Michigan Law Review

Volume 67 | Issue 6

1969

Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society

Arthur R. Miller
University of Michigan Law School

PERSONAL PRIVACY IN THE COMPUTER AGE: THE CHALLENGE OF A NEW TECHNOLOGY IN AN INFORMATION-ORIENTED SOCIETY

Arthur R. Miller

TABLE OF CONTENTS

PERSONAL PRIVACY IN THE COMPUTER AGE: THE CHALLENGE OF A NEW TECHNOLOGY IN AN INFORMATION-ORIENTED SOCIETY

*Arthur R. Miller**

> Probably the most distinctive characteristic of classical utopian designs is the basic "humanitarian" bent of their value structures. . . .
>
> And perhaps the most notable difference to be found between the classical system designers and their contemporary counterparts (system engineers, data processing specialists, computer manufacturers, and system designers) consists precisely in the fact that the humanitarian bent has disappeared. The dominant value orientation of the utopian renaissance can best be described as "efficiency" rather than "humanitarianism."[1]

I. INTRODUCTION

THE almost geometric expansion of published materials in recent years indicates that our society is experiencing an information, as well as a population, explosion. Fortunately, a technological revolution, centered around a species of machines generically referred to as "the computer," is in progress and promises to increase man's capacity to accumulate, manipulate, store, retrieve, and transmit information. Dramatic confirmation of the dimensions of this new technology's capability is provided each time man reaches toward the moon and the planets beyond. Our ability to thrust an object countless miles into space would be of limited value without the associated technological resources to measure and manipulate its flight, monitor the performance of its various systems and the body functions of the people inside it, and com-

* Professor of Law, University of Michigan. A.B. 1955, University of Rochester; LL.B. 1958, Harvard University.—Ed.

The author would like to thank Mr. Barry B. Boyer, currently a third-year law student at the University of Michigan Law School and one of the Article and Book Review Editors of the *Michigan Law Review*, for his extensive contributions to this Article. He gathered much of the documentation that appears in the footnotes and provided numerous substantive suggestions. In addition, his assistance in collecting, revising, and elaborating many of the author's past expressions on this subject—contained in various speeches, panel discussions, Senate subcommittee hearings, and several specialized articles published in nonlegal periodicals—was invaluable. Were it not for Mr. Boyer's efforts, it is doubtful that this Article would have been written. An additional note of appreciation is extended to Mr. Frederick W. Lambert, also a third-year law student at the University of Michigan Law School, for his valuable research assistance. As is usual in these matters, the author reserves credit for all heresies appearing in these pages.

1. R. BOGUSLAW, THE NEW UTOPIANS, A STUDY OF SYSTEM DESIGN AND SOCIAL CHANGE 202 (1965).

pute instantaneously where it is, where it will be, and when and where it will return to earth.

A number of contemporary prophets have predicted that the advent of the new information transfer technologies will prove to be as significant as the invention of movable type.[2] As they perceive the future, information will not be preserved as alphabetical imprints or pictures in a book but rather as holes in punch cards, magnetic fields on tapes or discs, electrical impulses moving through the memory core of a computer, and, perhaps, radiations generated in vats of complex chemicals.

But this transition is bound to be accompanied by abrasive dislocations and deviations from traditional norms. For example, in recent years there has been a growing awareness of the effects that certain applications of computer technology may have on individual privacy. The ponderousness of movable-type technology inhibited man's urge to collect and preserve information about his peers. But many people have voiced concern that the computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been stored in it, may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances, and our associations will be bared to a wide range of observers.[3] These fears have been exacerbated by the clarion in some quarters for the

---

2. A. CLARKE, PROFILES OF THE FUTURE 265-79 (1962); M. MCLUHAN, THE GUTENBERG GALAXY 11-279 (1962); H. KAHN & A. WEINER, THE YEAR 2000, at 88-98, 348-49 (1967); A. WESTIN, PRIVACY AND FREEDOM 158-68 (1967); *Hearings on the Computer and Invasion of Privacy Before a Subcomm. of the House Comm. on Govt. Operations*, 89th Cong., 2d Sess. 7 1966) (statement of Vance Packard) [hereinafter *House Hearings on the Computer and Invasion of Privacy*]; Russel, *Playing for Fun*, PLAYBOY, April 1969, at 110, 174. *See also* note 249 *infra*.

An example of the scientific community's views of the impact of the computer on our society is the following excerpt from a speech by Dr. Glenn T. Seaborg, Chairman of the Atomic Energy Commission, reprinted in *Hearings on Computer Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 1st Sess. 248 (1967) [hereinafter *Senate Hearings on Computer Privacy*]:

> Springing from our Scientific Revolution of recent decades is what is being called our "Cybernetic Revolution." This revolution which, comparatively speaking, is only in its infancy today amplifies (and will to a large extent replace) man's nervous system. Actually, this is an understatement because computers amplify the collective intelligence of men—the intelligence of society—and while the effect of the sum of men's physical energies may be calculated, a totally different and compounded effect results from combining facts and ideas . . . . Add this effect to the productive capacity of the machine driven by an almost limitless energy source like the atom and the resulting system can perform feats almost staggering to the imagination. That is why I refer to cybernation as a quantum jump in our growth.

3. V. FERKISS, TECHNOLOGICAL MAN 227 (1969); Miller, *The National Data Center and Personal Privacy*, THE ATLANTIC, Nov. 1967, at 53; *cf.* Osborn v. United States, 385 U.S. 323, 353 (1966) (Justice Douglas, dissenting); Lopez v. United States, 373 U.S. 427, 450 (1963) (Justice Brennan, dissenting). *See* also notes 141-44 *infra*.

establishment of a National Data Center, by the emergence of criminal-intelligence data centers and computer-based credit-reporting services, and by the hypnotic attraction for digital record-keeping being exhibited throughout government, industry, and academe.

The purpose of this Article is to survey the new technology's implications for personal privacy and to evaluate the contemporary common-law and statutory pattern relating to data-handling. In the course of this examination, it will appraise the existing framework's capacity to deal with the problems created by society's growing awareness of the primordial character of information.[4] The Article is intended to be suggestive; any attempt at definitiveness would be premature. Avowedly, it was written with the bias of one who believes that the new information technology has enormous long-range societal implications and who is concerned about the consequences of the notion that man shapes his tools and then they shape him. The assumption throughout is that the computer is not simply a sophisticated indexing machine, a miniaturized library, or an electronic abacus; it is the keystone of a new communications medium that eventually will have global dimensions. Thus, it would be overly simplistic to examine the computer-privacy issue from the perspective of a particular machine or group of machines operating in a federal office building, in the headquarters of one of the nation's major industrial complexes, or in the recesses of a great university. Indeed, the analogy between the forces that gave rise to the multifaceted regulation of the airlines, railroads, radio, and television and the problems that already are generating pressure for the regulation of computer transmissions and facilities seems obvious. It is against the template of the potential need for a comprehensive regulatory scheme embracing some uses of the technology in both the public and private sectors that the question of protecting individual privacy in the computer age must be placed.

II. The Cybernetic Revolution

A. *The New Technology*

Since the first commercial digital computers were introduced shortly after World War II,[5] there has been a rapid proliferation and

4. The computer's threat to personal privacy is beginning to attract attention in foreign countries also. *See generally* Conservative Research Department, Computers and Freedom (1968) (England); National Council For Civil Liberties, Privacy Under Attack (1968) (England); Ontario Law Reform Commission, Report on Protection of Privacy in Ontario (1968); N.Y. Times, April 21, 1969, at 50, cols. 7-8.

5. For a concise history of the early development of computers, *see* J. Bernstein, The Analytical Engine 50-80 (paper ed. 1966).

sophistication of data-processing devices, especially in this country.[6] During this relatively brief period of time, the burgeoning family of machines has outgrown its original role as an electronic calculator performing arcane tasks for scientists and has become the cerebrum of expansive multipurpose and multimedia information systems in business, government, and education. It is easy to understand why so many sectors of society have embraced the new technology so eagerly. The computer's basic ability to store vast quantities of data and to retrieve or perform operations upon it in accordance with a programmed set of instructions[7] enables the technology to be employed fruitfully in virtually any activity that requires the systematic manipulation of large bodies of information.

Perhaps the most dramatic aspect of the computer age has been the rate at which the technology has evolved. Computer "hardware"—loosely speaking, the physical elements of the machine—already has experienced three generations of development.[8] As a result, the present-day computer designer is able to draw on a variety of memory devices including relatively slow storage media such as punch cards or magnetic tape, faster devices such as discs, and, more recently, magnetic cores[9] that enable a computer to

6. At present there are over 40,000 computers in operation in the United States. This figure represents about 65 per cent of the total number of computers in the world. NEWSWEEK, Jan. 29, 1968, at 57. A more recent estimate puts the "computer population" at 67,200. Russel, *supra* note 2, at 116.

7. The following simplified description of a computer's capabilities was given by Dr. Emanuel R. Piore, Vice President of IBM, in *Senate Hearings on Computer Privacy* 118:

> The memory device, the storage device of the computer, contains a large number of cells. Each of these can hold a single piece of information, such as a number or a name in code. Each cell . . . has a numerical address.
>
> . . . .
>
> To process data, the computer can perform very rapidly such functions as these: It can move a piece of information from an input device to a memory cell; add the number in one memory cell to a number in another cell; send a copy of information in a memory cell to an output device.
>
> But before a computer can do anything whatsoever, someone must give it an organized sequence of instructions called a program.
>
> Each instruction specifies one of the basic functions which the computer can perform. And each instruction, like each piece of data, can be stored . . . in a memory cell of the machine.
>
> A user can put a program into the machine—and thus gain command of it—in two ways, and only two. He can put it in by hand, through a set of keys and buttons at the console of the central part of the machine. Or he can put in a program which in turn can bring in a second program from any input device, and give the second program temporary control.

A more detailed description of the workings of the computer, in terms intelligible to the layman, may be found in Campbell, *How the Computer Gets the Answer*, LIFE, Oct. 27, 1967, at 60. For a simplified description of programming techniques, *see* J. BERNSTEIN, *supra* note 5, at 3-17.

8. For a brief description of the different computer "generations," *see* Taylor, *Computer Systems*, in COMPUTERS AND THE LAW 40 (American Bar Assn. Standing Comm. on Law & Technology, 2d ed. 1969).

9. The choice of a particular storage medium will largely depend upon the nature

retrieve data at the rate of a few nanoseconds (billionths of a second) per bit of information.[10] Information-handling capacity is another characteristic of computer hardware that has changed dramatically over the years. As the requirements of modern science and industry provide the incentive for the hardware manufacturers to produce memories that can accommodate a billion bits of information in a single system, researchers are turning to exotic storage media using devices such as lasers,[11] photochromic materials responsive to ultraviolet light,[12] and complex chemical solutions.[13]

The "software" of the electronic age—the programs or instructions

---

of the tasks that a given computer system is expected to perform. *See* Mayer, *Computers on the Brain*, ESQUIRE, Jan. 1969, at 100, 103, 148:

> The central distinction between different kinds of black boxes is whether they are primarily memory ("storage and retrieval") systems, which is what business needs, or primarily computational systems for research use. The computer which prepares the payroll simply churns forward through lists of names, slotting in as needed appropriate changes in salary data, hours worked, percentages for deduction, etc. Though the memory function is vital, the memory device can conveniently be a simple reel of magnetic tape, which gives a predetermined sequential access rather than random access . . . .
>
> Other activities need the computer as a kind of super filing system, so decisions can be made on the basis of full information. . . . For this purpose, a memory on reels of magnetic tape is inadequate because the machine must do considerable checking back on already processed data. But the electronic speeds of . . . magnetic cores are not required; a mechanical whirling drum or disc with magnetic coatings will be sufficiently random and sufficiently fast. . . .
>
> Finally, a very different black box is required if the machine is to be used for immensely rapid computation of immense numbers of variables—to control a rocket, or to guide an airplane into a socked-in airport . . . . This system demands an enormous random-access memory delivering its information at maximum speed, because so many possible different programs must be available for processing depending on the results of prior computation.

10. Mayer, *supra* note 9, at 103. A nanosecond is to one second as one second is to thirty years. Ream, *New Directions in Computer Utilization*, in COMPUTERS AND COMMUNICATIONS—TOWARD A COMPUTER UTILITY 3, 6 (1968).

11. A working model of a system for storing information on plastic tape in the form of minute craters burned by a laser beam is described in A. WESTIN, PRIVACY AND FREEDOM 167 (1967). This process permits the storage of 645 million bits of data per square inch of tape, recorded at the rate of 12 million bits per second. A bit of information is described as follows in Furth, *Computers*, in COMPUTERS AND THE LAW 26 (American Bar Assn. Standing Comm. on Law & Technology, 2d ed. 1969):

> Basically information is represented in the various components of a computer in a form which requires only two distinct states of a storage position: ON or OFF, 0 or 1. Such a system of representation is called "binary" and each position of storage is referred to as a "binary digit" or a "bit."

12. Univac has advertised that it has developed "a non-fatiguing photochromic material . . . that can be used as a reservoir for computer information. Exposure of this material to ultraviolet light records the information. The information can then be read with a low-intensity light beam . . . ." The potential reductions in storage space made possible by this process have led the company to speculate: "Someday it may be possible to store the medical records of every American in the space of a cold capsule. Or the tax records of the nation may fit in one file cabinet." TIME, Sept. 27, 1968, at 51.

13. *Cf.* Diebold, *The New World Coming*, SAT. REV., July 23, 1966, at 17: "Looking ahead, we see important changes in technology such as chemical memories; fluid and pneumatic systems that have instantaneous response; ability to store images, graphs, drawings and photographs, and to transmit them around the world."

that control the storage, retrieval, and manipulation of information within the huge computer memories—has undergone a comparable transformation. Programs no longer are laboriously derived from highly personal and detailed computer languages useful and intelligible to only a few. Today's common programming languages such as FORTAN and COBOL are becoming the lingua franca of the new technocracy, enabling extraordinarily complex information-handling tasks to be performed in response to relatively simple instructions understood by virtually all machines. Sophisticated programs have been designed to edit raw data, to perform different operations in sequence with the contours of each step dictated by the results of the preceding process, to permit virtually instantaneous random access to any given item of information stored in the memory, and to shift a computer's information-handling capacity among a number of users so rapidly that each can proceed with his work almost as if the machine were reacting only to his commands. Although there still are significant problems of system compatibility to be solved, it may not be long before computers are communicating with each other and with their operators in much the same manner as their operators communicate among themselves. Indeed, there are some programs that enable machines to "learn" as part of a process that is very similar to the socratic method of teaching.[14]

14. The following dialogue between man and machine is given in Fano, *The Computer Utility and the Community*, in COMPUTERS AND COMMUNICATIONS—TOWARD A COMPUTER UTILITY 39, 48 (1968). The computer's responses are given in upper case letters, while those of the human operator are in lower case.

WHICH SCRIPT PLEASE
arithm
PLEASE BEGIN
The area of a sphere is pi times the diameter of the sphere squared.
The area of a circle is pi times the radius of the circle squared.
The diameter of an object is twice the radius of the object.
The radius of a ball is 10.
What is the area of the ball
THE ASSUMPTION THAT BALL IS SPHERE AND OBJECT IS CONSISTENT—SHALL I GO ON? yes
IT'S 1256.6359
What is the diameter of the ball
IT'S 20.
The radius of a dish is 10.
A dish is an object.
What is the diameter of the dish
IT'S 20.
What is the area of the dish
THE ASSUMPTION THAT DISH IS SPHERE IS CONSISTENT—SHALL I GO ON? no
THE ASSUMPTION THAT DISH IS CIRCLE IS CONSISTENT—SHALL I GO ON? yes
IT'S 314.15899
The radius of a globe is 10.
A globe is a sphere.
What is the area of the globe

Each rapidly succeeding stage of hardware-software development has been accompanied by substantial reductions in the cost of information-processing,[15] and has opened new vistas for the applica-

THE ASSUMPTION THAT GLOBE IS OBJECT IS CONSISTENT—SHALL I GO ON? yes
IT'S 1256.6359
The radius of a thing is 10.
A sphere is an object.
A thing is a sphere.
What is the area of the thing
IT'S 1256.6359
Thank you
YOU'RE QUITE WELCOME, COME AGAIN

[The answers above are erroneous past the fifth digit (for the smaller number) and past the sixth digit (for the larger). The error is apparently based upon an approximation of pi which is incorrect past the fourth decimal. (3.1415927, not 3.1415899, is the correct approximation to seven places.) For reasons peculiar to ease of computer expression, the programmer may not have intended accuracy past the fourth decimal, but if so, the program should have called for an answer with fewer digits.—Ed.] Professor Fano concludes:

> The important points to observe are that the information is provided in arbitrary order and in a relatively free format and that the program can make nontrivial inferences from the available information and generate reasonable conjectures in the absence of complete information. The program is being instructed in the way that people like to instruct other people, that is, by making statements and answering questions.

Id. at 47. For the view that man and machine ultimately will become indistinguishable, *see* R. LANDERS, MAN'S PLACE IN THE DYBOSPHERE (1966).

Professor Layman E. Allen, Research Associate Prudence C. Abram, and this writer have produced a computer-based dialogue to assist in teaching part of a first-year course in civil procedure. Although it was demonstrated at the 1968 annual meeting of the American Association of Law Schools and tested during March and April 1969 on approximately 150 first-year students at the University of Michigan Law School, it still must be considered experimental. Nonetheless, preliminary evaluation indicates a high level of receptivity on the part of the students and reasonable success in terms of educational values. N.Y.L.J., March 31, 1969, at 1, col. 1.

15. Diebold, *The New World Coming*, SAT. REV., July 23, 1966, at 17:

> Between 1963 and 1972—a single decade—there will be a decrease of 85 per cent in the cost of completing a typical data-processing job. During this period, the cost of storage by magnetic tape will go down by 97 per cent; the cost of image storage by 96 per cent; and communications line costs, because of increased speeds of transmission, will decrease by 50 per cent.

Even experts in the data-processing field frequently underestimate the potential market and rate of change; *see, e.g., Hearings on the Coordination and Integration of Government Statistical Programs Before the Subcomm. on Economic Statistics of the Joint Economic Comm.*, 90th Cong., 1st Sess. 3, 7 (1967) (statement of Dr. Edgar S. Dunn, Jr., Research Analyst, Resources for the Future, Inc.) [hereinafter *Hearings on Statistical Programs*]:

> [T]here is a tendency to grossly underestimate the value of new systems in the information field. Back in 1950 . . . IBM undertook a careful market study to determine whether they should try to get into [the computer] market. They concluded that there was a market for something like five or six of these machines in the United States. . . . With [sic] 5 years 1,275 machines had been sold and the entire industry was turning to the design of a whole new generation of computers. . . . [B]efore [the National Academy of Sciences] first acquired a Xerox machine they made a careful study of the staff to estimate its use. . . . Within a period of less than 2 years they had exceeded their estimate by something like a factor of 10 and had gone through two changes of equipment.

See also Burck, *The Computer Industry's Great Expectations*, FORTUNE, Aug. 1968, at 93.

tion of computer techniques. Among the well-publicized recent innovations are computerized medical checkups,[16] tax return preparation,[17] date-matching, and airline reservations.[18] It is perhaps less well known that computers also are being used to prepare astrological horoscopes,[19] to furnish religious leaders with statistical profiles of their congregations,[20] and to help teach basic educational skills in the ghettos. The possibilities for the future appear to be limited only by the ingenuity of the designers and programmers.[21]

---

16. Stevens, *Now—The Automated Physical Checkup*, READERS DIGEST, July 1966, at 95. *See also* Fleming, *The Computer and the Psychiatrist*, N.Y. Times, § 6 (Magazine), April 6, 1969, at 44; *How Computers Help MDs Diagnose*, BULL. INTERUNIVERSITY COMMUNICATIONS COUNCIL (EDUCOM), April 1966, at 3-6.

A related aspect of the computerization of medical files is the trend toward networking medical data systems so that a physician will have immediate access to a patient's complete medical record, regardless of where the patient is when he is taken ill. The U.S. Public Health Service currently is making a detailed study of the problems of interconnecting the nation's hospitals into a single computer network. N.Y. Times, June 18, 1968, at 47, col. 6. *See also* Freed, *A Legal Structure for a National Medical Data Center*, 49 B.U. L. REV. 79 (1969); Freed, *Legal Aspects of Computer Use in Medicine*, 32 LAW & CONTEMP. PROB. 674 (1967); Sarnoff, *No Life Untouched*, SAT. REV., July 23, 1966, at 21.

This type of technique also is being used to produce initial medical histories. Expenditure of doctors' time in performing a relatively ministerial task is reduced, and there is some evidence that the patient is more open with the computer than he would be with the doctor. Wall St. J., May 8, 1969, at 1, col. 5.

17. *See generally* Halstead, *Use of Computers in Preparing Tax Returns*, in COMPUTERS AND THE LAW 77 (American Bar Assn. Standing Comm. on Law & Technology, 2d ed. 1969). The Internal Revenue Service, on the other hand, is using computers to detect inconsistencies in individual tax returns. *Hearings on Statistical Programs* 23 (statement of Professor Richard Ruggles).

18. Star, *The Computer Data Bank: Will It Kill Your Freedom?*, LOOK, June 25, 1968, at 27, 28. The implications of this computer application are discussed in text accompanying notes 103-04 *infra*.

19. *That New Black Magic*, TIME, Sept. 27, 1968, at 42: "New York's TBS Computer Centers Corp. now cranks out 20-page personal horoscopes for a mere $15, the electronic brain taking only a minute to compute a life history that flesh-and-blood astrologers need a week to prepare."

20. TIME, March 29, 1968, at 92:

> This past winter, at their monastery near St. Louis, the Roman Catholic Redemptorist Fathers put into operation an electronic data-processing service designed to provide "a 71-facet view of each practicing Catholic." Pastors who want to make use of the service must distribute a questionnaire to their faithful, then wait for the Redemptorists to feed the answers to an IBM System 360 computer. The 180-page printout that the machine delivers gives the pastor a cybernetic summary of his parishoners' religious attitudes.

21. Even the Congress of the United States may be computerized. *See* Wall St. J., March 27, 1969, at 23, col. 2:

> House leaders are considering [a] computerized "information retrieval" system that would store and serve up data on legislation, the budget and other topics. The House Banking Committee installed a rudimentary version of such a system in January; it feeds information about banking legislation into a Library of Congress computer, which provides data via teletypewriter when the committee staff requests it.

Cf. H.R. 404, H.R. 5522, 91st Cong., 1st Sess. (1969); INFORMATION SUPPORT PROGRAM BUDGETING AND THE CONGRESS (1968). Chartrand, *Computer Technology and the Legislator*, in COMPUTERS AND THE LAW 90 (American Bar Assn. Standing Comm. on Law &

One of the pioneers of new programming techniques predicts that it soon will be cheaper to store a page of English text in a computer than to preserve it on paper,[22] a possibility that has startling ramifications for the publishing and printing industries.[23]

B. *The Development of Time-Sharing*

The growth in concern over the interrelationship between computers and personal privacy directly parallels the development of increasingly efficient methods of utilizing data-processing equipment. When computers were first marketed commercially, they were designed to handle data-processing jobs sequentially—to "batch process" different tasks. But this mode of operation leaves the heart of the machine idle during the period in which the data is being put into the system and again during the printout phase. In addition, the machines are so fast that few organizations were able to generate enough work to keep them busy. Thus, it was apparent that customers were using only a fraction of the computer's potential; in turn, the low level of computer use was a primary factor in the high cost of machine processing.[24]

The industry's solution was to connect several input-output terminals to the same machine, and to design a complex program that would enable the computer to switch its attention among the commands of the various users at very high speed.[25] Thus, some users could be inputting data, others receiving the computer-pro-

---

Technology, 2d ed. 1969). *See generally* Detroit Free Press, Dec. 14, 1968, § B, at 14, col. 1 (computer used to check chromosomes); Detroit News, Oct. 27, 1968, § H, at 1, col. 1 (computer used to appraise real estate); N.Y. Times, Oct. 10, 1968, § C, at 30, col. 1 (computer used to study molecular interaction); Wall St. J., Oct. 25, 1966, at 1, col. 1 (computer used in electronic sketching of technical drawings).

22. Fano, *supra* note 14, at 39.

23. *See, e.g.*, M. McLUHAN, THE GUTENBERG GALAXY 265-79 (1962). The potential implications of computers on copyrighted works also are causing a great deal of difficulty in the current attempt to revise the copyright laws. *See, e.g., Hearings on S. 597 Before the Subcomm. on Patents, Trademarks, and Copyrights of the Senate Comm. on the Judiciary*, pt. 1, 90th Cong., 1st Sess. 190-213 (1967). *See also* Miller, *Computers and Copyright Law*, MICH. ST. B.J., April 1967, at 11; Note, *Copyright Protection for Computer Programs*, 64 COLUM. L. REV. 1274 (1964); Recent Development, *Copyright—Protection Denied to Verbal Expression of Simple Subject Matter*, 67 MICH. L. REV. 167, 174-78 (1968); Project, *New Technology and the Law of Copyright: Reprography and Computers*, 15 UCLA L. REV. 931 (1968). The copyright revision bill currently being considered by Congress is S. 543, 91st Cong., 1st Sess. (1969).

24. *See, e.g.*, Irwin, *The Computer Utility: Competition or Regulation?*, 76 YALE L.J. 1299 (1967): "Under the traditional batch-processing method, access to the computer was limited to one user at a time, although even the most complex scientific problems consumed less than 10% of the computer's capacity."

25. Main, *Computer Time-Sharing—Everyman at the Console*, FORTUNE, Aug. 1967, at 88:

duced responses to their requests as output, and still others having their data processed by the system's central unit at the same time. This "time-sharing" procedure enabled users to employ the full capacity of the machine, and it gave each user the functional equivalent of his own computer at a greatly reduced cost. However, the simultaneous exposure of several distinct bodies of data in one information system created the risk that one user would gain access to another's files, either by accident or by design, and thus compromise the privacy of fellow users or of third parties whose personal data was being stored or manipulated in the time-share system.[26]

The next step in the maturation of time-sharing was to move the input-output terminals away from the central processor, to disperse them into strategic locations such as the regional offices of a national corporation or an important customer's place of business, and to link them with the computer's memory unit by communications channels. This seemingly obvious development has enormous implications for the development of information transfer capacity. Observers of recent trends in data-processing assert that remote-access time-sharing is merely the first stage in the ultimate amalgamation of computer and communications technologies.[27] They

---

[A] time-sharing computer requires an "executive" or "control" program. . . . The executive keeps the whole system running efficiently and in a sequence determined by priorities. It assigns actual computing time among its many users, say 200 milliseconds for each client on line. . . . The executive fetches the client's data or programs out of storage, and puts them back there once the client is finished. It also can prevent one user from interfering with the program of another and altering it or wiping it out—a facility that goes by the technical name of "memory protection." It keeps a record of who uses the machine, makes corrections, even gives helpful hints to unskilled users . . . .

. . . The executive—the critical item of software in a time-sharing system—is an enormously complicated set of instructions permanently stored in the high-speed core memory of the computer.

