Buffalo Law Review

Volume 24 | Number 2 Article 5

1-1-1975

Data Banks in a Free Society. By Alan F. Westin and Michael A. Baker. Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems

Mary Kay Kane
University at Buffalo School of Law

BOOK REVIEW

DATA BANKS IN A FREE SOCIETY. By ALAN F. WESTIN and MICHAEL A. BAKER. New York, New York: Quadrangle Books 1972, xxi + 522 pages $12.50.

RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington, D.C.: DHEW Publication No. (OS) 73094. *(concurrently published:* Cambridge, Massachusetts: Massachusetts Institute of Technology Press) 1973, xxxv + 346 pages $2.35 (paper).

MARY KAY KANE*

INTRODUCTION

Mankind's urge to pry, intrude, and eavesdrop is as old and basic as curiosity itself. As pointed out by one commentator, "[s]how me a man who doesn't eavesdrop, and I'll show you a man with a serious hearing problem."[1] However, the human memory is exhaustible, and it eventually fades. Written records are more durable; but they are costly to compile, expensive to preserve and inaccessible in proportion to their bulk. What the computer has done is to create virtually unlimited capacity to record, store and retrieve every bit of trivia about human lives, sometimes because it simply is easier to record the fact than to discard it, at other times because it is laudable and useful to do so. But most often this is done with no regard for the risk that at some later date the information may be used for different or destructive ends.

---

* Assistant Professor of Law, State University of New York at Buffalo; J.D., University of Michigan, 1971. Additional information bearing upon my qualifications to review these books, as well as upon my possibly disqualifying biases, is that I was the Associate Director, with Professor Arthur R. Miller of Harvard Law School, of a National Science Foundation project studying problems of privacy and social and behavioral science research data (GS-35291). Our report for that study will be available shortly to the public. However, I am obliged to say what should be obvious—the views I express in this review are my own; they should not be attributed to the National Science Foundation, nor to Professor Miller. Finally, I would like to express my appreciation to Professors Ronald J. Allen and Paul Goldstein, both of the State University of New York at Buffalo School of Law, for their helpful comments on earlier drafts of this review.

1. Schwartz, *The Hearing Tom is Everywhere,* NEWSDAY, Jan. 9, 1965, (magazine), at 9W, col. 1.

The two publications under review address themselves to this modern phenomenon—the computer—in attempts to determine whether 20th century record keeping does in fact pose greater threats to individual privacy[2] and, if so, what are the means of reducing or remedying this threat. The books appear to reach different, almost opposing, determinations as to the potential dangers of computerized record keeping and, as is so often the case, the reader may be convinced by the effectiveness of the authors' advocacy rather than by the merits of their position. Thus, in addition to commenting on the style and persuasiveness of each volume, it is my intention to examine the factual bases on which the authors rely in the hope of reaching an independent judgment on the question of the effects of modern data practices on the rights of citizens.

The Westin-Baker book, *Databanks in a Free Society,* deserves consideration by policymakers in the privacy arena for several reasons. Westin is renowned as a researcher and thinker in the field of personal privacy. Furthermore, the publication carries with it the substantial prestige of sponsorship by the Russell Sage Foundation and the Computer Science and Engineering Board of the National Academy of Sciences. It professes to be an empirical investigation, by "a staff well versed in computer science, economics, journalism, law, political science, psychology, and sociology,"[3] of the range of actual and potential computer abuse. As stated in its introduction, the book presents "a comprehensive body of facts about the actual effects that computers, communications, and allied information technologies have had on creating, sharing, and using files on individuals."[4]

Based on their field research, the authors perceive few problems (to which they offer solutions), concluding that computers despite their potential do not now, and probably will not in the foreseeable

2. "Privacy is the right to live one's life in one's own way, to formulate and hold one's own beliefs, and to express thoughts and share feelings without fear of observation or publicity beyond that which one seeks or acquiesces in." OFFICE OF SCIENCE AND TECHNOLOGY OF THE EXECUTIVE OFFICE OF THE PRESIDENT, PRIVACY AND BEHAVIORAL RESEARCH 8 (1967). *See also* Warren & Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 196 (1890). Utilizing this definition, when an organization either obtains personal information without the consent of the individual about whom it pertains or transmits personal data to others without his consent, a breach of privacy occurs. Thus, the central question in both books is to what degree the development of the computer and communications technologies facilitates unauthorized access.

