cf. Report, supra* note 311, at II-5 to II-6, which reads:

> As a practical matter, and perhaps also as a matter of legal compulsion, the user should be furnished by a knowledge bank with the following: (1) a description of the parameters of the data base indicating the intended scope and nature of the information utility he is dealing with; (2) a disclosure of the subjective criteria utilized by the knowledge bank's personnel to determine what is or is not suitable material for inclusion in the defined data base; (3) an outline of the methodology of processing input to output; (4) a disclosure of the methodology used in classifying and indexing information; and (5) identification of computer output by source as either abridgement, fragmentation, or interpolation from stored data.

that the courts will be able to devise satisfactory solutions if these vague provisions are made the subject of civil remedy actions.

Perhaps the most troublesome of these vague standards is the requirement that agencies "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.[323] The difficulty is that the technology of data security is not well developed,[324] and "the economics of information management and the concomitant costs of confidentiality and security of information in automated data systems are neither well-understood, well-documented, nor well-quantified."[325] The analyses of the subject that are available suggest that the concept of "technical security" is multifaceted, and that a really "secure" system is likely to be neither cheap nor easy to develop.[326] In a computer system, at least three distinguishable kinds of goals are encompassed in the notion of technical security:

1) Protection against physical mishaps involving data in the system, such as theft, fire, flood, and accidental or intentional destruction;

---

323. 5 U.S.C.A. § 552a(e)(10).

324. *See, e.g.*, U.S. DEPARTMENT OF COMMERCE NATIONAL BUREAU OF STANDARDS, GOVERNMENT LOOKS AT PRIVACY AND SECURITY IN COMPUTER SYSTEMS 20 (1974) [hereinafter cited as GOVERNMENT LOOKS AT PRIVACY AND SECURITY], where an expert in the computer security field is quoted as saying that "in practically all cases, the off-the-shelf computers and control programs supplied by the manufacturers have inadequate protection mechanisms for providing controlled access to a computer's assets." Two of the most intensive current efforts, IBM's research project and the RISOS program, were started within the past two or three years. *See* Thomas & Courtney, *A Systematic Approach to Data Security*, in APPROACHES TO PRIVACY AND SECURITY in COMPUTER SYSTEMS 26 (U.S. Department of Commerce, National Bureau of Standards 1974) [hereinafter cited as APPROACHES TO PRIVACY AND SECURITY]; Abbott, *The Problem of Protecting Data Privacy*, 4 J. CLINICAL COMPUTING 66, 72 (1974).

325. Davis, *A Technologist's View of Privacy and Security in Automated Information Systems*, 4 RUTGERS J. COMPUTERS & LAW 264, 278 (1975); *cf.* GOVERNMENT LOOKS AT PRIVACY AND SECURITY 25 (analysis of the cost question remains "more emotional than objective").

326. For example, an Air Force study has concluded that removing all of the known security deficiencies in a contemporary computer system would cost about two and a half million dollars, and one of the leading researchers on security has estimated that it requires about 18 man-months of work simply to do a "good integrity study" for the purpose of identifiying major security problems. GOVERNMENT LOOKS AT PRIVACY AND SECURITY 26. It seems to be generally accepted that security costs will be higher if it is necessary to remedy security defects in a previously designed system, rather than building in technical safeguards from the outset. Correcting security flaws in computer programs after a system is in operation may cost as much as ten times what it costs an intruder to "break" the system. GOVERNMENT LOOKS AT PRIVACY AND SECURITY 26; *cf.* Lipner, *Security Considerations in Information System Design*, in APPROACHES TO PRIVACY AND SECURITY 55, 56.