26. *See* Mayer, *Computers on the Brain*, ESQUIRE, Jan. 1969, at 100, 103:

M.I.T.'s Project M.A.C. is in process of moving from a system which permits about thirty access terminals to be used at once to a system which will have place for about fifty. "Its complexity," says [Robert M. Fano, the project's organizer] ". . . is at the limit of human understanding." Part of this complexity, incidentally, is required by the need to maintain the security and privacy of each user's programs. "Experience has shown," Fano wrote grimly in a recent issue of the *Journal of Engineering Education*, "that vandalism within a time-sharing system and the forging of user accounts are to be expected in universities as well as elsewhere."

See also text accompanying notes 74-83 *infra*.

27. *See, e.g.*, Bauer, *Computer/Communications Systems: Patterns and Prospects*, in COMPUTERS AND COMMUNICATIONS—TOWARD A COMPUTER UTILITY 13 (1968):

During this decade, a significant process is occurring—the marriage of two important technologies: computers and communications. The history of modern technology records few events of the importance and scope of this process—two giant industries, proceeding in the past on two relatively independent courses, are now on a path of confluence. Each technology is having and will have a great leavening effect on the other.

It has been estimated that half of all computer usage in the next decade will involve

also forecast that the result will be an "almost biological" growth of a natural monopoly[28] as small data-processing systems become integrated into one or more national and international networks.

The intersection of the two technologies already has become apparent in the context of the telephone system, which currently carries the bulk of "on-line" data transmissions along leased lines.[29] Telephone officials are beginning to recognize the significant parallels between the *modus operandi* of their system and that of the remote-access computer system.[30] Indeed, the telephone system is in the process of converting its electromechanical switching devices to electronic equipment[31] and eventually even voice transmissions will be sent over the telephone lines in digital form.[32] These changes will give the telephone system the basic attributes of a data-processing center.[33] To press the analogy between the two technologies

communications systems. Loevinger, *Federal Regulation of Computers*, in COMPUTERS AND THE LAW 101, 104 (American Bar Assn. Standing Comm. on Law & Technology, 2d ed. 1969).

28. *House Hearings on the Computer and Invasion of Privacy* 121 (statement of Paul Baran, computer expert for the Rand Corporation).

29. Federal Communications Commission Notice of Inquiry, Docket No. 16,979, reprinted in *Senate Hearings on Computer Privacy* 89.

30. Romnes, *Managing the Information Revolution*, BUSINESS AUTOMATION, Aug. 1966, at 31:

> The telephone system is itself a computer. Its components are dispersed across the continent but they work as one. Equipped with more than 90 million input-output stations, this enormous computer can be commanded to provide any one of the 3 million billion "answers" it takes to connect any one of its stations—telephones—with any other and do it in a matter of seconds. It is a "real time" operation by definition and design.
>
> It should not be surprising, then, that the communication and computer technologies should have much in common. Indeed, our newest electronic switching systems, like computers, are internally programed and are endowed with the same kind of quasi-human memory ascribed to commercial computers.

31. Irwin, *supra* note 24, at 1301.

32. *Why Ma Bell Chops Up the Signals*, BUSINESS WEEK, Jan. 13, 1968, at 82. The conversion to digital transmission will greatly improve the capabilities of the telephone system as a data carrier:

> A regular telephone line used in home and office does well if it carries 1,200 to 2,400 bits of data per second, enough for a Teletypewriter but slow for computers or facsimile transmission. By comparison, one voice channel equivalent on a digital transmission system carries 56,000 bits per second—about 22 times as much data as a normal voice channel.

Id. at 84. *See also* note 422 *infra*.

33. *See Senate Hearings on Computer Privacy* 158 (statement of Paul Baran, computer expert for the Rand Corporation) (emphasis in original):

> At present, these electronic switches are not believed to be more economical than their electromechanical switch counterparts. But their prime advantage lies in the *new additional services* that they offer because of the general computer nature of the control mechanism of the switching center. For example, it will be possible to dial only two digits to reach the few numbers that you call often. It will be possible to relay a call to another telephone if you are temporarily away.

The present reluctance of the Bell System to enter the data-processing field may be due to an antitrust consent decree. Titus, *Computers, Communciations, and the FCC*, 10 COMMUNICATIONS OF THE ACM 62 (1967).

further, one of the key concepts of computer time-sharing—the ability to switch messages among different users at very high speeds—has long been a mark of the communications common carriers.[34] Other communications media—private microwave systems,[35] the telegraph,[36] communications satellites,[37] and even the community antenna television systems[38]—are not far behind the telephone companies in their ability to provide mass transmissions of digital data. As computer networks multiply, both the data-processing and communications industries surely will tailor their systems to obtain the full benefit of the interaction between the two.

In light of the constantly broadening range of computer applications and the development of remote-access time-sharing, it does not require clairvoyance to predict that eventually there will be some form of national computer "utility" providing a variety of data-processing services to everyone, perhaps through the medium of inexpensive home terminals such as the touch-tone telephone.[39] Several time-sharing data-processing systems already are being offered to the public in two general configurations: either the customer provides the data to be stored in the service company's computers, or the service company provides a body of specialized data that can be tapped at will by time-share customers at remote terminals.[40]

Regardless of the form in which computing facilities ultimately

---

34. Notice of Inquiry, *supra* note 29, at 89.

35. *See generally* Comments of Microwave Communications, Inc. (submitted in connection with *In re* Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities, FCC Docket No. 16,979) (March 5, 1968).

36. Western Union is establishing computer centers in order to provide customers with data-processing services. Irwin, *supra* note 24, at 1301; Titus, *supra* note 33, at 62; Notice of Inquiry, *supra* note 29, at 88.

37. Statement of Control Data Corporation 20 (submitted in connection with *In re* Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities, FCC Docket No. 16,979) (March 1, 1968):

> [C]ommunications satellites may eventually provide the capability for flat-rate [data transmission] charges regardless of the distance traversed since there is no cost differential determined by the distance between transmission and receiving station locations. Distance related costs appear only from the point of origin to the transmitting station and between the receiving station to the destination.

See also Wall St. J., Sept. 26, 1966, at 1, col. 1.

38. *See* Brown, *Tomorrow's Many-Splendored Tune-In*, Sat. Evening Post, Nov. 30, 1968, at 38, 78.

39. *See generally* D. Parkhill, The Challenge of a Computer Utility (1966); Computers and Communications—Toward a Computer Utility (1968); Irwin, *supra* note 24. A comprehensive study of this subject was undertaken in a symposium entitled "Symposium on the Computer Utility: Implications for Higher Education, May 5-7, 1969. The symposium papers and proceedings will be published in book form.

40. Bigelow, *Legal and Security Issues Posed by Computer Utilities*, 45 Harv. Bus. Rev., Sept.-Oct. 1967, at 150, 151.

are offered to the general public, it is clear that the need for these services provides enough economic incentive to guarantee the continued centralization of large bodies of data—an indeterminate amount of which is personal information. In addition, the movement of this data among different machine systems over relatively low-security communications channels, such as telephone circuits, is certain to become more prevalent. Unfortunately, little is being done to insure that computerized data in central storage or transit is any safer from the intrusive activities of snoopers than private telephone conversations have been in the past.

C. *The Information-Based Society*

Ever since the federal government's entry into the taxation and social-welfare spheres, increasing quantities of information have been elicited from citizens and recorded. Moreover, in recent years access to governmental largesse—at all levels—has depended increasingly upon a willingness to divulge private information. Brief reflection about the data acquisition implications of federal involvement in home-financing, urban renewal, and public health as well as the activities of the Office of Economic Opportunity, the Job and Peace Corps, and the Department of Housing and Urban Development provides graphic evidence of these trends.

As information-recording processes have become cheaper and more efficient, this appetite for data has intensified and been accompanied by a predilection toward centralization and collation of file material. In accordance with a principle akin to Parkinson's Law, as capacity for information-handling increases there is a tendency to engage in more extensive manipulation and analysis of recorded data, which, in turn, motivates the collection of data pertaining to a larger number of variables.[41] The availability of electronic data storage and retrieval has accelerated this pattern in a number of contexts; witness the expansion in the scope of questions on the 1960 and the proposed 1970 censuses[42] and the ever-increasing number of government questionnaires to which individuals are subjected. It also is reasonable to assume that one consequence of increased computer capacity is that many governmental agencies will go beyond current levels of inquiry and begin to ask more complex, probing, and sensitive questions. Perhaps future interrogations will touch upon such subjects as associations with other

41. *See Senate Hearings on Computer Privacy* at 74-75 (statement of the author).
42. *See* discussion in text accompanying notes 341-66 *infra*.

people, location and activity at different points in time and space, medical history, and individual attitudes toward various institutions and persons.

The increased application of computer technology resulting from time-sharing, remote-access terminals, and other forms of cost reduction also is causing a profound change in the manner in which the industrial and academic sectors of our society regard information and the uses to which it is put. Perhaps this trend has manifested itself most clearly in the social sciences. Largely because of the computer, scholars in these disciplines are increasingly able to base their theoretical structures on mathematical models rather than on "intuitive feeling and casual empiricism."[43] To construct and manipulate effective and sophisticated models[44] of the environment with the expectation of analyzing and predicting human behavior and natural or societal phenomena necessitates vast amounts of detailed information—"microdata"—rather than the broad and comparatively superficial summaries that social scientists traditionally have used.[45] This is true partly because accurate description of a complex system often requires investigation of an enormous number of potentially significant variables.[46] In addition, there may be unsuspected relationships inherent in the data that

43. Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 216 (1968). Professor Ruggles describes the problems facing social scientists before the introduction of the computer:

> Where empirical research is undertaken, it generally tends to concern itself with observations of global aggregates or with very small samples of data to which the social scientist may have obtained access. This situation is not of the social scientists' own choosing. The kinds of information required for an understanding of the social system have not been available, and prior to the development of the computer would not have been usable even if they had been available.

44. The term "model" is generic, and encompasses a variety of techniques. Crosson & Sayre, *Modeling: Simulation and Replication*, in THE MODELING OF MIND: COMPUTERS AND INTELLIGENCE 3 (1968), subdivide models into (1) replications, which reproduce some physical aspect of the original; (2) formalizations, which are symbolic representations of an original system that can be analyzed by paper-and-pencil mathematical operations; and (3) simulations, which, in contrast to formalizations, produce not a general solution but rather a statistical description of a large number of particular solutions for the more important variables. The simulation is the kind of model that most frequently requires the use of an electronic computer. For a simplified discussion of the methodology involved in making this kind of computer analysis, *see* Lozowick, Steiner, & Miller, *Law and Quantitative Multivariate Analysis: An Encounter*, 66 MICH. L. REV. 1641 (1968). *See also* Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 270, 275-76 (1964). The computer also can be programmed to edit the raw data and discover inconsistencies that would go unnoticed in hand editing. The Internal Revenue Service is currently using this capacity to detect inconsistencies in individual tax returns. *Hearings on Statistical Programs* 23 (statement of Professor Richard Ruggles).

45. *See, e.g.*, *House Hearings on the Computer and Invasion of Privacy* 199; *Hearings on Statistical Programs* 4 (statement of Edgar Dunn, Jr., research analyst, Resources for the Future, Inc.).

46. *Cf.* Lozowick, Steiner, & Miller, *supra* note 44, at 1652-60.

would be lost if only summaries or smaller quantities of information were available for analysis.[47] Identification of individual units of information also is necessary if, for example, the researcher wishes to discover how certain characteristics of the members of a particular group change during a period of time.[48] Highly detailed information also may enable researchers to "use the same basic data again and again for different analytic purposes."[49]

Of course, social scientists are not the only ones employing the new technologies for assistance in decision-making, record-keeping, and various forms of analysis. Institutions of every description are turning to electronic data-processing to increase their information-handling capacity and to improve the efficiency of their operations. The result is a seemingly inexorable trend toward ever larger and more complex computer systems that digest greater quantities of information about increased numbers of people.[50] Without question, many of these systems help various governmental institutions in their economic policy-making[51] and social welfare programs,[52] en-

47. *House Hearings on the Computer and Invasion of Privacy* 199.

48. *See House Hearings on the Computer and Invasion of Privacy* 52, 59, 97-98 (statement of Raymond T. Bowman).

49. *House Hearings on the Computer and Invasion of Privacy* 199.

50. A. WESTIN, PRIVACY AND FREEDOM 161 (1967). THE INSTITUTE FOR DEFENSE ANALYSIS, TASK FORCE REPORT: SCIENCE AND TECHNOLOGY (1967) (a report to the President's Commission on Law Enforcement and Administration of Justice) [hereinafter TASK FORCE REPORT: SCIENCE AND TECHNOLOGY] documents several facets of this trend in the application of computers to the criminal justice field. In summarizing the typical evolution of a police data-processing system, the Report concludes that most agencies utilizing electronic data-processing began with relatively modest punched-card systems, then expanded them until that format became impractical, switching to electronic systems as funds became available. *Id.* at 157. The Report also notes a trend toward consolidating the records of all municipal agencies into one central file (*id.* at 159) and makes its own contribution to the acceleration of these movements, recommending at 71:

> [T]o support court and correctional decision-making some States could establish more detailed records on persons in their directories [of persons who have records with state criminal justice agencies]. This *registry* could contain such background information as education, employment, military service, and probation reports. Such files could also be used to provide basic data for assessing the effectiveness of the State's different correctional programs.

51. *See, e.g., Hearings on Statistical Programs* 129-30 (statement of Arthur M. Okun, Member, Council of Economic Advisors):

> At one time, the economic policymaker was essentially a fireman, standing by much of the time until the alarm sounded the onset of recession or inflationary boom. Now, however, policymaking is clearly a continuous matter, aimed to help promote steady growth and noninflationary prosperity all the time. An information system could be adequate in sounding the alarm to herald major disruptions and still fall far short of meeting the needs of our current policy strategy.
>
> . . . .
>
> A full employment economy also brings to the fore the interrelationship between monetary and fiscal policy. It increases the need for detailed information on the relation between financial flows and income-expenditure flows. This puts special emphasis on accurate and prompt flow-of-funds information that is integrated with the national income and product accounts.

52. *House Hearings on the Computer and Invasion of Privacy* 258:

> In part . . . the changes in information requirements stem from radical changes

able industry to develop products to meet spiraling consumer demands and to respond quickly to the needs of an increasingly mobile population,[53] and permit academic institutions to process applications, schedule classes, record grades, and handle the myriad tasks that beset a modern educational system.[54]

As a result of the heightened value being placed on information by contemporary institutions, a substantial portion of information that hitherto has been treated as private is now considered as appropriate grist for the computer mill and fair game for the data collector. It may be a bit premature to conclude that "information is becoming the basic building block of society"[55] or that "all forms of wealth result from the movement of information,"[56] but there does seem to be considerable truth in the assertion that electronic technology is making the world into a "global village"[57] in which the domain of strictly private action is steadily being eroded.[58] On the assumption that there are some intrinsically

---

in demand factors distinct from . . . responses to expanded technical capability. Public policy in recent years has turned increasingly to a concern about the problems of social structure. . . . The issues of poverty, education, health, area depression, urban organization, etc., all require an increase in relevant detail for sub-system components of the total economy or total culture. At the same time the analytical disciplines in the social sciences . . . have been turning increasingly to quantitative methods and procedures.

Cf. Benn, *Where Power Belongs*, THE NATION, Aug. 26, 1968, at 136:

Government should be allowed to know a great deal more than it does about the community it was elected to serve. This requirement is essential if we want to see decisions made on the basis of fact. You cannot manage an advanced society, which is a vast, complex, interconnecting system, unless the facts are available.

53. Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 270, 275 (1964):

As population and mobility increase, there will be other incentives to establish central data files, for these will make it easier for the consumer in new environments . . . to acquire quickly those conveniences which follow from a reliable credit rating and an acceptable social character. . . . In consequence, we can expect a great deal of information about the social, personal, and economic characteristics of individuals to be supplied voluntarily—often eagerly—in order that, wherever they are, they may have access to the benefits of the economy and the government.

54. *See generally* G. BROWN, J. MILLER, & T. KEENAN, EDUNET (1967); Miller, Privacy Implications of Instructional Technology—A Preliminary Overview (March 1969) (unpublished paper prepared for the Study on Instructional Technology).

55. Sarnoff, *No Life Untouched*, SAT. REV., July 23, 1966, at 21.

56. M. MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN 65 (paper ed. 1964).

57. M. MCLUHAN & Q. FIORE, THE MEDIUM IS THE MASSAGE 63 (paper ed. 1967). *See also id.* at 12-24.

58. *House Hearings on the Computer and Invasion of Privacy* 10 (statement of Vance Packard):

Unless there are safeguards, pressures will surely grow to assemble more and more specific data about specific individuals. When the social security program began we were assured that our social security number would be guarded as a secret so that no one could possibly use it to keep track of our movements. Today we must write our social security number not only on our income tax return, but must

valuable aspects of individual privacy that should be protected from this erosion, it is appropriate to turn to an examination of the ways in which computer technology is magnifying the threat to privacy that always has been present in the handling of personal information.

III. The New Technology's Threat to Personal Privacy

A. *The Individual's Loss of Control over Personal Information*

Privacy, as many commentators have noted, is a concept that is impossible to define[59] or to fit into a coherent framework of legal doctrine.[60] With greater frequency, however, lawyers and social scientists are expressing the view that the basic attribute of an effective right to privacy is the individual's ability to control the flow of information concerning or describing him[61]—a capability that often is essential to the establishment of social relationships[62] and the

---

supply it to banks holding our money and to organizations making payments to us. . . .

Or consider the census. The authors of the U.S. Constitution called for an "enumeration" of the population every 10 years. . . . . Many millions of citizens in 1960 had to answer 165 questions about their lives, purchasing habits, and incomes. And the pressure is growing to add a host of new inquiries such as ethnic origins, religious affiliation, schooling, et cetera . . . .

59. A typical complaint is the assertion that "[f]ew concepts . . . are more vague or less amenable to definition and structured treatment than privacy. Under this emotional term march[es] a whole congeries of interests, some closely interrelated, some almost wholly unrelated and even inconsistent." Dixon, *The Griswold Penumbra: Constitutional Charter for an Expanded Law of Privacy?*, 64 Mich. L. Rev. 197, 199 (1965).

60. *See, e.g.*, Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481, 485 (2d Cir.), *cert. denied*, 351 U.S. 926 (1956) ("The state of the law is still that of a haystack in a hurricane."); Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 Law & Contemp. Prob. 326, 333 (1966) ("[T]he tort [of invasion of privacy] has no legal profile.").

61. One of the clearest statements of this position can be found in Office of Science and Technology of the Executive Office of the President, Privacy and Behavioral Research 8-9 (1967):

> [W]hat is private varies for each person and varies from day to day and setting to setting. Indeed, the very core of the concept is the right of each individual to determine for himself in each particular setting or compartment of his life how much of his many-faceted beliefs, attitudes and behavior he chooses to disclose. Every person lives in several different worlds, and in each his mode of response may—indeed must—be different. . . . The right to privacy includes the freedom to live in each of these different roles without having his performance and aspirations in one context placed in another without permission.

See also Beaney, *The Right to Privacy and American Law*, 31 Law & Contemp. Prob. 253, 254 (1966); Fried, *Privacy*, 77 Yale L.J. 475 (1968); *Foreword* by former Vice President Hubert Humphrey to E. Long, The Intruders vii (1967). The idea is hardly a new one; *see* Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890): "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."

62. *See, e.g.*, Fried, *supra* note 61, at 482: "To refer . . . to the privacy of a lonely

maintenance of personal freedom.[63] Correlatively, when the individual is deprived of control over the information spigot, he in some measure becomes subservient to those people and institutions that are able to gain access to it.[64] Thus, it has been suggested that the individual whose data profile is bartered or sold has become little more than a commodity.[65]

Informational privacy has been relatively easy to protect in the past for a number of reasons: (1) large quantities of information about individuals have not been collected and therefore have not been available; (2) the available information generally has been maintained on a decentralized basis; (3) the available information has been relatively superficial in character and often has been allowed to atrophy to the point of uselessness; (4) access to the available information has been difficult to secure; (5) people in a highly mobile society are difficult to keep track of; and (6) most people are

---

man on a desert island would be to engage in irony. The person who enjoys privacy is able to grant or deny access to others." *See also id.* at 475-86; A. WESTIN, PRIVACY AND FREEDOM 32-39 (1967).

63. *Cf.* Griswold v. Connecticut, 381 U.S. 479, 484 (1965):

> [S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. . . . Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one. . . . The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

See also Fried, *supra* note 61, at 475; OFFICE OF SCIENCE AND TECHNOLOGY OF THE EXECUTIVE OFFICE OF THE PRESIDENT, PRIVACY AND BEHAVIORAL RESEARCH 2 (1967). *But cf.* Bettelheim, *The Right to Privacy Is a Myth*, SAT. EVENING POST, July 27, 1968, at 8.

64. *See, e.g., House Hearings on the Computer and Invasion of Privacy* 12-13 (statement of Vance Packard), describing the dangers of a federal data center:

> [T]here is [a] hazard [in] permitting so much power to rest in the hands of the people in a position to push computer buttons. When the details of our lives are fed into the central computer where they are instantly retrievable, we all to some extent fall under the control of the machine's managers. . . .
>
> The filekeepers of Washington have derogatory information of one sort or another on literally millions of citizens. The more such files are fed into central files, the greater the hazard the information will become enormously tempting to use as a form of control.

See generally Shils, *Privacy and Power*, reprinted in *Senate Hearings on Computer Privacy* 231.

65. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 988 (1964):

> No man wants to be "used" by another against his will, and it is for this reason that commercial use of a personal photograph is obnoxious. Use of a photograph for trade purposes turns a man into a commodity and makes him serve the economic needs and interest of others. In a community at all sensitive to the commercialization of human values, it is degrading to thus make a man part of commerce against his will.

unable to interpret and infer revealing information from the available data. But a casual perusal of the testimony elicited by various congressional subcommittees[66] and brief reflection on the intrusive capabilities of the new surveillance devices and information technologies leads to the conclusion that these traditional safeguards on informational privacy no longer are reliable.

In a computerized environment, the power to control the flow of data about oneself can be compromised in a variety of ways. On the theoretical level, computer systems and other media that handle personal information are capable of inflicting harm on the data subject in two principal ways: (1) by disseminating evidence of present or past actions or associations to a wider audience than the subject consented to or anticipated when he originally surrendered the information (deprivation of access control), and (2) by introducing factual or contextual inaccuracies that create an erroneous impression of the subject's actual conduct or achievements in the minds of those to whom the information is exposed (deprivation of accuracy control).[67] Traditionally, the law has attempted to remedy these two wrongs separately by dealing with them under the respective theories of invasion of privacy and defamation,[68] although the line between the two torts often proves to be extremely nebulous. Inasmuch as today's computer technology is the progenitor of a new communications medium, it seems desirable to determine the character and extent of the damage that can be inflicted on individual privacy by various aspects of data-processing. This should facilitate consideration of the possibility that the existing legal pattern is not sufficiently responsive to the challenges presented by the technology and requires modification or replacement by a new format.

1. *Deprivation of Access Control*

The most significant computer-privacy problem is caused by the vulnerability of machine components and software to accident or intrusion. In the typical time-sharing system, there are at least six

66. *See, e.g., Hearings on Commercial Credit Bureaus Before a Subcomm. of the House Comm. on Government Operations*, 90th Cong., 2d Sess. (1968) [hereinafter *House Hearings on Commercial Credit Bureaus*]; *Senate Hearings on Computer Privacy*; *Hearings on Statistical Programs*; *House Hearings on the Computer and Invasion of Privacy*.

67. *See* Karst, *The Files: Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342, 343 (1966); Comment, *Copyright Pre-emption and Character Values: The Paladin Case as an Extension of Sears and Compco*, 66 MICH. L. REV. 1018, 1035-36 (1968). *See also Senate Hearings on Computer Privacy* 68 (statement of the author).

68. *See* text accompanying notes 256-79 *infra*.

operational stages that deserve attention as possible points through which improper access to the stored data may be gained or at which distortion may occur.[69] The first, and perhaps most obvious of these, is the information files, which generally are stored on some memory device in machine-readable form when they are not being used. In this condition the records are exposed to the danger of theft—a possibility that is enhanced by the extreme compactness and concentration of computerized records. Similarly, machine-readable records can be duplicated more rapidly and with less effort than their paper counterparts, usually without leaving any trace of tampering.[70]

When information is moved from the files into the central processor of a time-sharing system, a number of additional dangers arise. Despite their image of infallibility, computers are so intricate and delicate that occasionally they can be rendered inoperative by a speck of dust.[71] As a result, a minor mechanical failure may cause random distortion of data[72] or direct a message to the wrong terminal on a remote-access system.[73] Furthermore, the computer's rapid

69. Except as otherwise indicated, the following discussion of security in time-sharing systems is generally based upon Ware, *Security and Privacy in Computer Systems*, 30 AFIPS CONFERENCE PROCEEDINGS 279 (1967).

70. Allen, *Danger Ahead! Safeguard Your Computer*, HARV. BUS. REV., Nov.-Dec. 1968, at 97, 99: "A tape with 50 million characters of data, say, can be copied in a few minutes, leaving no traces; this tape might be a valuable mailing list, a set of computer programs, or other sets of operating procedures."

Another aspect of the vulnerability of computerized records is that they are easier to destroy than paper files. A simple magnet or a match can erase the enormous quantities of information stored on a reel of magnetic tape. One incident has been recorded, and others undoubtedly have occurred, in which a single disgruntled employee using this technique virtually wiped out a business enterprise "in no time at all." Allen, *supra*, at 99. *See also* note 75 *infra*. By way of contrast, the logistical difficulties of destroying large quantities of information maintained in traditional record books are well illustrated by the abortive attempt—admittedly made under intense stress—to destroy classified documents during the seizure of the *U.S.S. Pueblo*. TIME, Feb. 14, 1969, at 22.

71. *See, e.g.*, Surface, *What Computers Cannot Do*, SAT. REV., July 13, 1968, at 58:

> [C]omputers need not be erroneously operated to precipitate calamitous situations. There is increasing evidence that computers can be so erratic or so easily made inoperative . . . that, when used for some functions, they still must be considered as experimental machinery. . . .
>
> Such difficulties are so potentially ruinous that they have fostered at least two new businesses: computer detective agencies and insurance against computer-inflicted disasters.

72. Allen, *supra* note 70, at 98:

> An electrical equipment company discovered a faulty magnetic tape drive in its computer only after it had incorrectly processed hundreds of reels of tape. The defective equipment was not identified immediately because although it was distorting data at random, it continuously checked its own operation and reported that it was functioning properly.

73. Given the present state of the art, any data communication will result in the creation of errors. According to the Sperry-Rand UNIVAC Response to the Inquiry of the FCC, H & I-11 to H & I-12 (submitted in connection with *In re* Regulatory and

switching among a number of users of a time-share system may leave a residuum of one customer's information accessible to the next user who is placed in control of the heart of the machine.[74] Even if the system is functioning perfectly, there remains a possibility that a snooper could "eavesdrop" on electromagnetic energy radiating from the computer; this energy then could be reconstituted elsewhere in the form of the information in the system at the time the radiations were captured.