3. A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY xx (1972).

4. *Id.* at xix.

future, pose a substantial threat to the privacy of American citizens. In short, the study carries impressive credentials, the aura of sound methodology, and persuasive argumentation. However, a close examination of exactly what is being said reveals glaring inconsistencies and a failure to appreciate some of the important implications of the data that was collected from the numerous organizations visited.

In contrast, the HEW report, *Records, Computers and the Rights of Citizens,* is hardly a book at all, nor is it the type of document that typically attracts the attention of a book reviewer or the general public. Nonetheless, among the members of the Secretary's Advisory Committee, who were responsible for the report, were many persons in the private and public sectors actively engaged in the assembly and recording of information about people, as well as computer specialists and noted civil libertarians.[5] Hence it is fair to assume that they also knew something about the dangers of which they spoke. In addition, the Committee's staff presented reports and arranged hearings at which testimony was given by over 100 witnesses representing more than 50 different organizations. On the basis of this evidence the Committee concluded that the problem of preserving privacy is not only acute, but also is growing worse in almost direct proportion to the availability of computer capacity.

I. The Findings

A. *The Westin-Baker Study*

As examples of the findings made from 55 site visits to various organizations in 1970-1971, Westin and Baker present 14 profiles of record keeping in different spheres of life—for example, law enforcement, credit bureaus, municipal governments, and religious organiza-

5. The Committee's members were: Willis H. Ware (Chairman), Professor Layman E. Allen, Juan A. Anglero, Senator Stanley J. Aronoff, Assemblyman William T. Bagley, Professor Philip M. Burgess, Gertrude M. Cox, K. Patricia Cross, Gerald L. Davey, J. Taylor DeWeese, Guy H. Dobbs, Robert R. J. Gallati, Florence R. Gaynor, John L. Gentile, Dr. Frances Grommers, Commissioner Jane L. Hardaway, James C. Impara, Patricia J. Lanphere, Professor Arthur R. Miller, Don M. Muchmore, Jane V. Noreen, Roy Siemiller, Mrs. Harold Silver, Sheila M. Smythe, and Professor Joseph Weizenbaum. HEW, Records, Computers and the Rights of Citizens xii-xiii (1973).

tions.[6] Analyzing the data obtained from these visits, the authors arrived at the following observations:

> (1) "the content of computerized records about individuals has *not* increased in scope compared to what was collected in their manual counterparts during the precomputer era";[7]
>
> (2) "the information that is considered most sensitive and subjective in each type of organization has *not* yet been put into computerized files, but is being maintained in manual records";[8]
>
> (3) "precomputer rules [on data sharing] have *not* been altered in computerizing organizations; rather, customary practices have been reproduced with almost mirrorlike fidelity."[9]

From these "facts" they conclude that earlier predictions that national, interlocking systems would erode traditional and cherished notions of privacy and even due process were inaccurate as well as totally uninformed and that computerization, in and of itself, poses little threat to these rights.[10]

A careful perusal of the profiles casts some doubts on the question whether there was sufficient evidence to support their position. For example, the organizations visited generally indicated that more sensitive data or increased data about file subjects were not being collected

---

6. The choice of organizations that were profiled is somewhat deceptive. Purportedly the profiles reflect "the real world of computerizing organizations during the past decade and today." A. WESTIN & M. BAKER, *supra* note 3, at 5. Clearly they do represent some of the better known and large organizations engaging in data banking. At least in some instances, however, that very prominence meant that better confidentiality control was exercised. For example, the Social Security Administration was described as an example of federal government record-keeping. That agency represents one of the few which have grappled with privacy problems. As the HEW report indicates, activities throughout the other sections of HEW were less laudable. Similarly, the American Council on Education was chosen as the research model. Again, that organization represents the exception rather than the rule in terms of the security measures taken. More typical research practices are described and analyzed in the forthcoming NSF report with which I have been connected.

7. *Id.* at 244.

8. *Id.* at 249.

9. *Id.* at 253.