> 2) Controlled access to assure that the user of the system is who he says he is, and can obtain access only to data and programs that he is authorized to use; and
>
> 3) Integrity of the system—that is, it performs in accord with specifications, fails within narrow bounds and has appropriate checks on the accuracy of data.[327]

Achieving these goals involves the interaction of many techniques, including both equipment (computer hardware and software, communications and encrypting technology, specially designed buildings, burglar alarms, and the like) and behavioral controls (legal prescriptions, administrative regulations and sanctioning procedures, hiring and management practices, ethical codes, education).[328] Different mixes of these control technologies within a given system create different cost tradeoffs, including the cost of diminished utility of the system that typically results from increased security.[329] A logical and systematic cost analysis for security purposes would require identification of individuals and groups that may be motivated to "break" the system, measurement of the "payoff" that they could obtain through penetration, and assessment of the difficulty or cost they would experience in trying to gain access.[330] In the medical records field, as in most others, this kind of information generally will not be available, and even if it were this intricate cost-benefit analysis hardly seems to be the kind of inquiry that courts are well-equipped to handle. If the civil remedies approach is to work in a nebulous, highly technical area like data security, the issues must be simplified (and probably over-simplified) through further administrative rulemaking,[331] or through an analysis which focuses only on the most obvious and easily implemented technical security measures.[332]

327, *Cf.* GOVERNMENT LOOKS AT PRIVACY AND SECURITY.

328. *See generally* Miller, *supra* note 174, at 1207-21; APPROACHES TO PRIVACY AND SECURITY; GOVERNMENT LOOKS AT PRIVACY AND SECURITY.

329. *Cf.* MEDICAL PRIVACY AND COMPUTER TECHNOLOGY, *supra* note 7, at 85: "[T]he attainment of total confidentiality would result in infinite cost for zero utility."

330. *Id.* at 86 (letter from Dr. Alvin A. Bicker, Director of Information and Computer Services, State University of New York at Stony Brook).

331. The OMB Guidelines at 28966 state:

> Until such [general] standards [for system security] are developed and promulgated, agencies will be required to analyze each system as to risk of improper disclosure of records and the cost and availability of measures to minimize those risks. The Department of Commerce (National Bureau of Standards) will be issuing guidelines and standards to assist agencies in evaluating various technological approaches to providing security safeguards in their system and for assessing risks.

332. *See, e.g.*, Thomas & Courtney, *A Systematic Approach to Data Security*, in

The cost questions arising from the technical security requirement raise the broader issue of whether ambitious privacy legislation like the Privacy Act of 1974 is socially justifiable. Even the relatively limited safeguards of the Privacy Act will probably cost several hundred million dollars a year to implement,[333] and neither the Act nor the legislative history provides a very clear statement of the values that will be realized from this expenditure. Since the legal system has generally not treated personal information as the property of the data subject and allowed a true market system to develop,[334] protection of privacy is usually justified on non-economic grounds. In discussions of medical privacy, the rationales for protection seem to fall into three broad categories: the utilitarian concern that the quality of medical care would decline if confidentiality between doctor and patient could not be assured; the belief that individuals would be subjected to psychological and social harm if they could not keep intimate facts private; and the

---

APPROACHES TO PRIVACY AND SECURITY 26, where threats to data integrity are listed in the following order of decreasing probability:

1) Errors and omissions;
2) Dishonest employees, mostly using data for improper purposes or system functions that they are authorized to use in their routine duties;
3) Fire;
4) Disgruntled employees sabotaging the system;
5) Water; and
6) "Others"—including strangers trying to penetrate the system.

See also WESTIN & BAKER at 306, where it is noted that all intrusion cases which the authors were able to document involved an "insider" who already had access to the system.

333. Commenting on an earlier draft of the bill, the Office of Management and Budget estimated that the costs of implementation "will be on the order of $200 to $300 million per year over the next four to five years, with an additional one-time start-up cost of about $100 million, which would be expended within the first two years." H.R. REP. No. 1416, 93d Cong., 2d Sess. 36 (1974).

334. *See, e.g.,* Gotkin v. Miller, 379 F. Supp. 859 (E.D.N.Y. 1974) (hospital records the property of the hospital rather than the patient). It has been argued that there is no theoretical reason why privacy could not be valued by a market system in which the data subjects essentially licensed data users to have access to personal information, analogously to a copyright proprietor licensing various uses of a book or song. Goldstein, *Information Systems and the Role of Law: Some Prospects,* 25 STAN. L. REV. 449, 473-75 (1973). Efforts to find "surrogate" market values for personal privacy by examining market transactions which are thought to have a privacy component appear to be primitive at best. *See, e.g.,* GOVERNMENT LOOKS AT PRIVACY AND SECURITY 24, which states:

> [A]pproximately 15% of the telephones in the U.S. have unlisted numbers for which the subscribers pay various rates varying from a $9.00 fixed charge to $.50/month. On a less discretionary basis, passengers on national airlines have been paying a surcharge on fares for airport security and anti-hijacking measures. Other widely used services which have a cost component for privacy or security include: recreation, housing, health, education, and local (commuting) travel. From these broad-based examples, it is possible to conclude that the costs for maintaining personal data confidentiality and security in government-operated information systems will be readily borne by the public.

fear that control over sensitive personal data presents a threat to political autonomy and personal freedom.