Indeed, the key software item of a time-share system—the monitor or control program—seems to be particularly vulnerable to purposeful intrusion. For example, there have been several reports that students have been successful in penetrating the protective features of university computers.[75] Once the access code of the control program of the particular computer system is broken, the intruder has the ability to display and manipulate the data stored within the system.

Policy Problems Presented by the Interdependence of Computer and Communications Facilities, Docket No. 16,979) (undated) [hereinafter UNIVAC Brief]:

> Studies published by the Bell System concerning error rates in data transmitted over voice channels at 600 bits per second and at 1,200 bits per second indicate that the frequency of the occurrence of incorrectly received data doubles when the speed of transmission doubles and increases in general with increases in distance. . . .
>
> In transmitting data, redundancy is the only remedy for faulty transmission. A single wrong bit, when detected, must either be corrected or retransmitted. To some extent, data may be corrected by error correcting codes which require built-in redundancy of the data transmitted. In most other instances erroneously received data must be retransmitted.

74. Petersen & Turn, *System Implications of Information Privacy*, 30 AFIPS CONFERENCE PROCEEDINGS 291, 298 (1967):

> [C]opying of residual information in the dynamic portions of the storage hierarchy during the following time-slice seems likely. Since erasing all affected storage areas after each time-slice could be excessively time consuming, a reasonable solution may be . . . to set aside certain areas of the core for private information and erase only those areas . . . after each time-slice.

75. ELECTRONICS, Jan. 9, 1967, at 25:

> The home of time-sharing, the Massachusetts Institute of Technology, has been having trouble with students who break the elaborate codes that are supposed to insure the privacy of the users of its Project MAC (machine-aided cognition) computers. On one occasion, it's been reported, students tapped into lines carrying Government data, including information from the Strategic Air Command at Omaha. Some of this tinkering has had the effect of jamming the lines.

Cf. Senate Hearings on Computer Privacy 84 (testimony of the author):

> Computer experts at the University of Michigan . . . tell me that a programmer with less than a month's training, can break the more elaborate encoding procedures currently being used in large data banks within 5 hours. . . . [A]t our institution . . . we occasionally leave a terminal unattended in an unlocked room to see if our students can work their way into the system by breaking the access code. They have never failed us.

See also Safeguarding Time-Sharing Privacy—An All-Out War on Data-Snooping, ELECTRONICS, April 17, 1967, at 157, 159; note 26 *supra*.

The experiment in computer-assisted instruction in law described in note 14 *supra* was almost destroyed by an unknown person who discovered one of the access codes for the University of Michigan remote-access terminal system. The intruder succeeded in destroying a number of other computer files.

The personnel servicing the central processor are another potential source of weakness in security. The programmer, for instance, could insert a secret "door" in the monitor program that would enable unauthorized people to bypass protective devices, or "could 'bug' a machine in such a sophisticated manner that it might remain unnoticed for an extensive period."[76] More simply, the computer's operator, or even a maintenance man, might reveal the nature of protective devices to snoopers or provide them with access keys. It also has been suggested that a corrupt repairman could "re-wire the machine so that certain instructions appeared to behave normally, whereas in fact, the protective mechanisms could be bypassed."[77]

When computerized information moves from the central processor through the communications links, the familiar specter of wiretapping is present. In addition to the relatively unsophisticated process of bugging the transmission line and recording or siphoning off the digital communications, the ingenious wiretapper with advanced equipment could attach a terminal to the line and join the group sharing the computer's services. This could be done in several ways: by using a previously planted "door" in the control program; by intercepting a user's communication and substituting his own; by invading the system while a remote-access user has his channel open but is not transmitting; or by intercepting and cancelling a user's sign-off signal in order to continue operating the system under that user's name.[78]

The next two stages of the data-processing system—the switching center and the remote console—also are vulnerable to attempts to eavesdrop on electromagnetic radiations. In addition, the switching center, either by mistake or as a result of tampering, may make a wrong connection and direct data to an unauthorized recipient. Finally, even when codes are used to protect the security of the remote-access terminals, an unauthorized user may "crack" the code or forge the required identification, or a malevolent authorized user may employ his console to alter the protective programs, "revise" the stored data, or misuse a printout of stored information that he obtained by a legitimate exercise of his access rights.

The simplest of these techniques—forging access codes and making unauthorized copies of storage media such as tape—seem to have been successfully employed already.[79] Although some of the

76. Ware, *supra* note 69, at 281.
77. *Id.*
78. Petersen & Turn, *supra* note 74, at 291.
79. *See* notes 70, 75 *supra.*

other techniques discussed above may seem rather esoteric, it would be folly to think that they are not within the realm of the technologically possible; some are feasible today, the rest will be in the future. The science fiction mystique surrounding cybernetics has a tendency to create a false sense of inviolability and impregnability, even among those on intimate terms with the machines. For example, one knowledgeable individual has argued that computerizing personal information will offer greater protection for privacy than does yesterday's manila folder because the putative snooper will need "a machine, a codebook, a set of instructions, and a technician" in order to gain access to the data and translate it into comprehensible notation.[80] It is doubtful that this is an accurate summary of conditions even in the present state of the eavesdropper's art. Indeed, other experts have flatly asserted that most program languages are easy to decipher,[81] that digital transmission of data "does not provide any more privacy than . . . Morse code,"[82] and that "modest resources suffice to launch a low-level infiltration effort."[83]

Even assuming the high cost of making a successful penetration of the data, there are countervailing factors that negate the supposed gain in protection achieved by converting data into a machine-readable format. For one thing, the payoff for a successful intrusion may be higher than would be true if the records were kept in a more mundane style. The centralization of formerly decentralized stores of information that results from computerizing records often will mean that one invasion will secure for the intruder vast quantities of data that formerly could be obtained only by several file penetrations. In addition, the snooper who has access to a single remote terminal will be able to reach all of the relevant data in a computer network that may be composed of numerous information nodes geographically distributed across the continent or around the world. Finally, the computer-based record system of the future simply is likely to contain more extensive information than traditional files. For these reasons, the snooper's "cost per unit of dirt" actually may be lower for poaching computerized records than it is for paper files.

Given the incentive of a potentially high payoff for invading computerized files or intercepting data transmissions, there is no

80. *House Hearings on the Computer and Invasion of Privacy* 94 (statement of Edgar S. Dunn, Jr., research analyst, Resources for the Future, Inc.).

81. Allen, *supra* note 70, at 100.

82. Petersen & Turn, *supra* note 74, at 291.

83. *Id.* at 298. *See also* UNIVAC Brief at J-15: "There are many devices on the market today which make it possible to pick up intelligence from a [computer] communications terminal and record the content of messages."

doubt that elements of organized crime, a variety of governmental agencies, and segments of private industry will invest sufficient resources to launch sophisticated snooping programs.[84] One group that undoubtedly will have the facilities and the inclination to intercept digital transmissions is the law enforcement establishment, which recently has been granted extensive statutory authority to wiretap and eavesdrop.[85] As the telephone company converts its voice lines to digital transmission,[86] police will have to acquire the equipment and expertise to convert digital to voice communication. And once they have that hardware and training, the police can be expected to apply it in contexts other than the simple interception of conversations being carried by digital transmission.

2. *Deprivation of Accuracy Control*

To the vulnerability of machine components must be added numerous possibilities for human error in information-handling that are created or exacerbated by computer technology. The risk that careless or malicious administrators will introduce errors into records containing personal data is a familiar one, and its origins cannot be attributed to the advent of the computer. However, as computer capacity increases the range and volume of individualized data that is stored, this risk undoubtedly will be magnified. Indeed, until highly accurate mechanical input devices—such as optical scanners[87]—become operational, the likelihood of human error in the recording process necessarily is going to be higher than it is in the context of traditional record-keeping because of the extra handling stage that is necessary to translate raw data from alphabetic notation into the appropriate computer input format.

For these and other reasons, there is a widespread and legitimate fear of overcentralizing individualized information and then increasing the number of people who, by having access to it, have the capacity to inflict damage through negligence, sheer stupidity, or a lack of sensitivity to the value of personal privacy. Unthinking people are as capable of injuring others by unintentionally rendering a record inaccurate, losing it, or disseminating its contents to unauthorized users as are people acting out of malice or for personal aggrandizement. It simply is unrealistic to expect subtle

84. It has been suggested that outside intrusion into a computer system could serve as the basis of a "change your dossier for a fee" service, for example. Petersen & Turn, *supra* note 74, at 292.

85. *See* text accompanying notes 327-345 *infra*.

86. *See* text accompanying notes 27-38 *supra*.

87. *See* text accompanying notes 106-08 *infra*.

standards of care and basic principles of individual privacy to be consistently understood or implemented by people in clerical positions.[88]

The centralization of information from widely divergent sources also creates serious problems of contextual accuracy. Information can be entirely accurate and sufficient in one context and wholly incomplete and misleading in another. As large numbers of remote terminals are linked to computers and as today's local and regional data centers are linked together in national or international networks, information will be moved and stored far from its point of original recordation and employed for purposes and by people unassociated with its collection—conditions that, it has been suggested, virtually guarantee inaccurate human interpretation.[89] Errors of this type can occur in a number of ways. Raw, unevaluated data about an individual can give rise to damaging inferences that a fuller explication, direct knowledge of the information's source, or a highly professional analysis would prevent. Illustrative of this type of distortion is a terse entry stating that the subject was arrested, convicted of a felony, and sentenced to a federal penitentiary for a certain number of years. The impact of this data on the individual's ability to obtain employment or credit surely will be detrimental. Yet the "felon" may have been a conscientious objector who could not meet the requirements for exemption from military service that existed at the time he was to be inducted. If the events occurred in the distant past and the legal or social attitude toward the particular "offense" has moderated, the entry is doubly dangerous.[90]

Other difficulties are likely to increase the risk of inaccurate interpretation in subtle ways. What appears to be "hard," "factual" data often takes on different shades of meaning in different contexts, and the individual who is asked to provide a simple item of information for one purpose may omit explanatory details that become crucial when his file is surveyed for unrelated purposes. An unexplicated notation of an individual's marital status conveys different connotations to the Selective Service System, a credit bureau, the Internal Revenue Service, and the Social Security Administration. Similarly, many information gatherers fail to appreciate the

88. *See generally Senate Hearings on Computer Privacy* 75-76 (statement of the author).

89. *House Hearings on the Computer and Invasion of Privacy* 24 (testimony of Professor Charles Reich).

90. Or consider the impact of a hypothetical dossier on Mr. William F. Rickenbacker, whose felony was to refuse to answer part of the 1960 census questionnaire. *See* United States v. Rickenbacker, 309 F.2d 462 (2d Cir. 1962), *cert. denied*, 371 U.S. 962 (1963).

necessity of entering supplemental data that may ameliorate an earlier entry that has some derogatory overtones.[91] For example, police departments throughout the nation can obtain an FBI "rap sheet" containing a suspect's criminal record by sending his fingerprints to Washington. These sheets are supposed to include information on the court disposition following each arrest, but in the past this data has not been furnished in thirty-five per cent of the cases.[92]

The computer's image of infallibility often leads people to accept its output unthinkingly. This is unfortunate. To paraphrase a remark by Senator Fulbright in the course of his debate with Secretary of Defense Laird over the ABM: Just because data is stored in a computer doesn't make it accurate.[93] But this belief does exist, and it may accentuate a problem that always has inhered in the compilation of personal information—the danger of relying on "soft" or subjective data for human evaluations or decision-making. Psychological tests can be designed for machine scoring, and the results, either in raw form or after evaluation, can be added to the individual's dossier. Despite the apparently authoritative character of such tests, a substantial number of people in the scientific community question their ability to reflect accurately the complexities of an individual's beliefs and attitudes.[94] Thus, their presence in a computer file, either as raw test responses or in the form of an evaluation, can be extremely dangerous to the subject unless the test data is accompanied by an extensive explanation of the conditions under which the test was administered and the purpose for which it was taken. Since the cost of preparing and storing such a lengthy caveat would be high, there is considerable likelihood that it will not be included.

Similarly, efficiency ratings for employees and students are valuable and have a long history of use, but there is a possibility that computerization will render them less reliable. For one thing, factors

91. Even if these information managers wanted to ameliorate pieces of data with supplementing information, there are a number of reasons why they might be unable to do so. First, their system may not be designed to accommodate such data. Second, since many large data banks may have many uses, the managers may have no idea when a piece of information is fed into the system whether or not amelioration will later be necessary. Furthermore, they may not be able to tell exactly what will ameliorate an entry, since they do not know all of the purposes for which the entry will be used.

92. TASK FORCE REPORT: SCIENCE AND TECHNOLOGY 76.

93. The Fulbright-Laird exchange is described in NEWSWEEK, March 3, 1969, at 22; TIME, Feb. 28, 1969, at 23-24; N.Y. Times, Feb. 21, 1969, at 1, col. 6.

94. Miller, *Psychological Testing and Privacy in an Information Oriented Society* (to be published in *Think Magazine* May-June 1969); Douglas, *Computerized Man*, 33 VITAL SPEECHES 700 (1967).

of cost, ease of administration, and system configuration may force evaluations to be framed in conclusory categories such as "excellent," "fair," or "good." Exchange of evaluative information among different organizations that lack common traditions of scoring or interpreting performance can compound the confusion, since a "fair" rating may denote average performance in one setting and very poor work in another.[95] The problem of sharing information based upon noncomparable categories or premises is not insubstantial.[96] Data gatherers always have exhibited a marked propensity to cooperate with each other in exchanging information,[97] and there is no reason to expect that the practice will decline as machine interfaces for the transfer of data become easier to establish. This ease of information movement, coupled with the technology's aura of omniscience, may motivate some administrators to rely on soft data without a reasonable investigation as to its source, the purpose for which it originally was collected, or the evaluation standards of the data originator.

Thus, success or failure in life ultimately may turn on what other people decide to put in an individual's file and the programmer's ability, or inability, to evaluate, process, and interrelate information. These prospects are made even more depressing by the realization that the great bulk of the data likely to find its way into the

95. Professor Karst, *supra* note 67, at 356, points out that the danger of personal evaluation "lies in the fact that the evaluator and the recipient of his information may not share the same standards for reducing a complex set of facts to evaluative inferences or even the same language." The example given is the military officer's effectiveness-rating system, in which an apparently average rating really connotes low quality performance. *See also Senate Hearings on Computer Privacy* 75-76 (statement of the author).

96. The difficulties caused by incompatible categories are one of the chief impediments to creation of a uniform federal statistical system. *See, e.g.*, SUBCOMMITTEE ON ECONOMIC STATISTICS OF THE JOINT ECONOMIC COMMITTEE, THE COORDINATION AND INTEGRATION OF GOVERNMENT STATISTICAL PROGRAMS, 90th Cong., 1st Sess. 3 (1967):

> In general, the bodies of data [collected by federal agencies] do not mesh according to any overall system and there is much inflexibility which often prevents fitting the micro data to behavioral models. Reasons for the incompatibility include the following:
>
> (1) differing definitions, classifications, and timing of respondent reports when uniformity is needed;
>
> . . .
>
> (3) differing qualities of data and inconsistent documentation.

The difficulties in obtaining comparable statistics even when the categories are uniform are discussed in *Hearings on Statistical Programs* 12:

> We have such things as a Standard Industrial Classified Code or codes which are in effect and utilized by different agencies. . . . The descriptive phrases which are used to label these collection boxes are supposed to be standard for the different agencies, but there are some practical problems. . . . It is possible for one agency or one statistical program to wind up with a box with the same standard classification label as another, but each containing a different collection of respondents. . . . Agencies may occasionally establish different cutoff points that determine which box will actually receive a given respondent unit.

See also id. at 116.

97. *See, e.g.*, notes 177-78, 376-91, 546-47 *infra* and accompanying text.

files will be gathered and processed by relatively unskilled and unimaginative people who will lack the discrimination and sensitivity necessary to warrant reliance on their judgment. Furthermore, a computerized file has a certain indelible quality—adversities cannot be overcome with time absent an electronic eraser and a compassionate soul willing to use it.

The computer's demonstrated ability to assemble and collate large quantities of information relevant to a given subject also may lead to an abdication of human responsibility for making important judgments or debilitate the willingness of decision makers to return to the original information source to seek out more or better data. Although it often is stated that the computer's utility necessarily is limited by the quality of the input—hence the maxim "garbage in, garbage out" (GIGO)—the hypnotic effect of being able to manipulate enormous data bases with the press of the proverbial button makes it questionable whether human evaluations always will provide a final check on the application of the computer's output. By using the computer to quantify intangible elements or by asking it the wrong questions, an administrator can produce plausible answers that, when acted upon, might precipitate disaster.[98] Some notion of the problems that may arise in the handling of personal data as an assist in policy-making can be divined from a report of one controversial computer application:

> [In New York a] . . . computer that had been fed accumulated information from bettors, police and other sources spewed out the names of eighty-six alleged bookmakers. Indictments followed. The machine had not only stored the information but had evaluated it. The government claimed that the three-year statute of limitations on the charges might have expired before human investigators could have evaluated the data.[99]

A number of disturbing questions are raised by this brief account. Although programming a computer to select names of people for indictment may fall within the prosecutor's discretion, are there any constraints on the procedures employed? Must they meet some minimal standard of computer science? More important, who determines what raw data has sufficient probative value to warrant being fed into the computer and what weight is to be assigned to particular items within each category of information? Will the official who is invested with authority to decide whether an indictment should be sought on the basis of the computer output

98. *Cf.* E. MORISON, MEN, MACHINES, AND MODERN TIMES 91-93 (1966).
99. E. LONG, THE INTRUDERS 54 (1967).

have enough understanding of the computer's capabilities and method of operation to make a rational assessment of its product? The possible prejudice to the individual resulting from the practice is not likely to end with the decision to seek an indictment. Commenting on this particular computer application, a lawyer observed: "[T]he . . . computer can tell you where the stars are going to be a million years from now. Do you think a jury is not going to believe that it can tell you where a bookie is in the Bronx?"[100]

B. *Cybernetics As an Instrument of Surveillance*

Perhaps the most serious apprehensions concerning the implications of the computer for personal privacy are warranted when considering the use of the new technology in concert with surveillance activities. One rather obvious application of this type that is alluded to throughout this Article is the development of a "record prison" from the computer's prodigious storage capacity. The ability of a sophisticated data center to generate a comprehensive womb-to-tomb dossier on an individual and transmit it over a national network is one of the most graphic threats of the computer revolution.[101]

Another possible application of the new technology stems from the capacity to manipulate a highly detailed data base in order to simulate the behavior of a complex organization. If a corporation has enough information about one of its competitors, for example, it may be able to predict the rival's future actions, a useful resource in the context of contract bidding. But beyond these relatively benign applications, it also seems feasible to employ computer analysis to determine what types of false stimuli or corporate feints are likely to cause a desired response on the part of the competitor.[102] It does not require a vivid imagination to conjure up a number of simulation activities involving human manipulation if extensive enough dossiers are available.

In addition to using the computer to construct and manipulate personal files, however, it also is possible to use the machine in conjunction with seemingly unrelated data files to analyze an in-

100. *Id.* at 54-55. For the most comprehensive discussion to date of the impact of science on problems of proof, *see* Korn, *Law, Fact, and Science in the Courts*, 66 COLUM. L. REV. 1080 (1966). *See also* B. BOTEIN, THE TRIAL OF THE FUTURE (1963).

101. *See, e.g.*, M. MCLUHAN & Q. FIORE, THE MEDIUM IS THE MASSAGE 12 (paper ed. 1967); Address by Arthur J. Goldberg, The Owen J. Roberts Memorial Lecture: Can We Afford Liberty?, Feb. 20, 1960, at 4. *See also* note 3 *supra;* notes 141-44 *infra; Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211 (1968).

102. *Big Corporations Can Have Their Own CIA*, THE NEW REPUBLIC, Feb. 18, 1967, at 18.

dividual's activities to see if they bear any relation to the conduct of other investigation subjects. This capacity for "inferential relational retrieval"[103] is demonstrated by the following description of American Airlines' seemingly innocuous flight reservation computer:

> American's computer can be queried about any traveler's movement in the past two or three months. In a furious burst of speed, the electric typewriter spews out a dossier; flights traveled, seat number, time of day, telephone contact, hotel reservation, car reservation, fellow travelers, etc.
>
> . . . [A] computer expert for the airline says that 10 to 15 investigators a day (Federal, state, local and other) are permitted to delve into the computer for such information. *Some of them want (and get) a print-out of the entire passenger list of a certain flight to see who might be traveling with a particular person.*[104]

A further significant threat to personal freedom is presented by the inevitable linking of computers to existing surveillance devices for monitoring people and their communications. One of the simplest of the present generation of snooping devices is the pen register, which, when attached to a telephone line, records on paper a series of dashes representing all numbers dialed from the selected telephone.[105] But this snooping capability would be increased by several orders of magnitude if a few pen registers were attached to suspects' telephone lines and the information drawn in by these devices fed into a central computer. This technique could quickly provide a revealing analysis of patterns of acquaintances and dealings among a substantial group of people. Indeed this may be possible without pen registers; when the telephone companies' move to digital transmission is complete, a by-product may be a ready-made data base on past communications that awaits only cross-correlation.

Yet, the computer-pen register combination is relatively primitive and its surveillance yield is relatively low compared to the forecasted marriage between computers and the emerging optical scanner technology. IBM recently announced the availability of

103. *House Hearings on the Computer and Invasion of Privacy* 119-35 (testimony of Paul Baran, computer expert with the Rand Corporation).

104. Star, *The Computer Data Bank: Will It Kill Your Freedom?*, Look, June 25, 1968, at 27, 28 (emphasis added).

105. Sullivan, *Wiretapping and Eavesdropping: A Review of the Current Law*, reprinted in *Hearings on S. 928 (Right of Privacy Act of 1967) Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 1st Sess., pt. 1, at 62-63 (1967) [hereinafter *Hearings on the Right of Privacy Act*, pt. 1]. A technical description of the pen register may be found in *Hearings on Invasions of Privacy (Government Agencies) Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 89th Cong., 1st Sess., pt. 2, at 954-61 (1965).

a mechanical page reader capable of reading and inputting into a computer typed or hand-printed letters, words, and numbers at the rate of 840 single-spaced typewritten pages per hour.[106] Because of the universally acknowledged need for accurate high-speed input devices, more spohisticated successors are certain to follow. The installation of these devices in strategic post office facilities across the country would enable the government to maintain "mail cover"[107] operations on a massive scale. By computerizing the data drawn in by the scanners and subjecting it to a sophisticated control program, this type of surveillance could yield exhaustive lists of the mail sent and received by thousands of individuals and organizations.

There are many other possible applications for scanners. For example, computers presently are being used to help trap scofflaws in a number of jurisdictions. The most common of the current procedures calls for police officers at a checkpoint to radio the license plate numbers of passing cars to a computer operator. The operator then inputs the number, the computer responds by providing a printout revealing whether any violations are outstanding against that license number or the person in whose name the car is registered, and the operator informs the officers of the results.[108] Optical scanners designed to decipher license numerals

106. N.Y. Times, July 16, 1968, at 61, col. 2. Early models of optical scanners are already in use in several government agencies. *Senate Hearings on Computer Privacy* 69-70, 97-98, 125; *Hearings on Statistical Programs* 123. Apparently most of the major computer companies are working to develop optical scanners. *See* Riley, *Punched Cards on the Ropes?*, ELECTRONICS, April 15, 1968, at 193, 202;

> Optical character readers are made by several companies, including the Optical Scanning Corp., National Cash Register, Farrington Electronics Inc., IBM, the Control Data Corp., Recognition Equipment Inc., and the Philco-Ford Corp. Some machines read only single lines, while others can assimilate whole pages. Some read only stylized type fonts, other[s] almost anything.

See also Senate Hearings on Computer Privacy 98 (letter from the author).

107. The Post Office Department's mail cover procedure was described as follows by the Chief Postal Inspector in *Hearings on Invasions of Privacy (Government Agencies) Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 89th Cong., 1st Sess. 67 (1965):

> A mail cover simply consists of recording from a piece of mail the name and address of the sender, the place and date of postmarking, and the class of mail. Mail is neither delayed nor opened. . . . Only the material appearing openly on the wrapper is noted. The recording is done by a postal employee. A mail cover is authorized only when there is good reason to believe that it may be instrumental in the solution of a crime. Information obtained from a cover is used as leads in an investigation, not as evidence in court.

The legality of mail cover operations has been upheld in United States v. Schwartz, 283 F.2d 107 (3d Cir. 1960), *cert. denied*, 364 U.S. 942 (1961), and United States v. Costello, 255 F.2d 876, 881-82 (2d Cir.), *cert. denied*, 357 U.S. 937 (1958). *See generally* E. LONG, THE INTRUDERS 102-08 (1967).

108. TIME, Sept. 3, 1965, at 72. *See also* Hirsch, *The Punchcard Snoopers*, THE NATION, Oct. 16, 1967, at 369, 371:

> [A] nation-wide computerized network designed to help keep undesirable drivers

and send them directly to the computer obviously would make the process more efficient—and, as a by-product, might enable the compilation of comprehensive records of the movements of a person's automobile, perhaps for later inferential relational analysis.

The ultimate step in mechanical snooping, however, may be the implantation of sensing devices in the human body itself. Assuming an improved state of the art, these devices might be capable of transmitting data relating to physiological and chemical changes resulting from various bodily processes to a computer that is programmed to monitor and record the data, transmit a response to the sensor, or sound an alarm when specified chemical or biological events occur. To be sure, monitoring systems of this type are adaptable to many beneficial and humanitarian purposes, such as allowing a patient under treatment to resume his normal activities wearing sensing devices that will warn his doctor instantaneously when physiological changes symptomatic of impending danger appear.[109] But telemetry also can be imposed on a so-called "antisocial" or "aberrational" individual in order to reveal whether or not the concentration of personality-altering chemicals in his bloodstream is at a "stable" level,[110] or to administer rewards and punishments

off the highway is being developed within the Department of Transportation. Each state will feed in the records of individual drivers whose licenses have been revoked; all states then will be able to check their driver license applications against this file, routinely and instantly. The basic idea is to prevent a driver who loses his license in one state from getting relicensed in another. Who will have access to this information has not been disclosed.

109. *See Senate Hearings on Computer Privacy* 72 (statement of the author); Freed, *Legal Aspects of Computer Use in Medicine*, 32 LAW & CONTEMP. PROB. 674, 691 (1967); Miller, *The National Data Center and Personal Privacy*, THE ATLANTIC, Nov. 1967, at 53; *cf.* Wall St. J., Feb. 14, 1969, at 11, col. 2:

> G.D. Searle & Co., a pharmaceutical manufacturer, said it has begun marketing a commercial line of biomedical instrument systems that can be used for rapidly screening and examining patients in large numbers.
>
> . . . [T]he system, which may be sold or leased to hospitals, clinics or physicians, consists of a variety of measuring instruments that feed data from the patient directly into a computer.
>
> . . . .
>
> . . . Automated instruments measure hearing, vision, blood pressure, height, weight, and other body functions.