10. The authors are strongly critical of the journalists who initially stirred up public alarm about data keeping policies, arguing that these reporters overreacted. *Id.* at 269-79. Nevertheless, their own studies show numerous cases in which corrective policies were instituted only in response to just such pressure. *See, e.g., id.* at 85-88 (Kansas City, Missouri, Police Department); *id.* at 105-07 (Santa Clara County, California); *id.* at 178-79 (Massachusetts Institute of Technology). Thus it is just as easy to conclude that without that pressure, which resulted in the exercise of some self restraint, some of the fears expressed by the early journalists would have come to pass.

as a result of computerization. At the same time, however, some of the persons interviewed mentioned that improved technology had resulted in the collection and retention of files on greater numbers of people[11] and in greater dissemination due to increased access.[12] Expanding the number of existing files, as well as their transferability and accessibility, clearly poses a threat to privacy. Yet, these developments appear to be either overlooked or viewed as of little moment by the authors. If the former were the case, the soundness of their findings could be disputed. But it is not. Westin and Baker firmly state that a direct effect of computerization is the creation of larger databases[13] and the greater use of the information in those files.[14] Thus, they must have determined that these effects were not worthy of concern. This being so, then I question their definition of privacy, which, to my mind, always has included the individual's right to decide to whom to reveal his own data.

Any doubts about the conclusions reached in this study are not aided by the fact that even Westin and Baker appear unconvinced by their findings.[15] The last sentence of their book states:

> Our task is to see that appropriate safeguards for the individual's rights to privacy, confidentiality, and due process are embedded in every major record system in the nation, *particularly the computerizing systems that promise to be the setting for most important organizational uses of information affecting individuals in the coming decades.*[16]

---

11. For example, in their discussion of the Bank of America the authors alleged that "the expansion of bank services to include Bank Americard and the creation of its massive files—high volume transactions for 1.9 million accounts—is largely attributable to the availability of computer technology." *Id.* at 122.

12. For example, personnel at the New York State Department of Motor Vehicles stated that computerization had meant a "much greater use of our system by law-enforcement agencies." *Id.* at 75. Also, officials at R.L. Polk & Co. talked about plans for an immense linking capacity that would be possible because of the availability of computers. *Id.* at 167.

13. *Id.* at 293-94.

14. *Id.* at 284-88.

15. At one point, they state: "What is significant for public policy understanding is that these managers conceive of computerization as neither an experiment nor a matter of much choice. They see it instead as a necessity . . . ." *Id.* at 234. They also admit that they "did observe the emergence through computerization and rapid communications systems of regional and national data systems that are linking more closely organizations that had shared information in the manual era, and that these networks are giving rise to some new patterns of information handling and use." *Id.* at 291.

16. *Id.* at 405 (emphasis added).

How can this statement be reconciled with their earlier findings that computerized record keeping does not threaten individual liberties?

The first set of observations indicating the benign character of computerization represents the major portion of the book, which may induce a false sense of security for the reader who does not discern this apparent conflict. In addition, the subsequent exhortation and suggestions for better record keeping practices necessarily lose some of their potential effectiveness because little need will be perceived to develop means to prevent what the authors had argued are nonexistent abuses.

Any feeling of complacency would be dangerous. All the Westin-Baker findings reflect is the fact that early enthusiasts underestimated the cost, time, and difficulties inherent in computerization.[17] The authors argue that "sociopolitical" forces will keep record keeping and computerization from getting out of control.[18] But, those forces are aroused only after a threat has been perceived. Thus, we are right back where we started before the release of the Wesin-Baker data, recognizing that problems will result from expanded uses of personal information unless we act now.

Let me make clear that I do not contend that the authors fail to see the crucial questions posed by increased data collection. Their suggestions for control mechanisms in the last chapter belie that conclusion. However, in their treatment of the profiles of organizations visited they focus so intently on the question of what records or pieces of information have been converted from manual to computer files and on the data handling practices, that they completely fail to point out the important confidentiality problems created by the record systems as they now exist. One might reasonably ask why it is so important whether organizations are collecting more data *as a direct result*

17. For example, the authors' profile of the failure in New Haven, Connecticut, to achieve the originally planned fully computerized central databank for municipal government illustrates the unrealistic approach taken by many data managers when computers first began to be utilized on a large scale. *Id.* at 88-100. As Westin and Baker describe it, city officials indulged in what might be termed "blue-skying," proposing and expecting a fully automated system, but not taking into account the time and research necessary to meet their requirements. The failure of that venture did not discourage the city administrators, however. All it did was make them more realistic in their expectations. As the Controller, Frank Kelly, stated: " 'We'll seek federal or state funds on a program-by-program basis to computerize only those things that are doable.' " *Id.* at 100.

18. *Id.* at 323-24.

of computerization or as a result of other causes. The point is that they are doing so, and the authors do not deny that computer capacity eventually, if not at the present time, will ease the problems of storage and dissemination.