The most commonly given justification for medical privacy, the utilitarian claim that patients will keep important information secret from their doctors or forego needed medical treatment if they do not have assurances of confidentiality[335]—is also the least substantial. For years, evidence scholars have pointed out that nobody has ever been able to demonstrate significant variations in health or health care utilization among states depending upon the existence *vel non* of a doctor-patient privilege.[336] In any event, apart from extraordinarily stigmatizing diseases like alcoholism or venereal disease, or the unique problems of mental illness,[337] it seems highly unlikely that substantial numbers of people would forego needed medical treatment out of concern for their privacy.

The second major theme of medical privacy justification, the need to protect the individual's emotional tranquility and relations in the community, has been articulated in various ways, ranging from the assertion in the Hippocratic Oath that patient confidences are "shameful to be spoken about"[338] to more modern theories of the role of intimacy in personality development:

> Present-day spokesmen for the right of privacy frequently employ the imagery of concentric circles or spheres. In the center is the "core

335. *E.g.*, Note, *Medical Practice and the Right to Privacy*, 43 MINN. L. REV. 943, 945 (1959), where the author states:

> The duty of professional secrecy is not based merely on an altruistic idea of "sacredness of the relationship"; nor is it based solely on interests of common decency in protecting the patient's reputation or his peace of mind, although these factors are both important underlying reasons for keeping confidential information secret. The principal reason is that without some assurance that information given to the doctor will be kept in confidence, a patient might be reluctant to reveal embarrassing facts which could be vital to proper diagnosis or treatment. And so the physician has a very serious obligation, both to his patient and to his profession, to keep all the information he acquires during the course of his professional relationships absolutely secret.

336. *See, e.g.*, Chafee, *Privileged Communications: Is Justice Served or Obstructed by Closing the Doctor's Mouth on the Witness Stand?*, 52 YALE L.J. 607, 609 (1943).

337. Freedman, *Implementation of Assured Confidentiality for Clinical Information*, 4 J. CLINICAL COMPUTING 84, 85 (1974): "Some psychoanalytic colleagues of mine who practiced in Germany during the 30's, recounted to me . . . that after 1933, it was quite impossible to practice psychiatry, in the way it had been done before, because the very oppressiveness and awareness of the possibility of others gaining access to such information completely blocked therapy."

338. The oath is quoted as follows in Note, *Legal Protections of the Confidential Nature of the Physician-Patient Relationship*, 52 COLUM. L. REV. 383 (1952): "What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of man, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about."

> self," which shelters the individual's "ultimate secrets"—"those hopes, fears, and prayers that are beyond sharing with anyone unless the individual comes under such stress that he must pour out these ultimate secrets to secure emotional release." According to this image, the next largest circle contains intimate secrets which can be shared with close relatives or confessors of various kinds. Successively larger circles are open to intimate friends, to casual acquaintances, and finally to all observers.
>
> . . . The patient, in distress, shares with the physician detailed information concerning problems of body or mind. To employ the imagery of concentric circles, the patient admits the physician to an inner circle. If the physician, in turn, were to make public the information imparted by the patient—that is, if he were to invite scores or thousands of other persons into the same inner circle—we would be justified in charging that he had violated the patient's right of privacy and that he had shown disrespect to him as a human being.[339]

This rationale seems more persuasive, at least if one assumes that the model of personality development in which it is based is a desirable one, and also one that it is not simply an ephemeral artifact of a particular historic period or narrow social class.[340] However, desire to protect the individual personality does not seem to account for many of the concerns evident in recent legislative proposals like the Privacy Act. If the harm to personality was thought to lie in the act of being forced to give up the intimate data unwillingly, regardless of the use to be made of it, one would expect to see more emphasis on limiting or pre-