Computer-linked sensing devices will undoubtedly play an increasingly large role in industry and commerce. *See, e.g.*, Sarnoff, *No Life Untouched*, SAT. REV., July 23, 1966, at 21:

> Even the soil will be computerized. The long-range outlook for agriculture includes new sensing devices that will be placed on larger farms, feeding information to the computer on soil moisture, temperature, weather outlook, and other details. The computer will calculate the best crops to plant, the best seeding times, the amount of fertilizer, and even the correct harvesting time for maximum yield.

A computer-based check verification system to thwart forgers is now available in California. Wall St. J., May 12, 1969, at 1, col. 4.

110. *See, e.g.*, Fleming, *The Computer and the Psychiatrist*, N.Y. Times, § 6 (Magazine), April 6, 1969, at 45:

> [T]he impact of drug therapy on psychiatry has been revolutionary. It is

by remote control when sensors reveal that the subject has engaged in certain kinds of behavior.[111] As might be expected, the proponents of these pervasively intrusive systems assert that they will be used only for "ethical" and "benevolent" purposes; but the enormous potential for abuse inherent in surveillance procedures of this type makes one wonder whether the assurances of these advocates are sufficient protection.[112]

C. *The Psychological Aspects of a Dossier Society*

Since the right to privacy has been conceived in part to assure the individual's emotional integrity,[113] it is appropriate to consider

---

currently saving the State of New York, alone, some $30-million a year, according to a report from the office of Dr. Alan D. Miller, Commissioner of Mental Hygiene. . . . [T]hanks largely to drug therapy, releases from the state's hospitals have soared from 10,394 a year in 1955 to 32,625 in 1968. Across the nation, in other states which invest more cash per capita in the care of mental illness . . . the results have been even more dramatic, with caseloads declining as much as 25 per cent.

See also Michael, *Speculation on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 270, 281 (1964).

The actual use of these techniques is described in Berry, *Project Brain Control*, reprinted in 111 CONG. REC. 16,181, 16,182 (July 9, 1965):

> ESB [electrical stimulation of the brain] has . . . been used experimentally to treat mental patients. At Tulane University . . . a select group of chronic mental cases were equipped with self-stimulators. Buttons on a special belt activated electrodes in their brains. Whenever a patient felt depressed, he pushed the button. ESB, washing away anxiety, helped restore a more cheerful mood. In cases where patients had severe psychotic seizures, ESB turned uncontrollable rage into euphoria.

111. Note, *Anthropotelemetry: Dr. Schwitzgebel's Machine*, 80 HARV. L. REV. 403, 407 (1966):

> If criminality is acquired, like other behavior, by imitation and social conditioning, it should be possible to remove it by conditioning more acceptable conduct. Tracking is a useful tool for such conditioning: it indicates when the act to be rewarded takes place, and it enables the reward to be given immediately, which is vital. Two effective rewards, [verbal] approval and electrical stimulation of the brain, are easy to administer through a tracking system.

See also Miller, *On Proposals and Requirements for Solutions*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 226-27 (1968). These concepts seem likely to gain increasing approval in medical and scientific circles. *See, e.g.*, McConnell, *Psychoanalysis Must Go*, ESQUIRE, Oct. 1968, at 176, 280:

> Maybe "mental illness" is a myth—maybe what's wrong with most patients is that they've learned bad or "sick" behavior patterns. And if they've *learned* those behaviors, they can be induced to *unlearn* them if we go about things in the right way.
>
> To phrase it another way, perhaps the trouble with crazy people is that they act crazy. Not that they *are* crazy, but that they *act* crazy. You and I act sane because we've been rewarded for acting sane, and punished severely if our behavior gets too far out of line. If we want to cure "sick" behavior, perhaps we can do so by rewarding patients for acting sane, or by punishing them for acting insane, or both. This very simple, intriguing idea is rapidly turning psychology and psychiatry upside down.

112. Some of the limitations on total surveillance are pointed out in V. FERKISS, TECHNOLOGICAL MAN 166-67 (1969).

113. *See generally* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-96 (1890).

briefly the possible psychological impact on our citizenry of unchecked computerization. In view of the computer's ability to preserve and retrieve vast quantities of minute personal data and assist in the administration of socially desirable welfare and environmental programs, it might seem anomalous that one of the chief apprehensions concerning the computer age is that it brings with it the threat of depersonalization.[114] Upon reflection, this incongruity unfortunately proves to be only superficial. As the populace becomes increasingly aware that a substantial number of personal facts are being preserved on "the record," people may start to doubt whether they have any meaningful existence apart from the profile in the computer's files.[115] As a result, they may begin to base their personal decisions, at least in part, on whether it will enhance their record image in the eyes of third parties who have control over important aspects of their lives:

> The terms consequential behavior and acting for the record . . . [may be] used interchangeably. They involve not only the control of forethought to our behavior, but also mean that one should act so that things must appear on the record in a limited way. One puts to oneself not only the admonition that "I had better be care-

---

114. Representative Corneilius E. Gallagher stated his view in *House Hearings on the Computer and Invasion of Privacy* 2:

> "The Computerized Man," as I see him, would be stripped of his individuality and privacy. Through the standardization ushered in by technological advance, his status in society would be measured by the computer, and he would lose his personal identity. His life, his talent and his earning capacity would be reduced to a tape with very few alternatives available.

This complaint is not unique to the computer age. It was a common objection to the industrial revolution and the so-called mass society and mass culture. *See generally* V. FERKISS, *supra* note 112, at 60-76.

115. Michael, *supra* note 110, at 277:

> As the society grows more complex and the individual's sense of his ability to influence it in his own interest seems smaller, the tendency to depend for placement and advancement on what can be revealed about oneself which can be evidenced and acted on "scientifically" may well increase. . . . This response also will be a natural extension of our dependency on the machine, which in this case will help the expert or make the decisions itself about the value of the individual, impersonally but with great precision . . . .

In fact, there may be a very real sense in which a person does not exist outside of his computer dossier. Consider the following colloquy taken from *House Hearings on the Computer and Invasion of Privacy* 145:

> MR. GALLAGHER. . . . Since the IRS has now set up a central data collection service and now that we have the potential of erasing from the computer's memory and truly making a person an "unperson," would it be possible for a skilled computer expert to make himself a nontaxpayer, by programming himself out of existence?
>
> MR. SQUIRES. That is a very interesting question. I suspect that it would be.
>
> MR. GALLAGHER. Therefore, by sending in the wrong card or the right card, or the wrong answers, he could be eliminated from existence from the rolls of the IRS.
>
> MR. SQUIRES. That seems to me quite reasonable.

> ful: This may go on the record," but also the question as to how will it look and be interpreted by those who are not immediately involved in this activity and will judge it from its appearance to them....
>
> Thus, the technical demand for more personal information to be recorded and a conscious public concerned with keeping the record straight lie at the root of the new invasion of privacy. It is a deprivation of privacy that cannot be legislated against nor moralized against. It is a source of social control which necessitates new techniques and a pervading inquiry into our social, economic, and political actions and our motivations for them. It is an invasion which most people willingly accept, since they have not known other conditions and are happy to be publicly significant to someone.[116]

This psychology may be augmented by the conception of the computer as the unforgetting and unforgiving watchdog of the information managers. As one observer has remarked, "the possibility of the fresh start is becoming increasingly difficult. The Christian notion of redemption is incomprehensible to the computer."[117]

It thus is not surprising that there appears to be a reaction against computerized decision-making and other appearances of human abdication to the machine. Increasingly, the computer is becoming a convenient scapegoat for a number of man's ills; there is evidence that the frustrations generated by the computerized environment are provoking highly irrational responses on the part of disenchanted groups. People have written letters to computers operated by commercial dating services, commenting on the dates that have been arranged for them;[118] naked protesters have picketed IBM offices with signs stating that "Computers are Obscene";[119] and computer operators reportedly have ascribed human personalities to their machines.[120] Personification of computers has carried over into the arts: computers have emerged from the world

116. Wagner, *Records and the Invasion of Privacy*, reprinted in 111 CONG. REC. 10,821, 10,823 (May 18, 1965).

117. *House Hearings on the Computer and Invasion of Privacy* 12 (statement of Vance Packard).

118. *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 289 (1968) [hereinafter *Senate Hearings on Computer Privacy*, pt. 2].

119. N.Y. Times, Nov. 4, 1968, § 1, at 27, col. 5.

120. *See, e.g., That New Black Magic*, TIME, Sept. 27, 1968, at 42:

> Computer technology is bewitched with superstition. For one thing, today's young cyberneticists tend to anthropomorphize their tools. Tom Allison, 25, a Coca-Cola executive in Atlanta, is convinced that his computer is feminine. "She keeps cutting me off at the most inopportune times," he complains. A programmer in Los Angeles will not feed blue cards into his computer—he feels she deserves pink. Seymour Greenfield, a research manager for the military DRC-44 computer program at Dynamics Research Corp. near Boston, complicates the matter further. "I hired everyone building the computer by the zodiac signs under which they were born," he says. As a Leo, he has prejudices. "I hired two Cancer men and they both ended up with ulcers."

of science fiction[121] to become sinister protagonists or anthropomorphic figures in novels,[122] plays,[123] motion pictures,[124] and poems.[125] It also has been suggested that widescale computeriza-

121. *E.g.*, M. FRAYN, THE TIN MAN (paper ed. 1965); R. HEINLEIN, THE MOON IS A HARSH MISTRESS (paper ed. 1966); O. JOHANNESSON, THE TALE OF THE BIG COMPUTER (1968); D. JONES, COLOSSUS (1966).

122. *E.g.*, E. BURDICK, THE 480 (1964); T. TYLER, THE MAN WHOSE NAME WOULDN'T FIT (paper ed. 1968).

123. *E.g.*, Kerr, *Push Button "A" for Laugh "B"*, N.Y. Times, Sept. 29, 1968, at D1, col. 1, describing a sketch in a play entitled "The Fourth Wall":

> [A] chap who was starved for female companionship, if it's still called that, arranged himself a date on the computer system, presumably getting a girl whose card-indexed characteristics matched his needs.
>
> She came, she was tall, she was red-haired, she was compliant. A less resistant partner for the evening could scarcely be imagined. Everything she said was right. The boy had no need to delay matters. "Would you like to kiss me?" he asked, fairly quickly. "I'm terribly excited," she said, responding in low tones, on cue.
>
> Only one thing wrong. Those tones. They were low, all right, just where they should have been. And they were cold, cold as an ice cube tray that has stuck to your hands because your hands are wet. They were efficiently responsive, mathematically responsive, synthetically responsive. At this point, of course, we tumbled to the joke. The girl herself was the computer, out for the night.

124. *E.g.*, *Hot Millions* (described in Dickon, *Hot Millions and the Computer Ethic*, CAREERS TODAY, Feb. 1969, at 12); *2001: A Space Odyssey*.

125. *E.g.*, Hayakawa, "Solemn Thoughts on the Second Industrial Revolution," 23 ETC: A REVIEW OF GENERAL SEMANTICS 7-8 (1966) [footnotes in original]:

> In each insurance company, in every bank and store,
> Are filing clerks and billing clerks and typists by the score;
> The work that all these people do will one day disappear
> In ERMA[1] systems tended by a lonely engineer.
>
> (But they'll never mechanize me—not me!
> Said Charlotte, the Louisville harlot.)
>
> While former auto workers try to fill their empty days,
> The automated auto-plant will turn out Chevrolets:
> With automatic pilots landing jet planes on the strip,
> The present men who guide them will not need to take the trip.
>
> (But how can they automate me? Goodness me!
> Asked Millie, the call girl from Philly.)
>
> Who'll keep the inventory up, who'll order the supplies
> Of paper towels, linens, iron pipe, or railroad ties?
> Executives now do this with a steno and a phone,
> But big computers soon will make decisions all alone.
>
> (They cannot cybernate me, tee hee!
> Laughed Alice, the hooker from Dallas.)
>
> Machines will teach our children how to read and add and spell;
> Because they've lots of patience, they will do it very well.
> If business men and managers are not on the alert,
> Their functions will be taken on by CPM[2] and PERT.[3]
>
> (I'll never be coded in FORTRAN[4]—whee!
> Cried Susie, the Hackensack floozie.)
>
> CHORUS OF CHARLOTTE, MILLIE, ALICE, AND SUSIE
>
> The future will be like the past despite all dire foreseeings;
> We stoutly shall defend the human use of human beings.
>
> 1 Electronic Recording and Machine Accounting.
> 2 Critical Path Method.
> 3 Program Evaluation and Review Technique.
> 4 Formula Translation.

See also Auden, "The Unknown Citizen," in MODERN POETRY 206-07 (2d ed., paper, 1961):

> He was found by the Bureau of Statistics to be
> One against whom there was no official complaint,

tion may give rise to an "underground" movement, reminiscent of the Luddites, to sabotage society's machines, perhaps by violating contemporary society's eleventh commandment: "Do not fold, bend, spindle, or mutilate."[126] In fact, one federal court has found it necessary to grant an injunction restraining a civil rights group from defacing an electric company's punchcard bills as a means of protesting the company's hiring policies.[127] Student activists have taken note of the new technology and have vented their anger on the computer and its trappings as symbols of the dehumanization of modern mass education.[128]

Perhaps little attention should be paid to such aberrational and atavistic behavior. After all, there is little doubt that the new technology actually promotes a number of vital humanistic concerns in our society, and it may even prove to be essential to the proper functioning and preservation of our representative form of government.[129] Moreover, the ability to present a parade of horribles does not

---

And all the reports on his conduct agree
That, in the modern sense of an old-fashioned word, he was a saint.
For in everything he did he served the Greater Community.
Except for the War till the day he retired
He worked in a factory and never got fired,
But satisfied his employers, Fudge Motors Inc.
Yet he wasn't a scab or odd in his views,
For his Union reports that he paid his dues.
(Our report on his Union shows it was sound)
And our Social Psychology workers found
That he was popular with his mates and liked a drink.
The Press are convinced that he bought a paper every day
And that his reactions to advertisements were normal in every way.
Policies taken out in his name prove that he was fully insured,
And his Health-card shows he was once in hospital but left it cured.
Both Producers Research and High-Grade Living declare
He was fully sensible to the advantages of the Instalment Plan
And had everything necessary to the Modern Man,
A phonograph, a radio, a car and a frigidaire.
Our researchers into Public Opinion are content
That he held the proper opinions for the time of year;
When there was peace, he was for peace; when there was war, he went.
He was married and added five children to the population,
Which our Eugenist says was the right number for a parent of his generation.
And our teachers report that he never interfered with their education.
Was he free? Was he happy? The question is absurd:
Had anything been wrong, we should certainly have heard.

126. Michael, *supra* note 110, at 284-85:

If the computerized world of tomorrow produces the kinds of rationalized standards which increase one's frustration and inhibition, then certainly this invasion of one's right to hope (*i.e.*, to fantasy antisocial success) will be interpreted as some kind of invasion of his personal freedom. If so, there most certainly will be an acceleration of a trend already under way: "Frustrate" the machines. In a spirit of desperation and vengeance people are bending punchcards, filling prepunched holes, and punching out additional ones. . . .

127. Potomac Elec. Power Co. v. Washington Chapter of C.O.R.E., 210 F. Supp. 418 (D.D.C. 1962).

128. TIME, Feb. 21, 1969, at 39; N.Y. Times, Feb. 12, 1969, at 3, col. 3.

129. Shubik, *Information, Rationality, and Free Choices in a Future Democratic Society*, DAEDALUS, Summer 1967, at 771, 777:

The influence of the high-speed digital computer upon society cannot be

provide a basis for jettisoning the technological developments of the past three decades. Nor does it advance the task of fashioning workable limits to preserve essential privacy values in a society that is increasingly oriented toward science and technology.

Nevertheless, the breadth of concern over the dehumanization of modern society and the animus directed at the computer cannot be ignored. The omnipresence of the computer cannot help but have a numbing effect on the congeries of values we subsume under the heading "personal privacy." Generations of children reared in an environment of terminals, punchcards, and computer assisted instruction cannot help but have a set of attitudes and values different from those of the present population, unless some effort is made to infiltrate the curriculum of the future with at least a minimal level of privacy indoctrination.[130] As Richard L. Tobin commented in a *Saturday Review* editorial captioned "1984 Minus Sixteen and Counting," "we cannnot assume . . . that privacy will survive simply because man has a psychological or social need for it."[131]

IV. Balancing the Efficiency Interest

It should now be apparent that it is necessary to undertake a thorough examination of the vehicles that the advocates of efficiency and economy have used to bring about the present trends in computer use. We also must probe the legitimacy of their objectives, and ultimately decide how best to achieve some equilibrium between these forces and the desiderata of personal privacy. In this section of the Article, two applications of information technology—one from the public sector and one from the private sector—will be dissected in the hope of shedding some light on the nature of the conflicting considerations. The proposal for a National Data Center and the activities of private credit bureaus were selected be-

underestimated. If we wish to preserve even modified democratic values in a multi-billion-person-society, then the computer, mass data processing, and communications are absolute necessities. . . . The computer and modern data processing provide the refinement—the means to treat individuals as individuals rather than as parts of a large aggregate.

The treatment of an individual as an individual will not be an unmixed blessing. Problems concerning the protection of privacy will be large.

See also Sherill, *Instant Electorate*, Playboy, Nov. 1968, at 155; Miller, *The Town Meeting Reborn*, Sat. Rev., July 23, 1966, at 34.

130. Miller, Privacy Implications of Instructional Technology—A Preliminary Overview 27-29 (undated) (unpublished paper prepared for the Study on Instructional Technology; copies are on file with the *Michigan Law Review*). *But cf.* Bettelheim, *The Right to Privacy Is a Myth*, Sat. Evening Post, July 27, 1968, at 8.

131. Sat. Rev., April 13, 1968, at 77-78. *See also* Maron, *Large Scale Data Banks*, 60 Special Libraries 3 (1969).

cause they present a cross-section of problems; numerous other computer applications also are spawning their own privacy problems and are in need of examination and prescription, but for present purposes the two chosen should suffice.

A. *The National Data Center*

The federal government long has been the nation's primary user of data-processing equipment; in fact, it was a government agency—the Bureau of the Census—that purchased the first commercial computer nearly two decades ago.[132] Reliance on data-processing was a natural response to the proliferation of citizen reports and data collection activities that are the inevitable by-product of expansive federal programs in health, social security, employment, taxation, and education. Administration of the social security and income tax programs alone necessitates more than 600 million annual reports.[133] Moreover, as noted earlier,[134] federal programs generate statistics that are becoming increasingly crucial as a foundation for sound social and economic research and policy-making. But these reports and statistics in turn beget additional reports and statistics, and the over-all effect is a seemingly unremitting stream of data engineered by some diabolical Sorcerer's Apprentice.

Computerized statistical and information systems have a vital role when the government commits itself to the solution of problems requiring analysis and correlation of a large number of factors. In these contexts, the computer's ability to manipulate vast bodies of detailed information permits the testing of hypotheses by using a greater mass of data concerning a larger number of potentially relevant variables encompassing longer periods of time than has hitherto been feasible.[135]

As federal agency functions currently are arranged, however, only one government bureau, Census, has the collection and analysis

132. *House Hearings on the Computer and Invasion of Privacy* 198.

133. HOUSE COMM. ON POST OFFICE AND CIVIL SERVICE, THE FEDERAL PAPERWORK JUNGLE, H.R. REPT. No. 52, 89th Cong., 1st Sess. 12-13 (1965) [hereinafter THE FEDERAL PAPERWORK JUNGLE].

134. *See* notes 51-52 *supra*.

135. *See generally The Design of a Federal Statistical Data Center* in *House Hearings on the Computer and Invasion of Privacy*, appendix C, at 288:

> Acceptable prediction under changing circumstances requires analytical models which give much more detailed and explicit recognition to interrelationships among the criteria and variables which will be affected by the changed conditions. Such analytical models generally describe the mechanisms in greater detail than associative models; they use more information, and they often rely less heavily on trends or the postulation of only slow changes among the variables in the model. The present and prospective accelerated pace of technological and statistical change now requires the development and use of more detailed and complex models than can be created or supported by the present Federal statistical system.

of statistics as its principal goal. The other agencies generate statistics only as an incident of their operations, and frequently fail to preserve data that might be valuable to some other governmental or private organization. Moreover, effective information practices are prevented because some agencies, such as the National Aeronautics and Space Administration and the Atomic Energy Commission, must operate under relatively stringent confidentiality requirements that preclude the general release of data.[136] A decentralized system also creates obstacles to the user of statistics; some government data is classified, and available collections of data often are almost impossible to locate, are arranged inconveniently for access and analytical purposes, or are difficult to compare because of differences in agency procedures.[137] With the possible exception of the Committee on Scientific and Technical Information (COSATI) of the Federal Council of Science and Technology,[138] there is no single government organization that can provide a reference guide to the kinds and locations of information being collected. COSATI also seems to be the only body that is directly concerned with the quality of the Government's information activities, despite the fact that the Government expends over one billion dollars annually in information activities.

These deficiencies in the federal government's information activities have several deleterious side-effects. First, the duplication of effort and time wasted in locating data and translating it into a form that is functional for second and subsequent users means a reduction in the over-all efficiency of governmental operations and an increase in its cost. Second, duplication in information collection often means an unnecessarily high and repetitious reporting burden on individuals and institutions.[139] Third, large quantities of useful

136. *Review of Proposal for a National Data Center* in *House Hearings on the Computer and Invasion of Privacy*, appendix 2, at 260-64. *See also id.* at 199, 201; *Senate Hearings on Computer Privacy* 28-29; *cf.* Sawyer & Schechter, *Computers, Privacy, and the National Data Center: The Responsibility of Social Scientists*, 23 THE AMERICAN PSYCHOLOGIST 810, 813 (1968):

> The major advantages a national data center holds for research are that (a) more data will be available, (b) data will be available more cheaply, (c) data will be available for more and better sampled respondents, (d) data collection will be less redundant, (e) variables will be more comparable, (f) variables will cover more areas, and (g) analyses will be easier to verify.

137. *See* note 96 *supra*.

138. *See generally* COMMITTEE ON SCIENTIFIC AND TECHNICAL INFORMATION OF THE FEDERAL COUNCIL FOR SCIENCE AND TECHNOLOGY, PROCEEDINGS OF THE FORUM OF FEDERALLY SUPPORTED INFORMATION ANALYSIS CENTERS (1967). The need for the development of an over-all information policy on the federal level is discussed by the chairman of COSATI in A. Aines, The Quest for National Policies for Information Systems (Feb. 18, 1969) (unpublished mimeo).

139. *See* Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 217-18 (1968).

data never see the light of day and never reach government users who would be advantaged by its availability. There is a significant store of data hidden away in the interstices of the governmental structure that could be utilized profitably in endeavors such as the quest for consumer protection; government information pools of this sort—and nongovernmental data bases of comparable character—should be made readily available to those people who are particularly vulnerable to or concerned about various social problems. All things considered, therefore, it was eminently logical for the Bureau of the Budget to take a moderate step toward reform by proposing the creation of a single federal statistical center that would relieve the operating agencies of the task of generating statistics and centralize the existing diffused bodies of data in one location.[140]

But the data center proposal became a lightning rod for the vague feelings of discontent and apprehension generated by the computer revolution. First Congress,[141] then the newspapers[142] and magazines,[143] and finally the law reviews[144] took turns castigating the idea, often in emotive or highly symbolic terms. To a degree, the clamor was most fortunate; the original proposals were incredibly myopic in their obsession with efficiency. For example, none of the three reports recommending establishment of a federal data bank gave the problem of privacy more than token attention and despite early protestations to the contrary, proponents of the data center later admitted that individual identification would have to be linked to data deposited in the center[145]—an admission that has enormous implications for individual privacy. One of the chief advocates of the center subsequently characterized this failure to

140. The proposal to create a federal data center was advanced in a series of three reports: Report of the Committee on the Preservation and Use of Economic Data to the Social Science Research Council (April 1965) (Ruggles Report), reprinted in *House Hearings on the Computer and Invasion of Privacy* 195-254; Statistical Evaluation Report No. 6—Review of Proposal for a National Data Center (Dunn Report), reprinted in *House Hearings on the Computer and Invasion of Privacy* 254-94; Report of the Task Force on the Storage of and Access to Government Statistics (Kaysen Report), reprinted in *Senate Hearings on Computer Privacy* 25-37.

141. *See generally House Hearings on the Computer and Invasion of Privacy*; *Senate Hearings on Computer Privacy*; *Senate Hearings on Computer Privacy*, pt. 2; 112 CONG. REC. 19,961 (Aug. 18, 1966).

142. *See, e.g.*, Labor, April 13, 1968, at 8, col. 1; N.Y. Times, July 28, 1966, § C, at 18, col. 1; *id.*, July 27, 1966, § M, at 33, col. 4.

143. *See, e.g., Chains of Plastic*, NEWSWEEK, Aug. 8, 1966, at 27; *A Government Watch on 200 Million Americans?*, U.S. NEWS & WORLD REPORT, May 16, 1966, at 56; Miller, *The National Data Center and Personal Privacy*, THE ATLANTIC, Nov. 1967, at 53.

144. Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400 (1968); Project, *The Computerization of Government Files: What Impact on the Individual?*, 15 UCLA L. REV. 1371 (1968).

145. *See House Hearings on the Computer and Invasion of Privacy* 52, 59, 97-98.

come to grips with the privacy question as "a gigantic oversight."[146]

Nonetheless, the failure of the center's proponents to give detailed consideration of the privacy question does not represent, as some suggested, a disregard of human values or evidence of bureaucratic bad faith. The proposals envisioned only a statistical center and they were limited in scope; thus, if the potential for expansion and individualization of the center's files is put to one side, reasonable men might view the threat to individual privacy as a relatively remote one. Moreover, until the contours of the center were more sharply delineated, the forms in which invasions of privacy might occur would remain obscure, making it difficult to formulate precise proposals for protection.

In the course of the congressional debate it became clear that the decentralized nature of the federal reporting system, which the statisticians and social scientists derisively characterized as inefficient, serves as one of the basic safeguards against the compilation of extensive government dossiers on each citizen.[147] Indeed, its maligned inefficiency virtually assures that. And, although proponents of the data center were astute to point out the excellent record of protecting sensitive information compiled by some federal agencies, most notably the Census Bureau, the dialogue also revealed that several federal agencies and bureaus had a less enviable past history in the privacy arena.[148] Moreover, it became apparent that the bodies of information that ultimately would find their way into the proposed data bank would be "orders of magnitude more sensitive than those now at the Bureau of the Census,"[149] with each failure of security likely to be "many times more destructive to an individual."[150] Chastened by the public outcry, the statisticians and administrators retreated to reconsider their proposal and to investigate the safeguards that would be necessary to render a National Data Center more palatable.[151]

146. Dunn, *The Idea of a National Data Center and the Issue of Personal Privacy*, reprinted in *Hearings on Statistical Programs* 32, 35.

147. *Cf. Senate Hearings on Computer Privacy* 74.

148. *See generally* notes 546-47 *infra*.