For example, one of the conclusions of this study was that "customary" data sharing practices are continuing even after initial computerization.[19] What does this mean? As the authors admit, informal data sharing is taking place under the "information buddy system,"[20] although this is not generally known by the public and is even in direct violation of formal confidentiality rules.[21] The crux of the matter is, of course, that the computer makes violation much easier—a problem which Westin and Baker should have addressed.

Another criticism of their study is that in some cases their investigations did not go far enough. Illustratively, time and again Westin and Baker note that subjective, sensitive data generally are left in manila files. But, this clearly does not solve all confidentiality problems. To begin with, is there a computerized entry indicating the existence of the manual file? For example, a computerized university system might include student grade records and the credit awarded for courses taken. Subjective data, such as a counselor's report or teacher evaluation, might be kept in manual files in the counseling office. One of the main security protections for this information is the fact that few know it exists. However, if there is a computerized entry in the student's central file indicating that psychiatric or counseling

19. The discussion of data sharing practices also presents an example of apparently inconsistent positions taken by the authors. After concluding that those activities have not been altered by the advent of computers, the authors go on to note: "In the public records area, we found that greater volumes of information have been made available to users because of computerization, and often to a larger number of users." *Id.* at 254. This expansion, they maintain, is not important because the class of users remains the same. But, the fact that the same type of data users as in the precomputer era participates in the computerized system does not, to my mind, a fortiori mean that no threats are posed. Much more data are now available to the user. For example, I might not object that my employer had access to my income information, but I would be distressed to discover that by a single request he could obtain my voting and marital history records in addition.

20. The "information buddy system" permits officially unacknowledged data sharing based on the personal relationships of individuals within and without a given organization. It exists typically because many corporate security officers and insurance and credit investigators are former federal or local law enforcement agents, permitting a flow of information between those agencies and the private organizations with which the former members are associated.

21. A. WESTIN & M. BAKER, *supra* note 3, at 253.

data are maintained elsewhere and if entry to that general record is available to a wide range of persons, then the manual file loses its anonymous character. Unfortunately, the authors never address this problem of computer indexes.

Perhaps I am overly skeptical, but I cannot get rid of the feeling that Westin and Baker accepted too readily the statements made by data handlers about their plans and cautions for the future.[22] Although they apparently felt that full cooperation was given them,[23] one may question whether it is reasonable to expect information managers to be perfectly candid about their plans. It should be recalled that the interviews took place in 1970-1971 following extensive hearings on the commercial credit industry and privacy, and on databanking in general. In that atmosphere, it is just as reasonable to assume that managers would be quick to make self-serving statements to disassociate themselves from any of the questionable practices revealed before the Congress. Moreover, the computer industry was entering a period of economic recession so that long-range plans for major expansions probably were not then feasible.[24] Finally, the technology

22. A case in point is the data base maintained by the American Council on Education. ACE officials contend that because the data which links names and responses are stored outside the country, the research data are free from subpoena since ACE does not control the link. Westin and Baker appear to accept this conclusion. *Id.* at 192. However, during my own interviews with ACE personnel in connection with the research mentioned earlier (*see* note * *supra*), I discovered that complete independence was not maintained between ACE and the linking agency. Indeed, the Council had sent some of its own programmers to aid in solving some of the linking agency's problems. ACE may be deemed to have some control over that agency, and, if so, a subpoena to it could require it to produce the linking data. *See* Societe Internationale v. Rogers, 357 U.S. 197 (1958).

Another example is the authors' treatment of grant-in-aid and similar governmental programs. Cavalierly, they dismiss these programs as presenting almost no threat to privacy because HEW receives only statistical reports. A. WESTIN & M. BAKER, *supra* note 3, at 31. But a closer look at how those programs operate shows that personalized, identifiable data often are forwarded to the federal government. *See* HEW, *supra* note 5, at 91-92.

23. A. WESTIN & M. BAKER, *supra* note 3, at 27.

24. The authors themselves note this effect. *Id.* at 240. At the time Westin and Baker wrote they expressed the view that certain business economics would deter the use of computers for socially wasteful and destructive purposes. Events have shown, however, that the evolution of ever more capacious and sophisticated machines has created a problem of excess capacity. As idle hands are said to make mischief, idle machines cry out to be used. Enterprises that could not possibly afford a computer, can and do have computer service available to them. Association of Data Processing Service Organizations, Inc. v. Camp, 397 U.S. 150 (1970), may seem to lawyers to be an important case on standing to sue; it is at least as important as a reflection of the fact that excess capacity will not stand idle.