---

339. Walters, *Ethical Aspects of Medical Confidentiality,* 4 J. CLINICAL COMPUTING 9, 12-13 (1974). *See also* Lavere, *Privacy and Human Person,* 4 J. CLINICAL COMPUTING 31, 32 (1974) (emphasis in original):

> Why are we . . . so chary about self-revelation in any form: . . . [T]he answer is simply that we are *human persons,* whose very existential integrity as conscious, and especially as self-conscious, beings requires *privacy,* the unique, inner, almost impenetrable world which is the immediate and sustaining environment of the self. From this mysterious center emanates all that we do in self-conscious commitment to what we are.
>
> But we are selective in what we say and do publically [*sic*], lest we reveal to an incomprehending and unappreciative world the inestimable inner richness of our subjective being, our very being, only to have this revelation ignored or ridiculed. This is why we are private and concerned about privacy.

340. *Cf.* Miller, *Privacy in the Modern Corporate State: A Speculative Essay,* 25 AD. L. REV. 231 (1973):

> I am inclined to believe, although admittedly the conclusion is reached intuitively rather than by hard evidence, that privacy is a value—a preference, if you will—mainly of the middle-class and upper middle-class—of, that is, the social group roughly labeled as the "elite" or the "establishment." . . .
>
> Personal privacy, thus, is like freedom: Both are 18th- and 19th-century values of diminishing significance in the modern age—if, indeed, they ever had any substantial basis in social attitudes and behavior.

Id. at 231-32.

venting the collection of data. If, on the other hand, the threat to personality is perceived as risk of disclosure to "significant others"—a fear that sensitive information will leak back to family, friends or colleagues who have been admitted to varying degrees of intimacy—then there ought to be little concern with what large, impersonal organizations may do with the information, so long as they are careful to keep it away from the data subject's circles of acquaintance and kinship. Some of the provisions of the Privacy Act do seem to be premised on one or the other of these rationales, but others—the right to find out if an agency has records affecting you, the ability to make corrections or file statements of disagreement, and assurances that the data concerning you is accurate, timely and complete—have only slight relevance to psychological development and intimacy with acquaintances. Nor do these provisions seem to serve the third major rationale of privacy, the political concern that the power of the state be limited by shielding areas of social and political life from official scrutiny.[341] Indeed, it seems anomalous to refer to these provisions as "privacy safeguards" in any traditional sense; if the basic nature of privacy is a "right to be left alone," these procedures embody a right *not* to be left alone, derived from due process concepts of notice and a right to be heard in decisions that affect basic personal interests. Thus, the access-and-correction procedures are tools which the individual may use to resist the manipulative efforts of public and private bureaucracies, whether in health care or elsewhere. In this respect they can be viewed as sharing a common objective with the more conventional "privacy" controls on collection, storage and disclosure of personal information: redressing the balance of power between the individual and the large, impersonal organizations that dominate society. If the outcome seems dubious,[342] the effort is at least worth making.

---

341. *See, e.g.*, A. MILLER, THE ASSAULT ON PRIVACY 38-46 (1971); WESTIN & BAKER at 14-20; Goldstein, *supra* note 334, at 472, quoting a paper by Prof. Westin entitled "Civil Liberties and Computerized Data Systems."

342. For a pessimistic appraisal, see Miller, *supra* note 310. Another factor militating against participation and control by the data subject is the cost of implementing access-and-correction rights for data subjects, which seem certain to be much higher than the costs for controls not involving such participation. *See, e.g., Report, supra* note 311, at II-9, which reads:

> [P]reparation costs (creation, editing, reviewing, and preparing for "publication") are likely, if anything, to be higher than they are today. These are people-dependent service functions which show a steady trend toward greater and greater cost. In addition, the kinds of people needed for these functions are scarce and, naturally, reluctant to devote themselves to such tedious tasks.
>
> As more and more expansion of knowledge services takes place, the difficulty and cost of information preparation will get worse. These pressures may make unlikely the re-doing of a bad knowledge bank . . . .