149. HOUSE COMMITTEE ON GOVERNMENT OPERATIONS, PRIVACY AND THE NATIONAL DATA BANK CONCEPT, H.R. REPT. No. 1842, 90th Cong., 2d Sess. 14 (1968) [hereinafter PRIVACY AND THE NATIONAL DATA BANK CONCEPT].

150. *Id.* at 11.

151. The House Committee on Government Operations recently recommended that "no work be done to establish the national data bank until privacy protection is explored fully and guaranteed to the greatest extent possible to the citizens whose personal records would form its information base." PRIVACY AND THE NATIONAL DATA BANK CONCEPT 6. *See also* Zwick, *A National Data Center*, in ABA SECTION OF INDIVIDUAL RIGHTS AND RESPONSIBILITIES, MONOGRAPH No. 1, at 32 (1967):

> There does not exist today . . . a fully developed plan for a National Data Center.

This apparent victory in the fight to preserve privacy, however, probably has been a Pyrrhic one. Information collections prepared for statistical purposes, which bore the brunt of the outcry during the data center controversy, comprise only about one fifth to one third of the reports extracted from citizens.[152] Thus, the public debate never really reached the question of preserving the integrity of the bulk of the sensitive data held by the government and the problem of regulating the government's penchant for increased information collection. Moreover, purely statistical studies generally do not contain sensitive data of the type that is attractive to snoopers; therefore, they are somewhat easier to protect against intrusion than investigative files, although the claimed distinction between statistical systems and surveillance systems[153] does not appear to be particularly valid.[154]

Ironically, the failure to establish a data center under a legislative mandate to take the steps necessary to protect individual privacy may undermine individual privacy if nothing is done to curb the present tendency of each federal agency to "constitute itself a data center."[155] The legal authority for this pattern already exists. The Administrator of the General Services Administration (GSA), for example, has statutory power to establish interagency pools of data-processing equipment and facilities,[156] and the

And without a carefully developed plan the Administration has no intention of creating a Data Center. Furthermore, the Administration is committed to obtaining congressional approval before it would proceed to activate a National Data Center.

152. THE FEDERAL PAPERWORK JUNGLE 18.

153. *E.g., House Hearings on the Computer and Invasion of Privacy* 92-93 (statement of Edgar S. Dunn, Jr., research analyst, Resources for the Future, Inc.):

> The distinction is basic. Intelligence systems generate data about individuals as individuals. They have as their purpose "finding out" about the individual. . . .
>
> . . . .
>
> [A] statistical system is busy generating aggregates, averages, percentages, and so forth that describe relationships. No information about the individual is generated.
>
> No information about the individual needs to be available to anyone under any circumstances for the statistical information system to perform its function.

154. *See House Hearings on the Computer and Invasion of Privacy* 112, 142; *Senate Hearings on Computer Privacy* 67-68.

155. *House Hearings on the Computer and Invasion of Privacy* 61. *See also* remarks of Rep. Gallagher on H.R. 7659 (authorizing a middecade census), 113 CONG. REC. 10,383 (Aug. 10, 1967): "[N]o matter what name the Census Bureau gives to its 'information system,' what it is actually creating is a very complete and thorough National Data Bank."

156. Pub. L. 89-306, 79 Stat. 1127, § 111(b)(1) (1965):

> The Administrator is authorized to transfer automatic data processing equipment between Federal agencies, to provide for joint utilization of such equipment by two or more Federal agencies, and to establish and operate equipment pools and data processing centers for the use of two or more such agencies when necessary for its most efficient and effective utilization.

See also id. § 111(g).

Deputy Administrator of the GSA has testified that "the most effective and economical" way to implement this authority is to augment existing computer equipment with the ultimate purpose of providing several agencies with "huge multiaccess, remote control, time sharing systems" servicing other agencies.[157] Moreover, the Secretary of Commerce has authority to develop uniform federal standards for data-processing,[158] and at present "a major standardization effort" is underway "to provide a universal language of machine intercommunication."[159] Finally, many of the panels and task forces operating under COSATI are addressing themselves to the facilitation of transmitting data among agencies and the improvement of access to federal information by various governmental and nongovernmental institutions and people.

At this writing approximately twenty federal agencies, bureaus, and departments operate time-sharing computer systems or are in the process of establishing them.[160] The system that currently is handling personal medical records in the Social Security Administration provides a rather graphic example of what we can expect in the future:

> The Social Security Administration [has a] . . . policy of storing in a computer in the Social Security Administration Headquarters, Baltimore, the basic data indicating the social security status of every

157. *Hearings on Data Processing Management in the Federal Government Before a Subcomm. of the House Comm. on Government Operations*, 90th Cong., 1st Sess. 54-55 (1967) [hereinafter *Hearings on Data Processing Management*].

158. Pub. L. 89-306, 79 Stat. 1128 § 111(f) (1965):

> The Secretary of Commerce is authorized . . . to make appropriate recommendations to the President relating to the establishment of uniform Federal automatic data processing standards. The Secretary of Commerce is authorized to undertake the necessary research in the sciences and technologies of automatic data processing computer and related systems, as may be required under the provisions of this subsection.

159. *Hearings on Data Processing Management* 72 (statement of A. V. Astin, Director of the National Bureau of Standards). *See also id.* at 25 (statement of Phillip S. Hughes, Deputy Director of the Bureau of the Budget):

> A number of important data processing standards have already been approved for voluntary use under the programs of United States of America Standards Institute; and these are now under consideration for adoption as Federal standards in which their use, with few exceptions, would become mandatory upon Federal agencies. . . .
>
> The development of greater compatibility among hardware and software will, however, solve only part of the problem related to the more effective development of our information systems. There still remains the need to develop greater compatibility among the data that is being exchanged. . . . To meet this problem, the Bureau of the Budget is formulating a Government-wide program for standardizing data elements and codes in those cases where standardization is essential.

160. Statement on Behalf of the Customer Interest of the Executive Agencies of the United States 9-27 (submitted in connection with *In re* Regulatory and Policy Problems Presented by the Interdependence of Computer and Communications Services and Facilities, FCC Docket No. 16,979) (March 5, 1968).

citizen with a social security registration. This has now been extended to equivalent records on all phases of the Medicare program.

. . . [T]he Social Security Administration has established some 725 field offices throughout the United States. Registrants visit or write to these field offices for information concerning their Social Security or Medicare status, or to apply for payments under the respective programs. Each such inquiry or application typically results in a communication to Baltimore. . . .

. . . [E]ach field station is equipped . . . with automatic transmitters, that transmit or receive at 100 words per minute. . . . [The information] is sent via high-speed, dedicated circuits to Baltimore, where it is received on magnetic tape ready for input to the Social Security Administration's computer. . . .

The Social Security Administration also maintains magnetic-tape-to-magnetic-tape transmissions systems from the National Blue Cross Headquarters to Baltimore.[161]

The growth of interconnected systems will enable the government to coordinate the information-gathering programs of the various agencies and to foster the sharing of data bases.[162] Since the Bureau of the Budget does have extensive authority to promote these activities,[163] it is apparent that as soon as enough agency interfaces

161. Johnson, *Computers and the Public Welfare—Law Enforcement, Social Services and Data Banks*, in COMPUTERS AND COMMUNICATIONS—TOWARD A COMPUTER UTILITY 173, 187-88 (1968).

162. *See, e.g., Hearings on Data Processing Management* 5 (statement of Elmer B. Staats, Comptroller General of the United States):

> We believe that, as third-generation systems grow and as data communications systems develop, the concept of sharing of large data bases and programs will come into play to such a significant degree that only through the greatest coordination of effort on a Government-wide, or, at least, on an interagency basis will we be able to avoid extensive duplication of effort in designing and redesigning of systems in future periods.

Congressman Roman Pucinski of the House Education and Labor Committee has actively pursued the idea that a national data-processing and retrieval system should be established under federal auspices to serve to integrate private and governmental information networks. H.R. 8809, 91st Cong., 1st Sess. (1969).

163. The Budget Bureau's powers were summarized as follows in SUBCOMM. ON ECONOMIC STATISTICS OF THE JOINT ECONOMIC COMM., 90th Cong., 1st Sess., REPORT ON THE COORDINATION AND INTEGRATION OF GOVERNMENT STATISTICAL PROGRAMS 8 (Joint Comm. Print 1967) (emphasis added):

> The major responsibility for the coordinating function is with the Bureau of the Budget through its Office of Statistical Standards. Legislation provides the Bureau with strong backing for its task of coordination. The Budget and Accounting Procedures Act of 1950 in Title I, Part I, Section 103, states that "The President, through the Director of the Bureau of the Budget, is authorized and directed to develop programs and to issue regulations and orders for the improved gathering, compiling, . . . and disseminating of statistical information. . . . This provision of law is carried out under Executive Order 10253.
>
> Specific authority is also provided by the Federal Reports Act of 1942 for the Director of the Bureau of the Budget (a) to transfer the responsibilities for the collection of statistical information from one agency to another, and with certain safeguards, *to transfer information among agencies to avoid duplication and promote efficiency*; and (b) to review, and approve or disapprove, . . . proposals by Federal executive agencies for obtaining information from the public.

Cf. House Hearings on the Computer and Invasion of Privacy 197.

are established a system roughly equivalent to, and perhaps even more all-embracing than, a National Data Center will exist, even though it may not be denominated as such.

The prospect of an omnibus, de facto federal data center evolving without prior comprehensive congressional review or any defined obligation to protect privacy is not a happy one in view of past revelations about some government information-handling practices. Perhaps most disheartening is the fact that the existing controls on the type and volume of information that may be exacted from the public seem to have been largely ineffectual. The Federal Reports Act[164] provides that federal agencies must obtain clearance from the Director of the Bureau of the Budget before collecting data from ten or more persons. Clearance is rarely denied;[165] indeed, the Budget Bureau has been known to act as an advocate as well as a judge, intervening in Congress to obtain support for certain information-gathering projects.[166] Even this highly permissive procedure is thought to be unduly burdensome by some agencies, however, and on occasion they have circumvented the Federal Reports Act by failing to obtain clearance for data-gathering done for them by independent contractors.[167] Agencies also may evade the clearance requirements by securing bodies of data from federally financed state agencies under the threat of withholding funds,[168] or by claiming exemptions from the requirements of the Act.[169]

Moreover, Congress' ultimate power over appropriations, which was advanced as a practical control mechanism on the nature of the information that might be stored in the proposed federal data center,[170] hardly seems capable of remedying deficiencies in the

---

164. 5 U.S.C. § 139 (1964).

165. THE FEDERAL PAPERWORK JUNGLE 14-15.

166. *Id.* at 39.

167. HOUSE COMM. ON POST OFFICE AND CIVIL SERVICE, STATISTICAL ACTIVITIES OF THE FEDERAL GOVERNMENT: PERSONNEL, EQUIPMENT, AND CONTRACT COSTS, H.R. REPT. 1130, 88th Cong., 2d Sess. 31 (1964).

168. THE FEDERAL PAPERWORK JUNGLE 94-95:

> Since federally supported State programs have mushroomed in recent years, we are faced with rapidly expanding reporting and paperwork programs which, for all practical purposes, fall outside of any Federal or State supervision. This situation lends itself to all kinds of abuses since the Federal agency can threaten the state agency by withholding funds unless all of its demands for information are met.

See also id. at 84.

169. *Id.* at 87: "Although the regulatory agencies are not specifically exempted from the Federal Reports Act (as are the fiscal and banking agencies), they claim that their organic acts give them full authority to collect information from the public . . . ."

170. *See, e.g., Senate Hearings on Computer Privacy* 5 (statement of Carl Kaysen, Director, Institute for Advanced Studies, Princeton University).

conduct of a number of individual agencies. Appropriation levels generally are determined on the basis of an over-all view of agency programs without any significant consideration of the reporting requirements that may be involved. In any event, appropriations committees usually are more concerned with agency personnel requests than with the minutiae of proposed programs.[171] The limited attention Congress gives to agency information practices should not be surprising in light of the fact that top-level administrators often are unaware of the amount and kinds of information that their own agency demands from the public.[172]

Another fact of federal agency life that argues against allowing interagency computerized information pools to grow without supervision is that governmental data gatherers may abuse their statutory data collection powers. A recent survey by a congressional subcommittee revealed many instances of excesses and concluded that "the majority of government forms require either nonessential or too detailed information from the individual citizen."[173] In addition, agency information collectors may deceive the public into believing that they are required by law to respond to reports that in fact are voluntary; "in their zeal to increase the coverage and accuracy of a survey," one report concluded, "administrators have been known to use deceptive language in the wording of their questionnaires" to coerce responses.[174]

171. THE FEDERAL PAPERWORK JUNGLE 98.

172. *Id.* at 14.

173. SUBCOMMITTEE ON ADMINISTRATIVE PRACTICE AND PROCEDURE OF THE SENATE COMMITTEE ON THE JUDICIARY, 90TH CONG., 1ST SESS., GOVERNMENT DOSSIER 8 (Comm. Print 1967) [hereinafter GOVERNMENT DOSSIER]. *See also* Okun, *Investigation of Jurors by Counsel: Its Impact on the Decisional Process*, 56 GEO. L. J. 839, 852-53 (1968):

> When the United States is a litigant it is the FBI which appears to play the major role in investigation of jury panels. . . . While the approaches and goals of the FBI are basically similar to those of private detective agencies, there are several factors which distinguish the FBI investigation. It has access to information which is usually beyond the reach of the commercial investigator. A given United States Attorney may feel that knowledge of the financial lives of the prospective jurors will be valuable in impaneling the jury. The FBI will probably be able to secure for him information from banks, stock brokerage firms, insurance companies, and other institutions which would not make available their records to the private investigator.
>
> . . . The guess may be ventured that in the overwhelming number of cases mere display of FBI credentials is a guarantee of rather full disclosure of all information sought. Moreover, the FBI is subject to no practical limitations on the type of inquiry it conducts or the extent thereof.

174. The FEDERAL PAPERWORK JUNGLE 36. *See also id.* at 33:

> On the surface it would appear that all Federal requests for information are "authorized" by law, since the Appropriations Committee must approve the funds for such activities and Congress must pass the appropriation acts for the departments and agencies. In fact, as brought out in subcommittee hearings, the general public often is misled into believing that all Federal reports are mandatory and, in cases of doubt, the respondent often feels "safer" if he complies with the request.

See also text accompanying notes 359-62 *infra*.

The deficiencies of the existing system of government information-handling and the threat of unrestrained expansion of computerization by the agencies are not simply problems of the unauthorized procurement of data. The information that is exacted, whether procured legally or not, often is taken without any assurance that it will be handled on a confidential basis; if the agency does make a pledge, it is a virtually meaningless one not to release the information outside of the government.[175] It is highly unrealistic to expect the donor of the data to have any accurate conception of the uses to which it will be put or the potential audience to which it will be exposed. Even if confidentiality restrictions control a particular agency's activities, they are likely to reflect little more than ad hoc judgments rather than a carefully developed statutory or regulatory system for protecting citizen privacy.[176] Those safeguards that do exist often are vitiated by the propensity of bureaucrats to cooperate with each other in exchanging information of the most sensitive nature.[177]

The reports of past excesses would be understandable, perhaps pardonable, if they had resulted solely from efforts to obtain data that is essential to the solution of pressing social problems. Often, however, this has not been the case. As a congressional subcommittee revealed, "a number of surveys are conducted at the request (and often at the expense) of industry groups, trade associations, and often business organizations."[178] Big business easily can absorb the cost of replying to myriad governmental questionnaires, and can hire the analysts and marketing experts necessary to make profitable use of government statistics.[179] On the other hand, the burden on small businessmen is a heavy one and they receive little or no

175. GOVERNMENT DOSSIER 8.

176. *See* BUREAU OF THE BUDGET, REPORT OF THE TASK FORCE ON THE STORAGE OF AND ACCESS TO GOVERNMENT STATISTICS, reprinted in *Senate Hearings on Computer Privacy* 25, 27-28, noting that in some agencies, "formal policies regarding disclosure have not been set up, and in many of these cases the protection depends on the judgment of those who are in charge of the different programs involved."

177. *See, e.g.*, Packard, *Don't Tell It to the Computer*, N.Y. Times, § 6 (Magazine), Jan. 8, 1967, at 44, 89:

> Federal agencies have also developed increasingly systematic patterns for exchanging information. When a Federal agent makes a National Agency Check on a person, for example, he customarily checks the files of at least eight Federal agencies. A Congressional investigator reported that the results of lie-detector tests taken by one agency were freely passed around to personnel officials in other agencies. And we know that various government units are developing a central information center to exchange information on individuals involved in criminal investigations.

Cf. Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 218-19 (1968).

178. THE FEDERAL PAPERWORK JUNGLE 39.

179. *Id.* at 64.

direct benefit from these statistical programs.[180] Ironically, when individual citizens become outraged enough to complain about the torrent of questionnaires, federal information managers often turn these supplications to their own advantage by requesting increased computer power and the authority to share bodies of data in order to "ease the burden on respondents." As might be expected, this argument was advanced by the advocates of the National Data Center.[181]

Of course, past abuses are not a justification for abolishing or drastically reducing the government's statistical or information activities. As stated above, extensive gathering and analysis of information is essential to the functioning of a highly complex society. However, past history does afford ample reason to be skeptical of demands for more information and facile assertions that the establishment of computerized government data centers will increase the protection given to individual records. The claim that these centers will make it easy and desirable to purge stale records because computer storage costs are relatively high no doubt has validity;[182] it becomes less persuasive, however, when considered in light of congressional findings that the mounting cost of storing paper records already is necessitating the destruction of stale data,[183] and that "computer technology shares the responsibility for increasing Federal reporting requirements."[184] This is consistent with the notion advanced earlier[185] that the very expansion of data-handling capacity tends to encourage an expanded appetite for information.

The denouement of the original proposal for a National Data Center and the debate over it should indicate that isolated re-

180. *Id.* at 41.

181. *See, e.g., Senate Hearings on Computer Privacy* 42-43 (statement of Charles J. Zwick, Assistant Director of the Bureau of the Budget); *House Hearings on the Computer and Invasion of Privacy* 49-50 (statement of Raymond T. Bowman, Assistant Director for Statistical Standards, Bureau of the Budget). *See also* Ruggles, *supra* note 177, at 217-18.

182. *House Hearings on Commercial Credit Bureaus* 89 (statement of H. C. Jordan, President of Credit Data Corp.):

> One of the statements which I hear most often with respect to computerized data banks is that a computer is unable to forget, and as a result of this mechanical "total recall" an individual is never able to redeem himself. . . .
>
> While the above is technically possible, it is neither desirable nor economically feasible. Unlike old-fashioned paper files, where storage is very cheap but removal of data is very expensive, in the case of the computer file, storage is very expensive and selective removal is very cheap. . . . Consequently, the storing of information which is old and outdated simply cannot be permitted. On the other hand, it is possible to review all of the data in a computer file within a few hours to remove that which is outdated.

183. THE FEDERAL PAPERWORK JUNGLE 49-52.

184. *Id.* at 47.

185. *See* text accompanying notes notes 41-42 *supra.*

action to individual information-gathering proposals will not end the growing incursions on personal privacy that are a natural by-product of the increased level of federal data collection. But the episode also confronts us with an interesting dilemma. If defeat of the National Data Center simply encourages the proliferation of unregulated intra-agency data centers and machine interfaces among the various agencies, then the cure may be more dangerous than the disease. The more attractive alternative appears to be a data center that is functionally circumscribed and is structured to place a heavy premium on privacy considerations. Prior to establishing such a center, the government's information policies must be comprehensively evaluated in the hope of achieving an over-all balance between the need for massive amounts of raw data that can be handled efficiently and used for a variety of purposes and the obligation of the national government to preserve the privacy of its citizens. Moreover, this evaluation must be a continuing one in order to keep pace with changing agency practices in the collection and use of data.

B. *The Computerized Credit Bureau*

The privacy implications of the increase in credit information services in the private sector have received almost as much attention in the recent past as has the proposal to establish a National Data Center. Buying on credit has become an integral part of daily life in the United States, and the number of credit consumers and the amount spent annually on credit purchases are steadily increasing.[186] Along with the new pace of credit transactions, the urbanization and mobility of the population has made it necessary for most credit grantors to base their decisions on information gathered by credit bureaus rather than on personal knowledge of the borrower as was true in more halcyon days.

The vast majority of people willingly (and often unthinkingly) supply lenders and credit bureaus with substantial quantities of personal information in order to obtain the benefits of the credit economy.[187] To augment this data, many credit bureaus also regularly comb newspapers, court records showing the institution of lawsuits, and other public files for bits of personal data that might be relevant to the decision about whether an individual is an acceptable credit

186. The growth of credit buying is documented in H. BLACK, BUY NOW, PAY LATER (1961). Each month approximately eight billion dollars worth of credit is extended in the United States. TIME, Dec. 20, 1968, at 79.

187. *See, e.g.*, Michael, *Speculation on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 53 GEO. WASH. L. REV. 270, 275 (1964).

risk.[188] In some instances this information is further supplemented with reports on a person's payment habits received by the bureaus from the previous credit grantors, and perhaps by reports of field investigators who check on the subject's status in the community. These activities and the pool of information they create pose substantial access and accuracy problems of the type discussed earlier.[189]

The credit-reporting industry's record of protecting personal privacy has been extremely spotty. Testimony presented to congressional subcommittees indicates that some of the practices of the retail credit-reporting associations—companies that cater primarily to insurance companies and employers—are subject to sharp criticism.[190] In addition to the activities described in the preceding paragraph, they engage in a fair amount of surveillance and rely on information gathered from third persons. As might be expected, these reports usually contain hearsay narratives gleaned from quick interviews with neighbors, landlords, employers, and "friends" conducted by poorly paid, relatively unsophisticated, and frequently insensitive functionaries.[191] By way of defense, in many cases it probably is true that the bureaus seek sensitive information only because their clients have requested it.[192] And, it is probably true that they

188. *See, e.g., Hearings on Commercial Credit Bureaus Before a Subcomm. of the House Comm. on Government Operations*, 90th Cong., 2d Sess. 125-26 (1968) [hereinafter *House Hearings on Commercial Credit Bureaus*].

189. *See* pt. III.A.-B. *supra.*

190. *See generally Hearings on Credit Bureaus Before the Subcomm. on Antitrust and Monopoly of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968) (These hearings have not been published as of this writing. General descriptions of them may be found in TIME, Dec. 20, 1968, at 79; N.Y. Times, Dec. 12, 1968, § 1, at 58, col. 2.); *Hearings on Commercial Credit Bureaus; Hearings on the Retail Credit Company Before the Subcomm. on Invasion of Privacy of the House Comm. on Government Operations*, 90th Cong., 2d Sess. (1968) [hereinafter *Hearings on Retail Credit Company*]. (These hearings have not been published as yet; page citations refer to the unofficial transcript.) *See also* note 218 *infra* and accompanying text.

191. *See, e.g.*, Sesser, *Big Brother Keeps Tabs on Insurance Buyers*, THE NEW REPUBLIC, April 27, 1968, at 11:

> Retail Credit officials are hesitant to discuss in detail their investigative techniques. But no such reluctance exists on the part of their main competitor, Hooper-Holmes Bureau Inc., which has files on nine million people. Hooper-Holmes and Retail Credit both say their operations are identical.
>
> . . . Frederick E. King, president of Hooper-Holmes, describes the procedure of an inspector suspicious of an extramarital affair: "You go to a neighbor and establish rapport," he says. "Then you ask, 'What's your opinion of X's home life; how do you think of him as a family man?' This will usually elicit some hint. . . . Then you start digging. You press them as far as they go, and if they become recalcitrant, you go somewhere else."

The president of Retail Credit Company has testified that their investigators customarily interview "[e]mployers, former employers, references, fellow club members, neighbors and former neighbors, [and] financial and professional people." *Hearings on Retail Credit Company* 52.

192. *See, e.g., Hearings on Retail Credit Company* 51 (testimony of W. Lee Burge, President of Retail Credit Co.):

> Life insurance companies want information which will be helpful in evaluating the applicant as a life insurance risk. This includes such matters as the appli-

do not record the disposition of a lawsuit against a file subject because it is very difficult to discover such information given the archaic filing practices of most courts.[193] But if the episodes recounted before Congress are any indication of the level of care being exercised by credit bureau investigators, or of their concern for privacy, it is clear that a substantial mass of dangerous and often inaccurate information has been gathered. This data undoubtedly is causing considerable damage to some individuals.[194]

In contrast to the retail credit bureaus, the commercial credit organizations—companies primarily designed to serve credit grantors[195]—claim to limit themselves to "hard" financial data that is less

---

cant's duties, his finances, his health history, the extent of his use of alcohol, his mode of living, and hazardous avocations. Automobile insurance companies, on the other hand, emphasize other factors, among them the ages and abilities of the drivers, the uses and condition of an automobile, distance driven, prior accidents, and the history, if any, of driving under the influence of alcohol. Similarly, there are varying requirements for information in connection with other types of business transactions, such as property lines of insurance, prospective employment, claims investigations, and marketing information.

193. *See, e.g.*, William J. Mangan, General Manager of the Credit Bureau of Greater Boston, Inc., Statement Before a Public Study Session of the Procedures and Practices of Credit Bureaus, Consumers' Council, Boston, Massachusetts, Oct. 15, 1968, at 7 (unpublished mimeo):

> We . . . copy from the local court houses filings of bankruptcies, divorces, attachments, and notices of supplementary process, which are a matter of public record, and we put this information into our files. . . .
>
> We have no difficulty picking up the filings of these matters because they are listed in the various records chronologically. We would like to pick up all dispositions on the same general basis, but it is impossible to do so. Daily dispositions are not available in a chronological listing; they are posted back to the original filing and we have no way of knowing which book to go to, let alone which page.

194. For example, an actual bonding report prepared by the Retail Credit Company was submitted to the House Subcommittee on Invasion of Privacy in conjunction with the *Hearings on Retail Credit Company*. The subject of the report, a retired army lieutenant colonel, was described as follows:

> He was known to be a rather wild tempered, unreasonable and uncouth person who abused his rank and wasn't considered a well adjusted person. He was known to roam the reservation at Ft. Hood and shoot cattle belonging to ranchers who had leased the grazing land from the Army.

Reports of this kind may be very common, in light of the company practices described by Retail Credit's President:

> We check the former employer. We check possibly his school record to determine what his record was in school if this is relevant to his particular employment situation. We check to see if he has certain characteristics that might be advantageous for that particular job.
>
> If, for example, he is a sales prospect, is he a man with an outgoing personality? Does he get along well with people, has he shown leadership characteristics and this sort of thing.
>
> Then, of course, we try to see if he has had job difficulty, difficulty holding a job, or if for any reason he hasn't gotten along well with his previous employers.

Hearings on Retail Credit Company 76 (testimony of W. Lee Burge, President of Retail Credit Corporation).