necessary to develop the communications links that would be the core of any national interlocking of databases and easy user access had lagged far behind hardware and software developments, so that those systems were not possible in 1970-1971. However, there already have been significant technological advances (and networking through packetswitching appears to be on the horizon), which would lower the cost of computer communications and networking significantly.[25]

B. *The HEW Report*

The approach taken by the HEW Committee was vastly different from that of Westin and Baker. The Committee held public hearings at which its members cross-examined information managers. It may very well be that this searching for facts in what was akin to an adversarial setting revealed more accurately and more extensively the true state of affairs. In part, this may explain why the HEW report reaches conclusions almost directly opposing those of Westin and Baker. In the words of the Committee:

> [T]he application of computers to record keeping has challenged traditional constraints on record-keeping practices. The computer enables organizations to enlarge their data-processing capacity substantially, while greatly facilitating access to recorded data, both within organizations and across boundaries that separate them. In addition, computerization creates a new class of record keepers whose functions are technical and whose contact with the suppliers and users of data are often remote.
>
> . . . [T]he net effect of computerization is that it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems.[26]

As alluded to above, the HEW Committee focused on an important point that was not considered by Westin and Baker—the creation of a class of trained data managers to manipulate the computers, and the implications this might have on citizens' rights. Computerized record keeping, coupled with the increased mobility of our population, clearly has reduced the interpersonal character of decisionmak-

25. *See* Browne, *Security in Computer Networks*, in NATIONAL BUREAU OF STANDARDS, APPROACHES TO PRIVACY AND SECURITY IN COMPUTER SYSTEMS 32-37 (NBS Special Pub. No. 404, 1974).

26. HEW, *supra* note 5, at xix-xx.

ing. Today's merchant or banker does not decide whether an applicant is credit worthy on the basis of an interview and an assessment of his present assets. Rather, he may check with the Bank of America computer, housing that person's entire credit history as well as 1.9 million others.[27] In a very real sense the managers and computer personnel at the databank, who most typically have never met the file subject, control his credit life. Whether he obtains the necessary credit will depend on whether these persons have recorded all his past transactions completely and accurately. Thus the HEW report justifiably addresses this situation as a potential problem, stating: "If we can comfortably assume that computers will not take control of anything on their own volition, we may still feel some disappointment that the application of computers will tend to remain in the hands of trained specialists whose competence is primarily in data processing rather than in the fields that data processing serves."[28]

Unfortunately, the HEW report does not include concrete examples of the findings from their hearings. For the most part, we are asked to accept on faith the needs perceived and the solutions suggested. This is the greatest shortcoming of this report. I am persuaded that the approach it suggests is both necessary and sound because my personal experience has demonstrated to me that the factual underpinning exists. I attended several days of the Committee's hearings as an observer and heard some of the startling revelations of record keepers regarding their practices. Further, in my own field research in this area I have seen time and again the types of abuses and lack of sensitivity on the part of data managers that the Committee is trying to combat.

II. Remedies

The privacy solutions offered by each book are remarkably similar in philosophy as well as approach, both concluding that a legislative resolution of the problem is best. However, the solutions suggested by Westin and Baker are too general and too vague to be of much

27. A. Westin & M. Baker, *supra* note 3, at 119.
28. HEW, *supra* note 5, at 22.

assistance.[29] They simply restate the same basic principles—that rights of access and challenge must be afforded, and rules of confidentiality and data sharing must be effectuated. Perhaps the authors were trapped by their own desire to be all-inclusive. They admit, and I concur, that no single law can solve the privacy-computer problem.[30] However, their field research covered a wide variety of different areas. The logical approach would have been to tackle each area separately, detailing the possible measures that might be applied there. This they clearly were unable to do—through no fault of their own. As illustrated by the HEW report dealing only with that agency's own record keeping practices, devising solutions for the problems of a particular agency is a monumental task. It would be unrealistic to expect Westin and Baker to deal in detail with data handling and storage procedures for each of the organizations they visited, given the time frame in which they were working.

The remedies portion of *Databanks in a Free Society* also suffers from the fact that virtually *total* reliance is placed on a statutory approach. Rejecting a judicial solution as too slow and unlikely to be achieved and not attempting to make any administrative suggestions (except the use of an information trust agency, an idea that has been discussed at least since 1968),[31] the authors place their faith in the legislature.