195. The distinction between "credit-reporting agencies" such as the Retail Credit Company, and "credit bureaus" serving retail merchants, such as the ACB, is discussed in *House Hearings on Commercial Credit Bureaus* 104-05. However, the distinction is far from sharp. For example, a wholly owned subsidiary of Retail Credit

vulnerable to objection.[196] But there is evidence that the commercial credit bureaus have been remiss in terms of limiting access to their files. As part of a television news report,[197] CBS News staff members created a fictitious "systems" company, which requested financial information from twenty commercial credit bureaus in various parts of the country. The reports requested were on people chosen at random from the telephone directories in the locale of the selected bureaus. The CBS company's letter simply indicated that it was interested in extending credit to a particular person residing in the area covered by the bureau that was contacted. Despite the vigorous assertions by Mr. John Spafford, Executive Vice President of Associated Credit Bureaus of America (ACB), a nationwide organization of independent credit bureaus, that it was "impossible" to secure a report from an ACB member bureau unless the requesting party was a "bona fide creditor," the fictitious CBS company received, "without further question," full reports from ten of the bureaus.[198] The experiment was repeated following the adoption of new ACB "Credit Bureau Guidelines To Protect Consumer Privacy," which require the signing of a contract in which the client certifies that inquiries will be made only for credit-granting purposes.[199] To make it even more difficult, the CBS letter of request did not indicate that the information sought was to be used for credit-granting purposes; moreover, credit reports were sought on people who had complained to congressional investigators about their credit problems. Nonetheless, seven out of twenty-eight of the selected bureaus provided the information without hesitation.[200]

In each sample group, some of the bureaus that did not comply with the initial request for a report stated in reply that they would

Company controls sixty credit bureaus, *Hearings on Retail Credit Company* 4, while the ACB makes its files accessible to more than 1,400 collection agencies. *Senate Hearings on Credit Bureaus* (Remarks of John L. Spafford, Executive Vice President of Associated Credit Bureaus, Inc., submitted Dec. 10, 1968).

196. *See, e.g., Senate Hearings on Credit Bureaus* (statements of Henry C. Jordan, President of Credit Data Corporation, and John L. Spafford, Executive Vice President of Associated Credit Bureaus, Inc.); *House Hearings on Commercial Credit Bureaus* 87-88.

197. CBS Evening News, March 17, 1969, reprinted in 115 CONG. REC. S3008-09 (daily ed. March 17, 1969) [hereinafter CBS News].

198. *Id.* at S3009.

199. Associated Credit Bureaus, Inc., Credit Bureau Guidelines To Protect Consumer Privacy, § C:

1. Credit bureaus shall require service contracts in which the regular subscriber or the occasional user certifies that inquiries will be made only for the purposes of credit granting or other bona fide business transactions. . . .
2. The bureau shall refuse service to any prospective subscriber or user who will not so certify.

200. CBS News at S3009.

furnish the information when the systems company signed a contract with them. In one case the fictitious company did this, and the information was immediately forthcoming, despite the fact that an investigation by the bureau would have revealed that the request did not come from a bona fide credit grantor. As CBS commentator Mike Wallace remarked: "It would seem that signing a written contract is not much of a safeguard; all the client has to do is lie."[201]

Even if the bureaus limit themselves to providing bona fide creditors with information about the financial history of consumers[202] and refrain from supplying derogatory or innuendo-filled tidbits,[203] the problem of how to insure the accuracy of the financial reports that reach the credit grantor remains. At present credit bureau practices are virtually unregulated. A simple notation describing the customer as "slow-pay," for example, can be extremely damaging, yet it may conceal an honest dispute in which the customer withheld payment in order to obtain the goods or services he bargained for in acceptable condition.[204] Once an error of this type finds its way into a file, it may be virtually impossible to correct, or even to discover.[205] One national organization, the Retail Credit

---

201. *Id.*

202. *See, e.g., House Hearings on Commercial Credit Bureaus* 110 (statement of John L. Spafford, Executive Vice President of the Associated Credit Bureaus of America):

> Some people mistakenly feel that the purpose of the credit bureau is to prevent individuals and families from obtaining credit. . . . On the contrary, the credit bureau, by providing factual information promptly and efficiently to credit grantors helps more people obtain more goods and services on credit.

203. *See* M. BRENTON, THE PRIVACY INVADERS 35 (1964), in which a credit bureau's manager is quoted as saying, "If everybody comes out white, the clients don't need us." It could be argued that a credit bureau which desires to maintain a reputation for accuracy will take measures to insure that its reports are truthful; but since the bureau's inaccuracy will be discovered only if credit is extended and the subject of the report subsequently defaults, it seems clear that the bureau's natural tendency would be to err on the side of supplying derogatory information.

204. *See Senate Hearings on Computer Privacy* 81 (statement of the author). *See also House Hearings on Commercial Credit Bureaus* 11 (testimony of Professor Alan F. Westin):

> I think all of us, as buyers and consumers, appreciate that withholding payment is our most effective leverage in getting the performance of the contract as we believe it has been made.
>
> But what may often happen, especially when hot words may be exchanged between the . . . dealer and the consumer, is that the seller may report this as simply nonpayment or slow payment. He may even take a certain amount of relish in the fact that the obnoxious lady on the telephone . . . is being fixed in the credit record . . . . It is an anonymous treatment, because the reporter of the information is never accountable for it.

205. *See, e.g.*, TIME, Dec. 20, 1968, at 79; The National Observer, March 3, 1969, at 1, col. 1.

Company, even has a provision in its contract prohibiting its customers from telling anyone that a credit report has been made.[206]

When the credit bureau is local, there may be a chance to learn about and correct inaccurate or misleading entries. However, these smaller, local bureaus seem destined to disappear. The average credit bureau using a manual file system is likely to be a relatively inefficient operation that will prove increasingly incapable of storing, updating, retrieving, and transferring[207] the information necessary to keep pace with the booming credit economy. Computer technology, mated with a high-speed transmission medium, is the ideal and inevitable method of improving the system. But this new equipment is expensive, and a trend toward large-scale credit information organizations already is evident.

As early as September 1965, Credit Data Corporation inaugurated a large on-line computerized credit information system in California. In 1967 that company linked its Los Angeles and San Francisco offices to provide, in effect, a statewide computer credit network. During the same year, Credit Data opened a computerized center in New York City, and plans are underway for another center in Detroit.[208] Credit Data responds to telephone inquiries from subscribers by reading a printout of the computerized

---

206. *Hearings on Retail Credit Company,* appendix A:

> All reports, whether oral or written, will be kept strictly confidential: except as required by law, no information from reports nor your identity as the reporting agency will be revealed to any other person except a person whose duty requires him to pass on the transaction in relation to which the report was ordered.

W. Lee Burge, President of Retail Credit Company, sought to justify this clause by explaining that "it is a protection to the sources of information." *Id.* at 31. He also described the tortuous process that an individual would have to go through in order to track down an error in a Retail Credit Company Report:

> Let me reconstruct a typical conversation between a personnel manager and a person who has just been declined a job.
>
> He might say "Why don't I get the job," and [the personnel manager would reply], "Because in our investigation we have found that through some of your previous employers you embezzled funds," and on the strength of this information he says, "Well, who made the investigation?" And the personnel man says, "I am not at liberty to divulge this."
>
> On the basis of this, then, the man begins to ferret around to find out who is likely to make investigations of this sort. Of course, we come to the forefront under circumstances like this simply because of our prevalence in the business information field.

Id. at 24-25. Obviously, the chances of an individual completing this process expeditiously are virtually nonexistent. *See* note 205 *supra.*

207. The importance of rapid retrieval and transmission is evident when it is realized that a computer system will enable data to be made available to a merchant quickly enough so that he can determine whether or not to grant credit before the customer leaves the premises or changes his mind about the purchase. *See Senate Hearings on Commercial Credit Bureaus* (statement of the author).

208. *See House Hearings on Commercial Credit Bureaus* 93, 147 (testimony of H.C. Jordan, President, Credit Data Corporation).

record on the potential borrower. The response time averages two minutes.[209]

At present, Credit Data serves lenders in a geographic area containing over thirty-five million people. It has computerized credit information on over twenty million Americans and is adding new files on approximately 50,000 Americans each week.[210] It is interesting to note that the company's original data base was secured by convincing a number of California banks to turn over their credit apparatus to them; Bank of America alone gave Credit Data eight million items.[211] It seems clear that Credit Data will continue to develop regional information nodes. It will then interconnect them by wire or microwave relay to establish a national credit information network. It also seems reasonable to forecast that large users of Credit Data's services will be provided with remote-access terminals permitting direct entry into the bureau's computerized files. This will greatly reduce the cost of having operators process individual telephone inquiries. Thus, a request for information at one point in the company's system would provide access to relevant data maintained at any other point in the network.

ACB has been working on computerization since August 1965, when research began on a real-time[212] computer system for member credit bureaus. The ACB system has been installed in Dallas and Houston, and another operation exists in Chicago. Currently there are more than 2,000 credit bureaus in this association, serving 365,000 credit grantors and maintaining files on approximately 100,000,000 Americans.[213]

In September 1968 ACB announced that it had signed an agreement with International Telephone and Telegraph Corporation to provide ACB members with computerized credit-reporting services. The new ACB-IT&T system will offer local credit bureaus the option of computerizing their own operations without bearing the heavy financial burden of buying or leasing computer equipment and developing their own data-processing systems and programs.[214] At the

209. *Id.* at 74; *cf. id.* at 111.

210. *Id.* at 87.

211. *Id.* at 83-84.

212. *See* UNIVAC Brief at A-9: "A real-time system is one which provides the ability to obtain information in time to affect events as they occur."

213. *House Hearings on Commercial Credit Bureaus* 109.

214. According to Harold S. Geneen, president of IT&T: "[IT&T] is currently accelerating its programs for the establishment of an international system of data processing service centers, supplementing existing operations in England, Sweden, Germany, and France." John L. Spafford, Executive Vice-President of ACB added: "This system will combine the most advanced communications and computer tech-

moment, computerization by individual bureaus within the association is not contemplated. However, given the resources of a company such as IT&T, the raw data available in the files of the more than 2,000 members of ACB, and the seemingly inexorable march of computer technology in terms of increased speed and storage capacity, the consequences of the ACB-IT&T operation seem obvious.[215]

Computerization of credit bureau files and the creation of national networks connecting numerous data bases whose contents will be available on a remote-access basis require concerted activity on the part of four previously independent industries: the computer manufacturers, the credit bureaus, the communications carriers, and the credit grantors. Probably only a few large credit information companies command the necessary financial resources, data bases, and technical expertise to survive in this sophisticated national market. For example, it took the ACB nearly four years to develop a standardized language of credit-reporting that would eliminate some of the softness in credit data and make machine processing easier.[216] In addition, recent hearings before the Senate Subcommittee on Monopoly and Antitrust revealed that firms in the other three industries may extend their operations into the credit information market,[217] and this may make it difficult for new firms to enter the field and may result in a potentially unhealthy level of business concentration.[218]

If in fact only a small number of companies or networks survive as suppliers of credit information, vast stores of financial and personal data will be centralized in the hands of relatively few people. This necessarily will result in the network managers having a considerable amount of economic power. In addition, a person's status in the community may be at the mercy of those who purport to have his financial history in their data bank.[219] Another concern about

---

nologies through the use of 'third-generation' computers, standard communications lines, and a variety of typewriter-like or visual display terminals." Credit News Bureau press release, Sept. 20, 1968.

215. *See Senate Hearings on Credit Bureaus* (statement of the author).

216. *House Hearings on Commercial Credit Bureaus* 105.

217. Western Union, for example, has acquired an interest in a firm which proposes to transmit credit information by common carrier, while International Telephone and Telegraph Company has designed a computer system for the ACB. *House Hearings on Commercial Credit Bureaus* 149; Credit News Bureau press release, Sept. 20, 1968. *See also* Irwin, *The Computer Utility: Competition or Regulation?*, 76 YALE L.J. 1299, 1302.

218. *See Senate Hearings on Credit Bureaus* (statement of the author).

219. *Senate Hearings on Credit Bureaus* (statement of the author); *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 236 (1968) (remarks of John de J. Pemberton, Jr.).

the trend toward computerization and concentration of credit data is that the capabilities of the new technology will encourage credit bureaus to acquire more information about individual and institutional borrowers than they have in the past. This "improvement" in the data means that the bureaus will inevitably gather soft and sensitive information.[220] In addition, given the massive investment required to computerize a large credit data base and the technology's ability to manipulate bits of information in unique ways, the temptation to use the data for non-credit-granting purposes will not be easy to resist. This is especially likely if the data base has been augmented by other information. A detailed account of a person's financial transactions, especially when accompanied by the type of investigative information collected by some of the credit bureaus, makes it easy to reconstruct his habits, associations, travel, and life style.[221] If data of this type is compiled on a large group, it can be used for a number of noncredit commercial purposes, such as generating a special mailing list containing the names of consumers with certain characteristics who might be interested in a particular product,[222] or rating the creditworthiness of a list of people who are likely prospects for a promotion campaign centered around the distribution of unsolicited credit cards.[223]

---

220. *See* pt. II.C. *supra.*

221. *See, e.g.*, A. WESTIN, PRIVACY AND FREEDOM 165 (1967); Westin, *The Snooping Machine*, PLAYBOY, May 1968, at 130.

222. Professor Westin has related that the editors of *Reader's Digest* used computer technology to generate a mailing list consisting of the neighbors of subscribers, which proved surprisingly effective:

> The approach had a kind of "All the neighbors are doing it" quality, but more significantly, the individual was pleased that the Reader's Digest knew him as an individual and could relate him to two others on his block. . . .
>
> Millions of people subscribe to the Reader's Digest. The Reader's Digest editors were struck by this because they said they didn't want so much power. They were appalled that they were able to affect so many people through such a simple technique.

House Hearings on Commercial Credit Bureaus 50. *See also* Trillin, *Onward and Upward with the Arts: You Can't Wear Out a List*, THE NEW YORKER, Sept. 24, 1966, at 126. A recent case in which several New York City bookstores were accused of selling lists of the names and addresses of women who had subscribed to computerized dating services is a rather extreme example of the abuse of the new technology. N.Y. Times, July 30, 1968, at 41, col. 1; *cf.* Lamont v. Commissioner of Motor Vehicles, 269 F.Supp. 880 (S.D.N.Y.), *aff'd per curiam*, 386 F.2d 449 (2d Cir. 1967); 39 U.S.C. § 4009 (Supp. III, 1965-1967) ("Prohibition of pandering advertisements in the mail").

223. *See, e.g.*, Credit News Bureau press release, November 20, 1967:

> [Cyril Jedlicka, banking counsel of the ACB] cited Western Auto in Kansas City as a profitable example of prechecking consumer credit before mailing unsolicited credit cards.
>
> "When Western Auto made the decision to go into the credit card business, they gave a list of a substantial number of names to the Credit Bureau of Greater Kansas City," Jedlicka said. "These names were checked by the credit bureau and rated A, B and C."
>
> "The A's, quite obviously, were the best credit risks; B's were in between; and C's were undesirable," Jedlicka said, "Western Auto mailed credit cards to everyone with an A rating."

Furthermore, employers,[224] insurance companies,[225] and government investigators[226] all have occasion to make extensive inquiries concerning certain individuals, and this task can be expedited measurably if the examination can start with an inexpensive and comprehensive credit bureau report, especially if the credit bureau itself supplies the requesting party with nonfinancial data.[227] Some credit bureaus open their files to government investigators without charge or protest,[228] possibly in the hope of currying official favor.[229] Even

224. E. LONG, THE INTRUDERS 50-51 (1967):

> The dossier-minded employer can be found in every line of business. . . . Often a private detective agency is employed to do the job. Its investigators check candidates thoroughly; their routine reports include examinations of academic records, court records, personal credit and litigation, marital status, police records, political affiliation, neighborhood background, newspaper files, past earning capacity and past employment records, personal (drinking and even sexual) habits and conduct, and moral character.
>
> The concern of the employer may extend to the prospective employee's wife and family. . . . There will be a full report on [the wife's] character and a compilation of her controversial characteristics, including her social mannerisms and drinking habits; reference will be made to her education and to her ability to adjust to her home and neighborhood; a list of her club and religious affiliations will be included.

225. *See generally* M. BRENTON, THE PRIVACY INVADERS 45 (1964).

226. M. BRENTON, *supra* note 225 at 30, makes the wry observation that "it must be assumed the nation's credit bureaus are ethical and doing a good job. Otherwise government investigators and local police departments would not be using the bureaus' files as much as they do." *See also* A. WESTIN, PRIVACY AND FREEDOM 160 (1967); Star, *The Computer Data Bank: Will It Kill Your Freedom?*, LOOK, June 25, 1968, at 27.

227. Retail Credit Company, with files on 45,000,000 individuals, performs insurance and employment reporting as well as providing credit information. *House Hearings on Commercial Credit Bureaus* 13. The firm has a staff of approximately 7,000 investigators. A. WESTIN, *supra* note 226, at 159; *cf.* M. BRENTON, *supra* note 225, at 29. It is estimated that the company controls sixty per cent of the credit reporting field. *Hearings on Retail Credit Company* 3.

228. *See, e.g., House Hearings on Commercial Credit Bureaus* 7-10, 121-24. *See also Hearings on Retail Credit Company* 90-91 (testimony of W. Lee Burge, President of Retail Credit Company):

> Let me illustrate what I mean by a favor report. Someone who is a regular contact of ours, an executive of a large business might be about to employ a new minister at his church. If there is some reason for us to make the investigation because of the reputability of the individual involved, and our business relationship with him, we might have the report made, and then we might look it over before it ever goes to him, and then, depending on the circumstances, we might say that we have investigated your prospective minister and he has a good reputation . . . .
>
> . . . .
>
> If we had some other things to say, we would handle it somewhat this way. We would say based on our investigation . . . we don't believe this man is the minister you want for your Church.

But cf. id. at 93.

229. *But cf.* the explanation offered by an ACB official in *House Hearings on Commercial Credit Bureaus* 133:

> Credit bureaus consider it a responsibility in the interest of good government to assist government investigations with information that may be helpful. Some of these agencies are interested in identifying information rather than credit information. If the bureau file shows a former address, a former employer, or other clue to pertinent history, the agency investigator uses the lead to continue his investigation. We believe that this substantially reduces the expenditure of time and money by the various agencies.

Both Retail Credit Company and Hooper-Holmes Bureau cooperate with government investigatory efforts. *Hearings on Retail Credit Company* 57; Sesser, *Big Brother Keeps*

if the credit bureau refuses, the file still may be vulnerable since the Government can resort to its subpoena power.[230] However, the legal obligations of a credit bureau to grant the Government access to its files have not been fully defined.

The possible abuses of a computerized credit information network are not the only aspects of the credit bureau of the future that deserve attention. The "watch service" offered by ACB members, for example, actually constitutes an unsophisticated form of surveillance. It involves monitoring the public records and an individual's transactions after he has made a credit purchase, in order to inform the lender promptly if there is any indication that the customer will not be able to meet his obligation.[231] Control over an individual's credit history also provides considerable leverage for collecting debts that otherwise might be written off by the credit grantor. ACB supplies economic data to collection agencies as well as to credit grantors,[232] and, in the course of "counselling" the consumer on his credit problems, bureaus and agencies that are members of ACB often are able to "convince" individuals to "rehabilitate their credit by paying off delinquent accounts over ten years old."[233] This practice reflects the enormous *in terrorem* effect of a permanent credit bureau file and graphically demonstrates its ability to outlive the applicable statute of limitations. Finally, it has been suggested that the ownership of Welcome Newcomer by ACB has potentially sinister implications for individual privacy.[234] If the welcoming committee sponsored by the local merchants is really a cloak-and-dagger group designed to report on the characteristics and status of new members of the community, would paranoia be unjustified?

Another trend that will have considerable long-range impact on credit bureaus is the increasing involvement of the banking industry in a variety of commercial fields that depend on computer technology and individualized information. Banks were among the first institutions to computerize financial information as a means of

---

Tabs on Insurance Buyers, THE NEW REPUBLIC, April 27, 1968, at 11. Credit Data Corporation seems to be the only national credit information company which has resisted the Government's attempts to use its files for fishing expeditions. *See House Hearings on Commercial Credit Bureaus* 90-93.

230. *See, e.g., House Hearings on Commercial Credit Bureaus* 91.

231. Credit News Bureau press release, Nov. 30, 1967.

232. *See* note 195 *supra*.

233. Credit News Bureau press release, Nov. 30, 1967.

234. News Release from Representative Cornelius E. Gallagher, March 20, 1969: "'I am particularly distressed to learn that the Associated Credit Bureaus, Inc. owns Welcome Newcomer,' Congressman Gallagher continued. . . . 'In spite of their flowered hats and sweet smiles, these hostesses are, in effect, private investigators [for the ACB].'"

expediting paperwork, and the string of machine-readable numbers at the bottom of checks now is universally familiar. Computers also have enabled the banks to provide a wider variety of customer services—payroll computations, accounting, mortgage servicing, and miscellaneous data-processing.[235] One endeavor that major banking institutions recently have embarked upon is the bank or universal credit card. Universal card systems often require individual card transactions to be processed through an independent credit bureau.[236] In California, however, a group of banks participating in a charge card plan apparently has established its own clearinghouse for credit transactions.[237] The increasing acceptance of the universal credit card has enormous significance; it may herald the first stage of a checkless, cashless society in which all financial transactions are reflected as electronic debits and credits in the cardholder's computerized account that are shifted among sellers, and bank computers linked together by a nationwide network of communications lines.[238] Present-day bank credit-granting easily can be incorporated into this system.

In a checkless, cashless society, the credit-granting and credit-rating industries might cease to exist as separate entities.[239] The customer in each transaction would inform the bank computer of the terms and conditions on which he had agreed to make payment through a remote terminal located in the retail store. The decision to grant credit would be made by the computer, on line and in real time, on the basis of the current status of the customer's computerized account and his past credit performance. If the transaction is approved, the merchant would be relieved of the risks of collection. Over time, procedures of this type would result in a diminution of the need for independent credit information and credit bureaus would be under great pressure to combine with the bank credit card systems or to find other profitable uses for their dossiers. Judging from some of the practices described earlier in this section, the commercial outlets chosen almost certainly would result in a sacrifice of individual privacy.

235. *See Money Goes Electronic in the 1970's*, BUSINESS WEEK, Jan. 13, 1968, at 54, 74; 115 CONG. REC. E2613 (daily ed. April 2, 1968).

236. *See, e.g., House Hearings on Commercial Credit Bureaus* 149.

237. *Money Goes Electronic in the 1970's*, BUSINESS WEEK, Jan. 13, 1968, at 54, 64.

238. *See, e.g., Senate Hearings on Computer Privacy*, pt. 2, at 327-33 (statement of Paul Armer, Associate Head, Computer Sciences Department, the Rand Corporation); O'Brien, *The Bank of Tomorrow: Today*, COMPUTERS AND AUTOMATION, May 1968, at 26; *Electronic Money*, FORBES, April 1, 1967, at 42; Kramer & Livingston, *Cashing In on the Checkless Society*, 45 HARV. BUS. REV., Sept.-Oct. 1967, at 141; E. Weiss, The Marketing Implications of the Checkless Society (1968).

239. *See* Karst, *"The Files" Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342, 375 (1966).

The credit-reporting industry has been surprisingly free of regulation thus far, but there is growing awareness of the potential threat to privacy created by credit bureaus. Congressional hearings have been held in both the Senate and the House,[240] and Senator Proxmire has introduced a bill that would add a new title to the recently enacted Truth-in-Lending Act[241] to provide safeguards in the field of credit-reporting.[242] The purpose of the bill is "to protect consumers against arbitrary or erroneous credit ratings, and the unwarranted publication of credit information." It would require that: (1) credit bureaus employ effective procedures for guaranteeing the confidentiality of the information they collect; (2) credit information be withheld from noncreditors such as government investigatory agencies without the express consent of the person involved; (3) an individual be given an opportunity to correct inaccurate information in his credit file, and be notified when a derogatory public record item is entered in his credit record; (4) procedures be developed for discarding irrelevant and outdated information in an individual's credit file; and (5) users of credit reports notify an individual who has been adversely affected by a report and identify the bureau that issued it.[243] State legislatures also are beginning to scrutinize the credit industry.[244]

240. *See* note 190 *supra.*

241. Pub. L. No. 90-321 (May 29, 1968).

242. S. 823, 91st Cong., 1st Sess. (1969); *see* 115 CONG. REC. S1163-69 (daily ed., Jan. 31, 1969). *See also* 114 CONG. REC. S10,029 (daily ed. Aug. 2, 1968). Broad hearings on the bill were held on May 19-23, 1969.

243. The current draft of S. 823 is not without deficiencies, however. For example, a strict reading of the bill, especially the language in section 164(c), limits its prohibitions to financial data and would not prevent free collection and utilization of the more dangerous forms of personal information described in text accompanying notes 190-94, 220-30 *supra.* Along the same lines, the bill requires only that the data subject be notified by the bureau "whenever information which is a matter of public record is obtained . . . and which is, or is likely to be interpreted by the agency or its clients as, adverse to the credit rating of the individual . . . ." Why shouldn't the individual be notified of the receipt of *any* form of adverse data whether or not it is from a public record? And why are his rights limited to submitting "an explanatory statement with respect thereto"? Why shouldn't he be enabled to have the items expunged from the agency's file if he can demonstrate their inaccuracy or their lack of probity? Moreover, the bill does not expressly insure that the individual's "explanatory statement" accompany any report that is disseminated on the individual. Finally, in most cases damage suits under the bill will involve under $10,000, the basic jurisdictional amount required by 28 U.S.C. § 1331 (1964). Arguably, therefore, the proposed act should confer subject matter jurisdiction for disputes arising under it without regard to the amount in controversy. Section 166 of the bill, even section 166(b), which appears to be simply a limitations provision, is unclear on this point.

244. *Cf.* Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy,* 57 GEO. L.J. 509, 529 (1969): "An Oklahoma statute [OKLA. STAT. ANN. tit. 24, §§ 81-85 (1965)] is the only legislation, state or federal, which specifically deals with the credit bureau problem." Bills have been introduced in several states during the past year.

Perhaps the most salient feature of the Proxmire bill is its recognition that information handlers have been remiss in excluding the data subject from transactions involving information relating to him. By assuring the individual access to his credit file, the proposal enables people to have a modicum of control over the flow of information about them. It also represents an important step toward imposing obligations on the credit bureau industry that will help achieve some type of balance between the need for accurate financial data to maintain the flow of credit throughout the nation and the preservation of the right of individual privacy.

Obviously in the hope of avoiding the imposition of legislative restraints, ACB has developed a series of guidelines, mentioned earlier,[245] to protect consumer privacy. Although these guidelines contain some safeguards, they were composed by an industry group with minimal consumer representation, they are not binding upon anyone—particularly not upon the many bureaus unaffiliated with ACB—and they are bountifully endowed with loopholes. For example, the ACB guidelines authorize the bureaus to collect matters of public record—bankruptcies, lawsuits, arrests, indictment or conviction of crime—but they are obliged only to "make a *reasonable* effort to learn and report disposition" of each such item.[246] ACB seeks to absolve its members by putting the onus on the credit grantor to "inquire further as to the . . . disposition of any items of significance to his credit decision, or authorize the bureau to do so,"[247] and by requiring the complaining consumer to sign "a statement granting immunity from legal action both to the credit bureau and to its sources of information."[248] Perhaps ACB is to be congratulated for its effort; unfortunately, the CBS News experiment described earlier indicates that a number of bureaus

See, e.g., N.Y. Sen. Introductory No. 338, N.Y. Assembly Introductory No. 570 (1968); Des Moines Register, April 14, 1969, at 10, col. 1. At this writing, however, none of them appears to have been enacted.