Throughout their book, Westin and Baker argue that unlike their predecessors they are taking a realistic view of the situation, based on empirical fact. Experience with the legislative approach, however, indicates that exclusive reliance on that mechanism is unrealistic. The first major federal privacy legislation did not appear until the 1970 Federal Fair Credit Reporting Act.[32] Although several privacy bills

29. For example, the authors make the following statement, without any elucidation or suggestions on implementation.

> Where the fault lies with insufficiently clear or detailed policy directives, these must be reformulated. Where the fault is with inadequate administrative supervision and enforcement mechanisms, those must be revised. And where technological safeguards are required to give effect to those confidentiality rules, society has a right to insist that safeguards be installed appropriate to the dangers involved.

A. WESTIN & M. BAKER, *supra* note 3, at 373.

30. *Id.* at 350.

31. *Hearings on Computer Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary,* 90th Cong., 2d Sess., pt. 2, at 310-11 (1968).

32. Fair Credit Reporting Act, 15 U.S.C. §§ 1681-81t (1970).

were introduced after that act and despite the public outrage and extended hearings in 1971 over army surveillance,[33] it was not until the recent revelations of government spying and record keeping in connection with the Watergate scandal that the Congress again attempted to act. This most recent law is the Privacy Act of 1974,[34] which provides a code of information practices for government record-keeping and establishes a privacy board to oversee the administration of that code. But the powers of that board appear weak, and it is unclear what actual effect the law will have. Moreover, its limited scope attacks only one aspect of the privacy problem, and further regulation is needed.

Unlike Westin and Baker, the HEW report sets out specific recommendations for action, as well as proposing a "Code of Fair Information Practices"[35] which would include principles providing that:

> 1) no record keeping system be kept a secret;
>
> 2) file subjects be given access to their files and information regarding how it is used;
>
> 3) a method be provided to prevent information collected for one purpose from being used for another without the file subject's consent;
>
> 4) procedures exist for ways to correct inaccurate files; and
>
> 5) data keepers assure the reliability of their information and prevent its misuse.

Although the HEW Committee also concludes that a legislative resolution is the best, it goes on to recognize that legislatures are not always quick to act and, as a result, recommends interim administrative safeguards. In short, the HEW report provides a workable guide for action.[36]

In keeping with its more detailed approach, the HEW Commit-

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

34. Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974).

35. HEW, *supra* note 5, at 41.

36. In fairness to Westin and Baker it should be pointed out that the task given to them by the National Academy of Sciences and the Russell Sage Foundation emphasized fact finding on the "actual effects" of modern technology on "creating, sharing, and using files on individuals," rather than on devising solutions to perceived problems. A. WESTIN & M. BAKER, *supra* note 3, at xix. In contrast, the charge to the HEW Committee was, among other things, to make recommendations on "[s]afeguards that might protect against potentially harmful consequences," and on "[m]easures that might afford redress for any harmful consequences." HEW, *supra* note 5, at ix.

tee discusses issues not even alluded to in the other book. For example, emphasis is placed on the need for informed consent (informing an individual whether he is legally required to give data and the specific consequences of providing that data) and on restricting the transfer of data between organizations unless the individual about whom the data pertains consents or the transferee system demonstrates that it adheres to the same privacy safeguards which govern the transferor system. These suggestions, as well as others set out in the notes,[37] are based on what is described as a principle of mutuality in record keeping. "A record containing information about an individual in identifiable form must . . . be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it."[38]

A further example of the refined character of the approach taken in the HEW report is its attempt to distinguish between administrative and statistical systems for purposes of applying safeguards. The different purposes behind the creation of each of these records indicate that different solutions to potential privacy problems may be appropriate. Illustratively, since by definition a system maintained exclusively for statistical reporting and research is developed not for the benefit of the individual file subjects but to serve the ends of the agency desiring the statistics, it was felt that any personal data stored therein should be protected by statute from compulsory disclosure in identifiable form.[39] At the same time, there was no requirement which guaranteed data subjects access to their files. Since their files were not designed to affect their rights there was no need to afford them a means of monitoring the data keeping practices. Whether the reader agrees that the suggested safeguards are appropriate is not the issue, the fact is that by engaging in such a refined approach, the HEW Committee aptly demonstrates one way of attacking the privacy problem created by modern record keeping practices. It is the careful attention given to issues such as the above that distinguishes this book and makes it invaluable.

37. Among other things, the HEW Committee suggests that a log be maintained on those persons who have access to each file so that the subject can better monitor the use of his data. HEW, *supra* note 5, at 56. In addition, a recommendation is made that individual file subjects be notified before the record keeper complies with any subpoenas requesting access. *Id.* at 63.

38. *Id.* at 41.

39. *Id.* at 96.