Congressman Cornelius Gallagher commented on this situation in *House Hearings on Commercial Credit Bureaus* 115:

> In every State and every township in the country there are regulations concerning the transfer of ownership of dogs . . . yet there are really no regulations whatsoever pertaining to the transfer of this kind of information affecting a man's standing in the community, his dignity, his economic transactions, his private life, his very name itself . . . .
>
> An individual American certainly has far less [sic] rights under this system than a dog has.

245. *See* note 199 *supra*.

246. ACB, Inc., Credit Bureau Guidelines To Protect Consumer Privacy, § E(1)(b) (emphasis added).

247. *Id.* at § E(1)(c).

248. *Id.* at § A(2).

failed to implement the guidelines. But even rigorous application of these guidelines does not obviate the need for further regulation.

C. *Regulating the Flow of Information—The Need for a Broad Perspective*

The problem of safeguarding the individual's right to exercise some control over information relating to him must be approached with the realization that we are dealing with an entirely new medium of communications, one that is likely to restructure our society in much the same manner as did movable type or the Industrial Revolution.[249] As suggested above, it may not be sufficient simply to apply the existing legal structure to the new fact situations created by computer technology. Unfortunately, the law historically has been slow to accommodate existing doctrines to new technologies. The length of time it took the law of warranty and tort to adjust to the automobile and the years of confusion that transpired before radio, television, and the airplane came under effective regulation testify to the legal system's somewhat ponderous reaction to novel situations posed by technological advances. Thus, it would not be surprising if the existing patchwork of legal proscriptions governing the misuse of individualized information—although suggestive of meaningful restrictions on the increasing flow of highly personal data—proves to be unequal to the challenges posed by the computer revolution.

Before examining in detail the existing common-law doctrine and legislative pronouncements on the handling of personal information, an important reminder must be interjected. As the discussion of the proposed National Data Center and the credit bureau industry indicates, the patterns of growth and integration among computerized data-processing services are widespread, complex, and

249. *See* note 2 *supra*. *See also* E. MORISON, MEN, MACHINES, AND MODERN TIMES 78 (1966):

> [O]ur society [is] based upon the instrumentation of the industrial process. All our economic and social arrangements—how we feel about what we do, which is all that culture is—are founded upon the way our industrial energy is organized. How large a part and what kind of part do we want the computer, with its overriding skill in the rational analysis of the measurable data, to take in the decisions that determine the way this energy will be organized?

A rather pessimistic assessment of our long-range ability to control computer technology is given in Clarke, *The Mind of the Machine*, PLAYBOY, Dec. 1968, at 116, 118:

> [I]t should be realized that as soon as the borders of electronic intelligence are passed, there will be a kind of chain reaction, because the machines will rapidly improve themselves. In a very few generations—*computer* generations, which by this time may last only a few months—there will be a mental explosion; the merely intelligent machine will swiftly give way to the *ultra*-intelligent machine.

See also Clarke, *The Computer Takes Over*, The Chicago Daily News, July 13, 1968, Panorama Magazine, at 4.

often uncertain. It seems clear, therefore, that an attempt to achieve a workable balance between privacy and efficiency for any *particular* application of computer technology has little promise of success unless proper account is taken of the great variety of factors and relationships that tend to encourage computerization, system interconnection, and data-sharing. The National Data Center and credit bureaus merely provide two intrinsically interesting models for study—the parameters of the problem have a much wider scope. Increased abrasion between computers and individual privacy can be anticipated in many individual contexts. Businesses,[250] hospitals,[251] educational institutions,[252] and federal,[253] state,[254] and local[255] governments are quickening the pace of computerization and recognizing common interests in having data flow among them. But these new applications should not be examined one at a time. As suggested earlier, nothing short of a complete survey of the rami-

250. *See generally* Allen, *Time Sharing Takes Off*, HARV. BUS. REV., March-April 1968, at 128; Burck, *The Computer Industry's Great Expectations*, FORTUNE, Aug. 1968, at 92; Dearden, *Computers: No Impact on Divisional Control*, HARV. BUS. REV., Jan.-Feb. 1967, at 99; Brady, *Computers in Top-Level Decision Making*, HARV. BUS. REV., July-Aug. 1967, at 67.

251. *See, e.g.*, Freed, *A Legal Structure for a National Medical Data Center*, 49 B.U. L. REV. 79 (1969); Freed, *Legal Aspects of Computer Use in Medicine*, 32 LAW & CONTEMP. PROB. 674 (1967); Sarnoff, *No Life Untouched*, SAT. REV., July 23, 1966, at 21; Stevens, *Now—The Automated Physical Checkup*, READERS DIGEST, July 1966, at 95.

252. A number of colleges and universities are recognizing the advantages of maintaining joint computer facilities and sharing data bases. *See, e.g.*, the description of a nonprofit corporation formed by Harvard University and the Massachusetts Institute of Technology for the purpose of establishing a joint telecommunications system based on shared computer facilities in N.Y. Times, July 7, 1968, § 2, at 52, col. 4. The Interuniversity Communications Council (EDUCOM), another nonprofit corporation, also is designed to promote the application of the new communications technology to education. *See also* Miller, *Potentialities of a Multi-Media, Inter-University Educational Network*, in CIBA FOUNDATION SYMPOSIUM ON COMMUNICATION IN SCIENCE: DOCUMENTATION AND AUTOMATION 235-52 (1967).

253. *See* the description of the FBI's computerized National Crime Information center in notes 385-88 *infra* and accompanying text. This center is designed to facilitate the exchange of various kinds of dossiers among federal, state, and local law enforcement officers.

The Law Enforcement Assistance Administration of the Justice Department is considering a proposal to create a national computer system devoted to information on organized crime. The system would contain data supplied by police departments, information on real estate transactions from recorders' offices, and records of state and local tax and license fees. Chicago Daily News, April 19, 1969, at 1, col. 3 (state weekend ed.).

254. *See, e.g.*, the description of California's efforts to establish a statewide data-processing system in *Project—The Computerization of Government Files: What Impact on the Individual?*, 15 UCLA L. REV. 1371, 1401-10 (1968). *See also Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 234-35 (1968) (description of the New York State Identification and Intelligence System by Professor Richard Ruggles). Wall St. J., April 9, 1969, at 1, col. 6 (description of Maryland State Employment Service computerized "job bank").

255. *See, e.g., A City Where Computers Will Know About Everybody*, U.S. NEWS & WORLD REPORT, May 15, 1967, at 78.

fications of the new technologies will suffice if a reasonable accommodation is to be reached between individual privacy and the effective flow of information in society.

V. The Current Law of Privacy: The Common Law and the Constitution

The development of the law relating to personal privacy is a familiar tale. Indeed, the courts and commentators have had a strong interest in the subject during the past three quarters of a century, and the judicial and secondary literature is rich. No useful purpose would be served by tracing the path to the present state of the law once more. Rather, this section will simply try to indicate why the existing common-law doctrines are unable, especially in light of the implications of the first amendment, to provide a meaningful resolution of the computer-privacy issue.

A. *The Availability of Common-Law Protection*

The inadequacy of contemporary legal theories of privacy to deal with the realities of the computer age is clearest in the context of the common-law doctrines, which traditionally have used an intrusion upon the individual by one of the mass media as a model.[256]

256. The exception, according to Dean Prosser, is the relatively small class of cases described by the term "intrusion," which usually involves some form of wiretapping or eavesdropping. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 389-92 (1960). Privacy actions have been allowed even when the eavesdropper has not communicated the information to anyone else. *See, e.g.*, Fowler v. Southern Bell Tel. & Tel. Co., 343 F.2d 150 (5th Cir. 1965); McDaniel v. Atlanta Coca-Cola Bottling Co., 60 Ga. App. 92, 2 S.E.2d 810, 817 (1939) ("Publication or commercialization may aggravate, but the individual's right to privacy is invaded and violated nevertheless in the original act of intrusion."); LaCrone v. Ohio Bell Tel. Co., 182 N.E.2d 15 (Ohio Ct. App. 1961); Roach v. Harper, 105 S.E.2d 564 (Sup. Ct. App. W. Va. 1958). Similar cases are collected in Restatement (Second) Torts § 652B comment *b* (Tent. Draft No. 13, 1967). *See also* note 258 *infra*. In several cases that purport to be based on mass publication, the amount of publicity held sufficient to sustain the action has been rather small. *See, e.g.*, Brents v. Morgan, 221 Ky. 765, 299 S.W. 967, 55 A.L.R. 964 (1957) (posting notice of plaintiff's indebtedness in store window); Beiderman's of Springfield, Inc. v. Wright, 322 S.W.2d 892 (Mo. 1959) (plaintiff's indebtedness proclaimed orally in restaurant for three successive days). The minimum requirement seems to be that the information is made available to the general public, whether or not it actually reaches a large number of people. In Dean Bloustein's view, the mass publication requirement is based on the premise that "[u]nless there is a breach of a confidential relationship . . . the indignity and outrage involved in disclosure of details of a private life, only arise when there is a massive disclosure . . . ." In short, "[t]he damage is to an individual's self-respect in being made a public spectacle." Bloustein, *Privacy As an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 981 (1964).

In Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964), a case involving the bugging of a married couple's bedroom, there is language indicating that in some circumstances the plaintiff might not have to show that the defendant actually overheard personal information:

> If the peeping Tom, the big ear and the electronic eavesdropper . . . have a

Thus, before an injured party can recover for a public disclosure of private facts—the form of privacy invasion that seems to be most analogous to a misuse of computerized information[257]—he must show that the private information was given "publicity," or that it was communicated to the public at large.[258] 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.[259] 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."[260] These narrow exceptions have been relatively unimportant in the past, but they may prove crucial in constructing a workable common-law theory for remedying an improper dissemination of computerized information—the prototypical privacy case of the future.[261]

In terms of privacy in a computerized environment, the critical dissemination of information may well take place when one user of

---

place in the hierarchy of social values, it ought not to be at the expense of a married couple . . . who have never asked for or by their conduct deserved a *potential* projection of their private conversations and actions . . . . *Whether actual or potential* such "publicity with respect to private matters of purely personal concern is an injury to personality . . . ."

106 N.H. at 112, 206 A.2d at 242 (emphasis added).

257. RESTATEMENT (SECOND) TORTS § 652A (Tent. Draft No. 13, 1967):

The right of privacy is invaded when there is
(a) unreasonable intrusion upon the seclusion of another . . . or
(b) appropriation of the other's name or likeness . . . or
(c) unreasonable publicity given to the other's private life . . . or
(d) publicity which unreasonably places the other in a false light before the public . . . .

See also Prosser, *supra* note 256, at 392-98; W. PROSSER, TORTS § 112, at 833-44 (3d ed. 1964).

258. RESTATEMENT (SECOND) TORTS § 652D, comment *b* (Tent. Draft No. 13, 1967):

"Publicity" . . . differs from "publication," as that term is used . . . in connection with liability for defamation. "Publication," in that sense, is a word of art, which includes any communication by the defendant to a third person. "Publicity," on the other hand, means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.

259. *See* note 258 *supra*; W. PROSSER, TORTS § 109 (3d ed. 1964); Bloustein, *supra* note 256, at 979-80.

260. Bloustein, *supra* note 256, at 980. In this situation, the author concludes, the wrong "is not the disclosure itself, but rather the disclosure in violation of a relationship of confidence. Disclosure, whether to one person or many, is equally wrongful as a breach of the condition under which the information was initially disclosed." Prosser, *supra* note 256, at 393, is in substantial accord. *See* note 262 *infra*.

261. When the improper dissemination is a result of government action, the rights of the parties almost always will be determined by statute or regulation. *See* pt. VI *infra*.

a time-sharing system permits another user to have access to private files, or when the operators of two different systems agree to exchange tapes or interconnect their computers. Once an unauthorized user has gained access, he can interrogate an individual's computerized file at will or disseminate its contents still further, possibly causing damage that may never be traced to an abuse of the file. In many of these situations, it it doubtful that a traditionally required relationship of trust or confidence exists between the file subject—the potential plaintiff—and the authorized user—the potential defendant—so as to give rise to a right of compensation. Ideally, the mere fact that the authorized user is a custodian of sensitive personal information should establish a duty of confidentiality as a matter of law, but the willingness of the courts to imply such an obligation is quite conjectural at this time.[262]

Another inherent difficulty of a common-law action based on the public disclosure of private facts is the rule that the information disclosed must be accurate. If it is not, in theory the plaintiff is remitted to an action for defamation to remedy his injury. In recent years this distinction has not been strictly adhered to; some privacy actions, notably those involving unwanted publicity that puts the plaintiff in a "false light in the public eye,"[263] have been viewed as a form of defamation.[264] However, the Supreme Court appears to

262. Implying the duty would have the desirable effect of removing a latent anomaly in the confidential-relationship theory. The anomaly arises from the fact that the confidentiality of a relationship depends upon the reasonable expectations of the party asserting an invasion of privacy; thus, an organization that is powerful enough *vis-à-vis* the individual to coerce or entice information from him while giving him notice of the fact that it will not keep the information in confidence could drastically reduce the scope of personal privacy. Josephson, Book Review, 15 UCLA L. REV. 1586, 1597-99 (1968).

Apparently the English courts have been more alert than their American counterparts to the unique dangers of handling personal information, and more willing to imply a confidential relationship. *See, e.g.*, Jacob & Jacob, *Confidential Communications*, THE NEW L.J., Feb. 6, 1969, at 133:

> It seems clear that the courts have imported ideas from the law of trusts and bailment into the law of confidence, for they now treat the fact that information is handed over for a particular purpose as itself normally sufficient for an implied bond of confidence to arise; and the donee of the information is not entitled to use the information so given for any purpose other than that for which it is given.

263. *See* note 257 *supra*.

264. The fact that the two theories have overlapped significantly in practice is discussed in Wade, *Defamation and the Right of Privacy*, 15 VAND. L. REV. 1093 (1962). *See also* Hazlitt v. Fawcett Publications, Inc., 116 F. Supp. 538 (D. Conn. 1953); Spahn v. Julian Messner, Inc., 23 App. Div. 2d 216, 260 N.Y.S.2d 451 (1965), *vacated and remanded*, 387 U.S. 239, *aff'd*, 21 N.Y.2d 124, 233 N.E.2d 840, 286 N.Y.S.2d 832 (1967); Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROB. 326, 339-41 (1966); Prosser, *Privacy*, 48 CALIF. L. REV. 383, 398-401, 422-23 (1960). *But cf.* Nimmer, *The Right To Speak from Times to Time: First*

have given renewed vitality to the fact-fiction line of demarcation in *Time, Inc. v. Hill.*[265]

This dichotomy between fact and untruth seems to be increasingly unworkable. It is insensitive to the many subtle ways in which personal data may be distorted or misused in a society that puts a premium on collecting and transmitting large quantities of information about individuals and using it for many purposes. The biased "soft data" or evaluation, the derogatory entry that does not reveal subsequent ameliorating events, or the unexplicated bit of information that appears damaging when it is introduced in a context unrelated to the one in which it was collected, all may be "factual" in the strict sense of the word and yet not portray an individual or his activities and aptitudes accurately. Thus, although the existing legal framework provides a theory for rectifying an improperly disseminated truth as well as a theory for remedying an untruth, neither approach focuses sharply enough on the penumbral area or takes account of the realities of modern communications. As a result, an injured plaintiff is left subject to the risk of falling between the conceptual stools.

A good illustration of the problems confronting an individual who believes that he has been injured by dissemination of soft data is provided by *Ellsworth v. Martindale-Hubbell Law Directory, Inc.*[266] The plaintiff, an attorney, brought a defamation action claiming that his professional rating had been lowered for no apparent reason by a national directory. In affirming a directed verdict for the defendant, the Supreme Court of North Dakota indicated the high burden of proof that is likely to be imposed on a plaintiff when the damaging information is a subjective evaluation:

> [The plaintiff's] . . . witnesses do not all agree that his ability is "very high." . . . He complains that several lawyers in [his home town] were rated as "very high" when he was rated as only "high." There is no showing that these lawyers were not of exceptional ability. Clearly a defamation of A is not proved by showing that

---

Amendment Theory Applied to Libel and Misapplied to Privacy, 56 CALIF. L. REV. 935, 958 (1968):

> Defamation protects a man's interest in his reputation. Reputation is by definition a matter of public knowledge. . . . The right of privacy protects not reputation, but the interest in maintaining the privacy of certain facts. Public disclosure of such facts can create injury regardless of whether such disclosure affects the subject's reputation.

265. 385 U.S. 374 (1967). *See* text accompanying notes 280-87 *infra*.

266. 69 N.D. 610, 289 N.W. 101 (1939).

someone says B is a better lawyer than A, when the legal ability of B is not shown.[267]

These proof difficulties would be compounded if the plaintiff had been rated as a "fair" worker by an organization that considered this classification a mark of average ability, and this rating was later made available to another organization in which "fair" connoted unusually low performance.

The final problem in determining whether tort relief is available for an alleged invasion of privacy is, of course, the issue of whether the information in question can justifiably be categorized as "private." The difficulty of enunciating a manageable standard for determining what kinds of personal information should be protected from public disclosure was foreseen by Warren and Brandeis in their classic 1890 article advocating recognition of the right-of-privacy tort:

> Since . . . the propriety of publishing the very same facts may depend wholly upon the person concerning whom they are published, no fixed formula can be used to prohibit obnoxious publications. . . .
>
> In general . . . the matters of which the publication should be repressed may be described as those which concern the private life, habits, acts, and relations of an individual, and have no legitimate connection with his fitness for a public position which he seeks or for which he is suggested . . . and have no legitimate relation to or bearing upon any act done by him in a public or quasi public capacity.[268]

Some of the uncertainty inherent in the suggested balancing of public and private interests was alleviated by incorporating an extensive body of privilege into the nascent law of privacy. Indeed, Warren and Brandeis themselves stipulated that in addition to the mass media's freedom to publish "matters of public or general interest," the doctrine of privacy should be subject to the complex rules of privilege that had developed in the law of defamation as well as to the defense of consent.[269] In theory, at least, these defenses mark off an area in which the individual's interest in preventing

267. 69 N.D. at 622, 289 N.W. at 105.

268. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 215-16 (1890). Dean Prosser's approach to the problem of defining what is "private" also is rather nebulous. He suggests that "what emerges is something in the nature of a 'mores' test, by which there will be liability only for publicity given to those things which the customs and ordinary views of the community will not tolerate." Prosser, *supra* note 264, at 397; *cf.* Batt, *Law and the Bedroom*, SAT. REV., Aug. 3, 1968, at 45, in which it is suggested that the protectible "zones of privacy" should be categorized as the family, sexuality, the psyche or psychology of an individual, and sensual and emotional impression and expression. *See also* Rider, *Legal Protection of the Manifestations of Individual Personality—The Identity-Indicia*, 33 S. CAL. L. REV. 31 (1959).

269. Warren & Brandeis, *supra* note 268, at 214-19.

the spread of personal data is outweighed by society's need or right to have access to that data.

It seems doubtful, however, that balances struck at a time when the principal threat to a person's emotional tranquillity and privacy was the excesses of a newspaper gossip column[270] can be applied without substantial modification to the incursions on individual freedom that are likely to arise in an age of electronic data-processing and high-speed transfers of large quantities of digital information over vast distances. For example, one extensive and relatively vague class of defamation privileges applies when "the publisher and the recipient have a common interest, and the communication is of a kind reasonably calculated to protect or further it."[271] A familiar application of this qualified[272] privilege is the immunity of mutual credit organizations and credit-rating agencies in divulging financial data to those who have an "apparent, present interest in the report."[273] In the contemporary environment, one in which credit reports often are cavalierly given over the telephone by ministerial personnel, presumably any party that knows a credit grantor's identifying code number[274] and has access to a telephone can tap a reservoir of detailed financial information that currently is maintained on over 100,000,000 persons. Should the credit bureau be permitted to claim the privilege on the basis of the snooper's "apparent interest"? And what will be the law's reaction to computerized credit bureaus which will enable large institutional lenders to have direct access to bureau files from remote terminals located in

---

270. *See id.* at 196: "The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery."

271. W. PROSSER, TORTS § 110, at 809 (3d ed. 1964).

272. The privilege "is conditioned upon publication in a reasonable manner and for a proper purpose." *Id.* at 805. As applied to credit bureau operations, the privilege must be exercised "in good faith and not as a mere cloak for coercion of payment." *Id.* at 809-10.

273. *Id.* at 809. *See also* Note, *Credit Investigations and the Right to Privacy*, 57 GEO. L.J. 509, 513-19 (1969). In Watwood v. Stone's Mercantile Agency, Inc., 194 F.2d 160, 161 (D.C. Cir.), *cert. denied*, 344 U.S. 821 (1952), the court stated:

> The harm that such statements occasionally do to applicants for credit is believed to be small in relation to the benefits that subscribers derive from frank reports. Since marital status and number of dependents bear on credit, the qualified privilege is broad enough to cover the statements [implying that the plaintiff had given birth to an illegitimate child].
>
> The agency need not show that the subscriber was actually interested in the plaintiff's credit.

274. *House Hearings on Commercial Credit Bureaus* 147; William J. Mangan, General Manager of Credit Bureau of Greater Boston, Inc., Statement Before a Public Study Session on the Procedures and Practices of Credit Bureaus, Consumers' Council, Boston, Mass., Oct. 15, 1968, at 5 (unpublished mimeo).

their offices;[275] will the bureaus be protected by the privilege on the ground that anyone who gains access to a client's terminal apparently is an authorized user?

The common-law limitations on the availability of the privacy tort are not the only constraints on securing protection for individuals. Ironically, in the context of the credit bureau industry, federal statutory law may contribute to the defeat of individual privacy in a way that is tangentially related to privileges. When the credit bureaus organize a trade association, as, for example, ACB, the association's ability to regulate its members' dissemination of credit information is circumscribed by the antitrust law. If the network suspects that a particular member or a credit granter is misusing credit information or supplying the bureau with incorrect data, the most effective method of maintaining file integrity is to deny the offending bureau access to the association's facilities or to terminate service to the offending subscriber. But the ACB is subject to an antitrust consent decree that justifiably makes it wary of refusing to deal with any party requesting service.[276] This unhappy squeeze between contributing to the invasion of privacy and violating the antitrust laws was appropriately described by an ACB official as being caught "between Scylla and Charybdis."[277] Along analogous lines, when a credit bureau opens its files to a government investigator, it could seek to avoid liability by claiming, in the nature of a privilege, that it is obliged "to give information to proper authorities for the prevention or detection of crime."[278] In view of these impediments to the vindication of individual privacy through the law of torts, it is small wonder that credit reports regularly are purchased and circulated by those who have no legitimate credit-granting purpose.[279]

B. *The Effect of the First Amendment*

The body of privilege surrounding the first amendment freedom of the press to comment on newsworthy events also serves to restrict the availability of common-law relief for an invasion of informa-

275. These remote terminals are now being installed. *See, e.g., House Hearings on Commercial Credit Bureaus* 93 (statement of H. C. Jordan, President of Credit Data Corporation).

276. *House Hearings on Commercial Credit Bureaus* 128-29. *See also Senate Hearings on Credit Bureaus* (statement of the author).

277. *House Hearings on Commercial Credit Bureaus* 129 (testimony of John Lashly, ACB lawyer).

278. W. PROSSER, TORTS § 110, at 811 (3d ed. 1964).

279. The ease of obtaining supposedly confidential credit reports is discussed in M. BRENTON, THE PRIVACY INVADERS 36-38 (1964). *See also House Hearings on Commercial Credit Bureaus* 3-10, 121-24; text accompanying notes 197-201 *supra*.

tional privacy. The plaintiff's ability to avoid this bar has been substantially limited by the Supreme Court's decision in *Time, Inc. v. Hill.*[280] In *Hill,* the plaintiff's suit for invasion of privacy arose out of a "fictionalized" magazine article describing an unpleasant, but newsworthy, event that had involved him and his family several years earlier.[281] Although he was successful at trial, the Supreme Court ultimately held that the first amendment required the plaintiff to meet the same burden of proof as in an action for defamation —Hill had to show that the defendant was guilty of knowing or reckless falsehood. This standard—formulated in *New York Times Co. v. Sullivan*[282]—has been quite difficult to satisfy in practice.[283]

Hill may well have aborted much of the doctrinal growth capacity of the law of privacy. At this writing, however, the precise implications of the decision must be considered unclear, especially since the case was founded on (and much of the opinion is devoted to) New York's somewhat peculiar privacy statute.[284] If the Court's opinion is read narrowly, its effect may be limited to the "false light" line of privacy cases, which are viewed by some as similar to traditional defamation actions.[285] Support for this view is found in the majority opinion's explicit reservation of the question whether the constitutional standards employed in defamation cases apply to the publication of truthful matters.[286] On the other hand, the burden-of-proof standard used in *Hill* easily could be extended to

---

280. 385 U.S. 374 (1967).

281. The Hill family had been held captive by escaped convicts in a much-publicized incident, and the event later became the topic of a popular play. *Life* magazine published an article describing the play and distorting what actually had happened to the Hill family during their imprisonment.

282. 326 U.S. 254 (1964).

283. *See, e.g.,* Nimmer, *supra* note 264, at 952:

> [Under the *New York Times* standard] the issue before the jury will not be the truth or falsity of the defamatory statement, but rather the narrow question of the speaker's good faith. A jury will probably not go wrong on this narrow question of fact in view of the Court's statement in *Times* that the Constitution demands a standard of "convincing clarity." Moreover, the burden of proof on this narrow issue makes it increasingly likely that an appellate court will reverse jury determinations against the speaker when the standard of convincing clarity has not been met.

See also Time, Inc. v. Hill, 385 U.S. 374, 411 (1967) (Justice Fortas, dissenting); Kalven, *The Reasonable Man and the First Amendment: Hill, Butts, and Walker,* 1967 SUP. CT. REV. 267, 284: "The logic of *New York Times* and *Hill* taken together grants the press some measure of constitutional protection for anything the press thinks is a matter of public interest."

284. N.Y. CIV. RIGHTS LAW §§ 50-51.

285. *See* notes 263-64, *supra* and accompanying text.

286. 385 U.S. at 383 n.7:

> This limitation to newsworthy persons and events does not of course foreclose an interpretation of the statute to allow damages where "Revelations may be so intimate and so unwarranted in view of the victim's position as to outrage the community's notions of decency." . . . This case presents no question whether truthful publication of such matter could be constitutionally proscribed.

all of the mass publication forms of the privacy tort, at least when there is no independent ground for state regulation, as might be true in cases involving intrusive behavior by the defendant.[287] The latter approach is consistent with the Warren and Brandeis article, which advocated the application of all defamation privileges to privacy actions,[288] apparently on the theory that truth is entitled to at least as much protection as falsehood. Only a few years have passed since Dean Prosser found that "there is still no reason to doubt this conclusion."[289]

In considering *Hill* in the context of the computer age, two rather basic questions spring to mind: (1) Should the decision be applied to the intrasystem dissemination of data maintained in computer networks, as well as to dissemination by the conventional media? (2) How does the decision affect transfers of information from computer systems to the news media? The answer to the first question is not as simple as might appear. If, as many commentators assert and as several passages in the *Hill* opinion indicate,[290] the protection bestowed on the press by the Constitution is premised on the concept that the people must receive an unrestricted flow of information in order to govern themselves intelligently—the "Meikeljohn interpretation" of the first amendment[291]—then the role of the new information transfer technology must be evaluated in terms of this objective to determine how it should be characterized. It certainly is true that computerized data-processing and information transfer capabilities already are important to the effective

287. *See* notes 303, 306 *infra* and accompanying text.

288. *See* note 269 *supra* and accompanying text.

289. W. PROSSER, TORTS § 112, at 851 (3d ed. 1964). *But cf.* Nimmer, *supra* note 264, at 962-63:

> The Court fell into error by reason of its failure to pierce the superficial similarity between false light invasion of privacy and defamation, and by its failure to formulate a doctrine which rationally relates the false light cases to the underlying interest in privacy. The heart of the problem of finding a conceptual base for the false light privacy cases lies in the erroneous assumption that the untrue representations in a false light case are necessarily defamatory (or reputation-injuring) in nature.
>
> . . . .
>
> . . . [T]he injury to the plaintiff's peace of mind which results from the public disclosure of private facts may be just as real where that which is disclosed is not true. . . . The sensibilities of the young lady whose nude photo is published would be no less offended if it turned out that her face were superimposed upon someone else's nude body. The resulting humiliation would have nothing to do with truth or falsity. The unwarranted disclosure of intimate "facts" is no less offensive and hence no less deserving of protection merely because such "facts" are not true.

290. 385 U.S. at 387-91.

291. *See, e.g.*, Bloustein, *supra* note 256; Brennan, *The Supreme Court and the Meikeljohn Interpretation of the First Amendment*, 79 HARV. L. REV. 1 (1965); Comment, *Privacy, Defamation, and the First Amendment: The Implications of Time, Inc. v. Hill*, 67 COLUM. L. REV. 926 (1967).

functioning of government, industry, and academe, and they are likely to become even more significant in the future.[292] Nonetheless, it also seems clear that computer systems, with their immense capacity for building individual dossiers, predicting human and organizational behavior, and aiding in decision-making, may well be more suited to institutional control of the people than vice versa. Moreover, the existing entities typically are closed and not accessible, in any practical sense, to the vast bulk of the population. These systems are not designed to perform any mass media functions *vis-à-vis* the citizenry. From this perspective, the data centers and networks of today and the immediate future do not seem to fit the traditional first amendment mold.

Of course, the current state of affairs is not immutable. Some observers predict that the computer terminal eventually will be as common as television and radio receivers,[293] that they will be multimedia in character, and that they will perform a wide variety of information functions—including those discharged by today's daily newspapers and newscasts.[294] Should this come to pass, computer networks will be as much a part of the "marketplace of ideas"[295] as are other media, and therefore equally entitled to first amendment protection for all applications which do not constitute purely "com-

292. *See* pt. II.C. *supra.*

293. *See, e.g.*, Sarnoff, *No Life Untouched*, SAT. REV., July 23, 1966, at 21:

> By the end of the century, for the equivalent of a few dollars a month, the individual will have a vast complex of computer services at his command. . . . The computer in the home will be joined to a national and global computer system that provides services ranging from banking and travel facilities to library research and medical care. High-speed communications devices, linked to satellites in space, will transmit data to and from virtually any point on earth with the ease of a dial system.

See also The National Observer, Oct. 17, 1966, at 1.

294. *See* Brown, *Tomorrow's Many-Splendored Tune-In*, SAT. EVENING POST, Nov. 30, 1968, at 38, 78; Russel, *Playing for Fun*, PLAYBOY, April 1969, at 110, 174:

> In the next medium, the medium after television, you have a terminal at home, with a screen—probably with higher definition than today's television . . . . There's a keyboard or a dial for making your wishes and feelings known, plus some kind of print-out device for hard copy—text and illustrations. This home communicator is connected by a simple cable through a buffer and switcher to the vast computer network and its omnibus memory. . . . News is added to the bank as fast as it is digested; and if you want to know more about something, you merely ask.

295. In *Time, Inc. v. Hill*, Justice Harlan advocated using the concept of a "marketplace of ideas" or "independent [public] interest" in the subject of the publication as a test for the operation of first amendment privileges. 385 U.S. at 407-08. *But cf.* Kalven, *The Reasonable Man and the First Amendment: Hill, Butts, and Walker*, 1967 SUP. CT. REV. 267, 300:

> For centuries it has been the experience of Anglo-American law that the truth never catches up with the lie, and it is because it does not that there has been a law of defamation. I simply do not see how the constitutional protection in this area can be rested on the assurance that counterargument will take the sting out of the falsehoods that the law is thereby permitting. And if this premise is not persuasive, the whole Harlan edifice trembles.

mercial speech."[296] However, as long as computer technology remains a relatively esoteric art, understood by and available to only a few, and applied primarily for record-keeping rather than dissemination, full-scale protection under the first amendment for intrasystem transfers seem inappropriate. A premature application of the first amendment could subvert the very values that the constitutional guaranty is designed to protect.

The ramifications of transplanting privileges developed in the context of more traditional media to the information distribution aspects of computer technology is indicated by the broad scope of the immunity from defamation and privacy actions that has been achieved by the press in recent years. As Professor Kalven has observed, the *Hill* decision points toward a time when anything that the press decides to print will be held newsworthy and therefore within the first amendment's protection and beyond the law of privacy.[297] This is consistent with trends in the closely related area of defamation.[298] Since *New York Times Co. v. Sullivan* was decided, the class of "public officials" who must prove knowing or reckless disregard for the truth as a prerequisite to recovery[299] has expanded to such an extent that it now appears that the term may encompass categories of individuals who are not even on the public payroll.[300]

---

296. The distinction between ideas and information, which are protected by the first amendment, and "purely commercial" advertising, which is subject to regulation, was established in Valentine v. Chrestensen, 316 U.S. 52 (1942). The continuing validity of this distinction is indicated by the citation of *Valentine* in the *Hill* decision, both by Justice Brennan for the majority and by Justice Harlan in dissent. 385 U.S. at 381, 405. Clearly, some types of computer use, such as the sale of computerized mailing lists, could be prohibited under this rationale. It also is at least arguable that the vast majority of computer operations in the private sector that generate information about specific individuals have such a limited relationship to the need for public information that their work product could be regarded as "commercial speech." *Cf.* Note, *Freedom of Expression in a Commercial Context*, 78 HARV. L. REV. 1191, 1194-203 (1965).

297. Kalven, *supra* note 295, at 283-84:

> Although it was not necessary in *Hill* to delineate the outer boundaries of the newsworthy, the Court may be surprised by the extent of its commitment. The tort law of privacy has wrestled with the matter for some years now; and it is a rough generalization that the courts will not, and indeed cannot, be arbiters of what is newsworthy. Newsworthiness will almost certainly become a descriptive and not a normative term.

But cf. Bloustein, *Privacy, Tort Law, and the Constitution: Is Warren and Brandeis' Tort Petty and Unconstitutional As Well?*, 46 TEXAS L. REV. 611, 625-26 (1968).

298. *See* Pearson v. Dodd, No. 21,910 (D.C. Cir. Feb. 24, 1969).

299. New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

300. In Rosenblatt v. Baer, 383 U.S. 75, 85 (1966), the Supreme Court held that "the 'public official' designation applies at the very least to those among the hierarchy of government employees who have, or appear to the public to have, substantial responsibility for or control over the conduct of governmental affairs." The Court then added, however, that "[t]he employee's position must be one which would invite public scrutiny and discussion of the person holding it, entirely apart from the scrutiny and

In the same vein, the class of "public officials" who can defame individuals with corresponding impunity is potentially as large.[301]

Obviously, there is a certain element of bootstrapping in the notion that the first amendment protects the publication of that which is newsworthy and it is the press that decides what is newsworthy. Perhaps in the context of a traditional invasion of privacy, which is well represented by the *Hill* case, there is usually some semblance of an objective standard—an event or occurrence with some independent contemporary significance. But this may not always be true when the invasion of privacy takes the form of someone rummaging through the entrails of the computer dossier maintained on one of his fellow men. In this context there is no newsworthy event other than the disclosure of the file's content. Although the Supreme Court's desire to preserve the policies favoring free dissemination of information that underlie the first amendment cannot be faulted in terms of a motivating theory, it is problematical whether these policies always require vindication at the expense of individual privacy. In light of the broad implications of the new technology, it seems desirable to reflect carefully before extending the *Hill* privilege to the emerging information exchange formats.

---

discussion occasioned by the particular charges in controversy." 383 U.S. at 87 n.13. In a concurring opinion, Justice Douglas observed:

> [I]f free discussion of public issues is the guide, I see no way to draw lines that exclude the night watchman, the file clerk, the typist, or for that matter, anyone on the public payroll. And how about those who contract to carry out governmental missions? Some of them are as much in the public domain as any so-called officeholder. . . . And the industrialists who raise the price of a basic commodity? . . . And the labor leader who combines trade unionism with bribery and racketeering?

383 U.S. at 89. *But cf.* Curtis Publishing Co. v. Butts, 388 U.S. 130, 155 (1967): "We consider and would hold that a 'public figure' who is not a public official may also recover damages for a defamatory falsehood whose substance makes substantial danger to reputation apparent, on a showing of highly unreasonable conduct . . . ." Chief Justice Warren, concurring in the *Butts* case, stated that "differentiation between 'public figures' and 'public officials' and adoption of separate standards of proof for each have no basis in law, logic, or First Amendment policy." 388 U.S. at 163. *Cf.* Kalven, *supra* note 295, at 307: "When . . . we remember that the appearance of victory for Harlan in *Butts* is a fluke, occasioned by Warren's vote to save the verdict for the plaintiff, it is apparent that the Court stands 5 to 4 in favor of the Brennan-Warren standard and hence in favor of an across-the-board application of *New York Times*."

301. In Barr v. Matteo, 360 U.S. 564 (1959), the Supreme Court held that falsehoods published by a government official acting within the scope of his discretionary authority are absolutely privileged. In dissent, Justice Brennan strongly criticized the scope of this privilege:

> I see no warrant for extending [the absolute privilege] to the extent done—apparently to include every official having some color of discretion to utter communications to Congress or the public . . . . [The majority's] approach seems to clothe with immunity the most obscure subforeman on an arsenal production line who has been delegated authority to hire and fire and who maliciously defames one he discharges.

360 U.S. at 587.

One other facet of the problem deserves brief mention. In the information field, as elsewhere, the distinction between government and the private sector has become increasingly tenuous and the movement toward concentration is now quite pronounced. As Chief Justice Warren has observed:

> Since . . . World War II, there has been a rapid fusion of economic and political power, a merging of science, industry and government, and a high degree of interaction between the intellectual, governmental, and business worlds. . . . [N]ational and international problems . . . demand national and international solution. While these trends and events have occasioned consolidation of governmental power, power has also become much more organized in what we have commonly considered to be the private sector. In many situations, policy determinations which traditionally were channelled through formal political institutions are now originated and implemented through a complex array of boards, committees, commissions, corporations, and associations, some only loosely connected with the government.[302]

In the context of computer technology this trend is exemplified by the concentration of power over information and the institutionalization of the flow of data among both public and private organizations. Considerations such as these, which have been but a peripheral concern in cases dealing with freedom of the press, will be at the heart of the question of the extent to which a data system and its managers should be immunized from liability for transferring damaging private information about an individual. The potential for centralization of power that inheres in the new information transfer technology, the lack of internal safeguards, and the frequently secretive nature of the dissemination counsel a skeptical attitude toward any assertion that notions of free communication developed to safeguard the press should be applied to a computer network, at least in the absence of a demonstration that the network is performing functions comparable to those discharged by traditional "news" media.

Assuming that there are no insuperable constitutional obstacles to imposing legal inhibitions on the flow of information within and among computer systems, the question remains as to what standards can and should be imposed on the movement of information from computer systems to today's mass media. As statements in the *Hill* opinion indicate, information that the press obtains by intrusive or trespassory behavior still can create liability.[303] This rule, although

302. Curtis Publishing Co. v. Butts, 388 U.S. 130, 163 (1967) (concurring opinion).

303. 385 U.S. at 385 n.9. *See also* the concurring and dissenting opinion of Justice Harlan at 404: "No claim is made that there was any intrusion upon the Hills' soli-

helpful when snooping or surveillance techniques are employed to extract data from a computer system, does not reach the situation that is more likely to prove troublesome in the electrically configured environment of the future—cooperation between the data gatherers within the computer medium and the data disseminators within the news media. This liaison is hardly unique to the computer age; the seductive minions of the press always have been able to cajole public and institutional officials into granting access to sensitive files by employing the blandishments of personal publicity or the threat of public criticism.[304]

The magnitude of the problem may be radically altered by the computer, however. If predictions made earlier in this Article concerning the increased computerization of personal information prove to be accurate,[305] there will be a change in the quantity, sensitivity, and variety of information that the mass media may be able to extract from a system once access to it has been secured. Moreover, when a reporter is able to procure dossiers from an investigatory agency, the printout is likely to consist of public-record data intermingled with subjective investigative reports, information given with the subject's actual or technical consent, and possibly informa-

---

tude or private affairs in order to obtain information for publication. The power of the State to control and remedy such intrusion for newsgathering purposes cannot be denied . . . ."

Private information that is obtained as a result of intrusive behavior should retain its nonprivileged character, even though the subject later becomes newsworthy. This rationale was adopted in Dietemann v. Time, Inc., 284 F. Supp. 925 (C.D. Calif. 1968), a case in which the plaintiff, apparently a quack doctor, had been surreptitiously photographed and tape-recorded in his home by *Life* magazine reporters posing as patients. The plaintiff was subsequently prosecuted for his illicit medical activities, and *Life* then published a story and some photographs obtained during the visit to his house. The court rejected a claim of privilege:

> Defendant [asserts] that because plaintiff was prosecuted all facts relating to his offenses became public information. If this be so, then the press may prepare a dossier on persons by illegal means, including trespass, pictures taken by hidden cameras in homes, offices, or other private places, conversations transmitted by radio transmitters, and even theft of material, then await a prosecution and publish everything which might in some degree relate to the offense charged, although such facts were not used as evidence or made a part of the public record. Such conduct cannot be justified under the right of freedom of the press.

284 F. Supp. at 931.

304. For example, consider the following description of conditions in the state of New York prior to the recent revision of police record-keeping systems:

> Violation of files was frequent. Police reporters looking for a good story were given free access to files on suspects, and as a result were able to publish in the newspaper some interesting but in many cases misleading, irrelevant, and damaging pieces of information. Those police chiefs who tried to protect the confidentiality of their files received poor press treatment, so that they would be encouraged to cooperate with the press more fully in the future.

Hearings on Government Statistical Programs 28 (statement of Professor Richard Ruggles).

305. *See* pt. II.C. *supra.*

tion transferred through interfaces with one or more other systems. A reporter unfamiliar with the structure of a computer network and the sources from which it draws its stored information is unlikely to be able to make intelligent judgments about the reliability or utility of various data items, as he might in the context of a manual filing system containing information from a circumscribed number of sources.

It is also unrealistic to assume that all managers or proprietors of computer systems will be concerned about how the data they release to the press is used or interpreted. A modicum of restraint would be provided if the immunity afforded by *Hill* is not extended to those who supply private data to the mass media.[306] In any event, the task of effectively protecting the individual from the risk of mass circulation of intimate and misleading information requires clear legal standards that impose a duty of care on the mass communications media in handling dossier information. In addition, legal standards also must be fabricated for the operation of computerized data systems delineating what categories of information are available: (1) for general release, (2) for circulation among specified other computer systems, or (3) for use only within the confines of a given system. Some suggestions along these and other lines will be offered at a later point in this Article.[307]

C. *The Consent Placebo*

The process of establishing effective controls over the flow of computerized information is complicated by another weakness in the existing common-law tort of privacy—the defense that the plain-

306. In Pearson v. Dodd, No. 21,910 (D.C. Cir. Feb. 24, 1969), it was held that newspaper reporters who had published information they knew had been obtained by an unauthorized intrusion into the plaintiff's files were not guilty of invasion of privacy. The court reasoned that the intrusion and the publication aspects of the tort "should be kept clearly separate." *Id.* at 6. Applying this analysis, the court concluded that the publication was within the ambit of the first amendment privilege and, since the reporters had not been parties to the intrusion, they were not held liable in tort:

> If we were to hold appellants liable for invasion of privacy on these facts, we would establish the proposition that one who receives information from an intruder, knowing it has been obtained by improper intrusion, is guilty of a tort. In an untried and developing area of tort law, we are not prepared to go so far.

Id. at 5-6. Since the plaintiff's employees who had originally intruded into his files were not parties to the action, the court did not reach the question of whether they would be able to assert the newspaper's first amendment privilege. Apparently the reporters did not advance this argument, but rather contended that the employees' disclosure was privileged by a public policy in favor of exposing wrongdoing. *Id.* at 5 n.19.

307. *See* pts. VII, VIII *infra*.

tiff consented to the dissemination of personal information,[308] or waived his right to protest by engaging in activity inconsistent with a desire to maintain his privacy. Unfortunately, the application of both of these concepts by the courts has been somewhat Draconian. "Waiver" often is employed to characterize the plaintiff's participation in some newsworthy event; however, the defense has been used under circumstances in which the notion of volitional acquiescence in the invasion is nothing short of unrealistic.[309] But even beyond that, the propriety of a defense to a privacy action should be assessed in terms of whether or not there is an overriding public interest in the free dissemination of information about the event, rather than on the basis of an assumption as to the plaintiff's intent.

Fortunately, there is a growing realization that the consent defense is insensitive to the psychological pressures and the need for the material realities of modern life that often force individuals to disclose personal data. When information is "voluntarily" given in the context of a police interrogation,[310] an application for welfare

---

308. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 218 (1890). *See also* Reitmeister v. Reitmeister, 162 F.2d 691 (2d Cir. 1947); Jenkins v. Dell Publishing Co., 143 F. Supp. 952 (W.D. Pa. 1956), *aff'd*, 251 F.2d 447 (3d Cir. 1958).

309. *See, e.g.*, Metter v. Los Angeles Examiner, 35 Cal. App. 2d 304, 95 P.2d 491 (1939) (woman "waived her right to privacy" by leaping from twelve-story building). Concern over chilling the dissemination of information by the press may extend to situations in which there is little apparent interest in communication of information. For example, in Gill v. Hearst Publishing Co., 40 Cal. 2d 224, 253 P.2d 441 (1953), a young couple who were photographed embracing in a public market place were held to have "waived" all right to object to publication of the photograph in a national magazine because, *inter alia*, the opposite result might have deterred the publication of all photographs of street scenes. The dissenting judge sharply criticized the artificiality of the waiver rationale:

> By plaintiffs doing what they did in view of a tiny fraction of the public, does not mean that they consented to observation by the millions of readers of the defendant's magazine. In effect, the majority holding means that anything anyone does outside of his own home is with consent to the publication thereof, because, under those circumstances he waives his right of privacy even though there is no news value in the event.

40 Cal. 2d at 232-33, 253 P.2d at 441. *cf.* Lopez v. United States, 373 U.S. 427, 452 (Justice Brennan, dissenting):

> [The suggestion that the right of privacy is lost by the auditor's consent to the electronic transcription of the speaker's words] invokes a fictive sense of waiver wholly incompatible with any meaningful concept of liberty of communication. If a person must always be on his guard against his auditor's having authorized a secret recording of their conversation, he will be no less reluctant to speak freely than if his risk is that a third party is doing the recording. . . . In a free society, people ought not to have to watch their every word so carefully.

See also Osborn v. United States, 385 U.S. 323, 347 (1966) (Justice Douglas, dissenting); Greenawalt, *The Consent Problem in Wiretapping and Eavesdropping*, 68 COLUM. L. REV. 189 (1968).

310. *See, e.g.*, Miranda v. Arizona, 384 U.S. 436, 468 n.37 (1966) [quoting P. DEVLIN, THE CRIMINAL PROSECUTION IN ENGLAND 32 (1958)]: "[T]here is still a general belief that you must answer all questions put to you by a policeman, or at least that it will be the worse for you if you do not."

payments,[311] an employment relationship,[312] or a psychological experiment,[313] a variety of complex factors may have combined to subvert the subject's freedom of choice. Even a questionnaire sent out under the imprimatur of a federal agency has an inhibiting effect on many individuals; it may even benefit from the respondent's natural, but erroneous, assumption that it is a "crime" not to answer every inquiry by the sovereign.[314] Although a great deal obviously depends on the circumstances surrounding the disclosure and the individual's personal characteristics, in many of these situations "consent" is simply a conclusory epithet that serves to place responsibility for invasions of privacy on the victim. Of course, it is the data gatherer who should be subject to a duty to refrain from employing coercion to obtain information.

A blatant example of an attempt to manipulate consent to provide a shield for possibly intrusive practices is provided by the action of a national credit bureau which became alarmed at the prospect of a congressional investigation. It drafted the following clause for inclusion in its credit applications:

---

311. *See generally* Handler & Rosenheim, *Privacy in Welfare: Public Assistance and Juvenile Justice*, 31 LAW & CONTEMP. PROB. 377 (1966). *See also* OFFICE OF SCIENCE AND TECHNOLOGY OF THE EXECUTIVE OFFICE OF THE PRESIDENT, PRIVACY AND BEHAVIORAL RESEARCH 18 (1967) [hereinafter PRIVACY AND BEHAVIORAL RESEARCH]:

> Free consent may be compromised by the subject's external circumstances. . . . The gravest invasions of privacy are likely to occur among the weakest and most helpless segments of the population—children, the very poor, the very sick, those who do not speak the language, and minority groups.

312. *See, e.g.*, S. REPT. No. 534 (to accompany S. 1035), 90th Cong., 1st Sess. 5 (1967):

> Each section of the bill [protecting the privacy of Federal employees] is based on evidence from many hundreds of cases and complaints showing that generally in the Federal service, as in any similar organizational situation, a request from a superior is equivalent to a command. This evidence refutes the argument that an employee's response to a superior's request for information or action is a voluntary response, and that an employee "consents" to an invasion of his privacy or the curtailment of his liberty. . . . For this reason, the bill makes it illegal for officials to "request" as well as to "require" an employee to submit to certain inquiries or practices or to take certain actions.

See also Creech, *The Privacy of Government Employees*, 31 LAW & CONTEMP. PROB. 413 (1966).

313. PRIVACY AND BEHAVIORAL RESEARCH 4, 18:

> Behavioral science seeks to assess and to measure many qualities of man's mind, feelings, and actions. In the absence of informed consent on the part of the subject, these measurements represent invasion of privacy. The scientist must therefore obtain the consent of his subject.
>
> To obtain truly informed consent is often difficult. In the first place, the nature of the inquiry cannot be explained adequately because it involves complex variables that the nonscientist does not understand. . . . Secondly, the validity of an experiment is sometimes destroyed if the subject knows all the details of its conduct. . . .
>
> . . . .
>
> In other situations the principle of free consent falls short for less obvious reasons. The subject may desire to please the experimenter, he may need to talk about very personal problems, or he may wish to place himself on exhibit. . . . Requiring consent can thus pose a problem for the investigator without providing the desired protection of subjects.

314. *See* note 174 *supra* and accompanying text.

> I hereby authorize the person to whom this application is made, or any credit bureau, or any other investigative agency employed by such person, to investigate the references herein listed, or statements, or other information, oral or written, obtained from me or any other person pertaining to my credit and financial responsibility . . . . I hereby release any claims, damages and suits whatsoever which may at any time be asserted by me by reason of such investigation.[315]

Clearly, personal privacy would become a chimera if adhesion provisions of this stripe were accepted by the courts.

In sum, assertions of "consent" and "waiver" must be regarded with skepticism. The defenses should not be widely available to permit data collectors to shift the risks of their activities. Instead, a fiduciary duty that is related to the degree of coercion or pressure under which an individual yields control of personal information should be imposed on the data extractor.[316]

D. *Privacy on the Societal Scale—Some Bases for a Judicial Balance*

As a partial counterweight to the elaborate doctrinal network for securing the public interest in a free flow of information, the courts have delineated several constitutionally grounded rights in personal information that are deserving of protection. Given the danger that the first amendment rationale of *Hill* may be unduly extended at the sacrifice of informational privacy, these affirmative constitutional doctrines take on added significance. Perhaps the most clearly developed of these is the right of associational privacy, which recognizes the "vital relationship between the First Amendment freedom to associate and privacy in one's association."[317] Thus, when the government attempts to gather data concerning an individual's association with a group dedicated to the advancement of certain beliefs

315. *House Hearings on Commercial Credit Bureaus* 28. *See also* text accompanying note 248 *supra*.

316. *Cf.* PRIVACY AND BEHAVIORAL RESEARCH 4:

> [I]f behavioral research is to be effective, some modification of the traditional concept of informed consent is needed.
>
> . . . [T]he right [of the subject] to discontinue participation at any point must be stipulated in clear terms. In the meantime, when full information is not available to him and when no alternative procedures to minimize the privacy problem are available, the relationship between the subject and the scientist (as well as with the institution sponsoring the scientist) must be based upon trust. This places the scientist and the sponsoring institution under a fiduciary obligation to protect the privacy and dignity of the subject . . . .

317. NAACP v. Alabama, 357 U.S. 449, 462 (1958). *See also* Bates v. City of Little Rock, 361 U.S. 516 (1960). The principle has been applied whether the organization is forced to reveal the names of its members, as in *NAACP v. Alabama*, or the individual is compelled to reveal all organizations of which he has been a member, as in Shelton v. Tucker, 364 U.S. 479 (1960).

in "political, economic, religious, or cultural matters,"[318] it must "convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest."[319] However, the successful assertion of associational privacy appears to depend upon a showing that disclosure will result in restraint on an individual's ability to exercise his freedom of association.

The threat that computer technology poses to associational privacy is particularly acute. Electronic data-processing techniques facilitate the composition of lists of people associated with various types of activities and institutions from previously uncollated bodies of data; thus, relationships can be inferred from apparently disparate information.[320] The risks created by this type of analysis will be magnified if the trends toward increased collection of individualized data, the computerization and centralization of information, and information exchange through computer networks continue. As these practices become more prevalent, judicial relief based upon a constitutional right of associational privacy will be an increasingly important source of protection even though it is available only when the "chilling effect" of the inquiry is in some measure attributable to state action rather than purely private conduct.[321] In addition,

318. 357 U.S. at 460.

319. Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 546 (1963). *See also* District 12, UAW v. Illinois State Bar Assn., 389 U.S. 217 (1967).

320. For example, computerized financial records could easily provide a list of all payments that an individual has made to a given organization, or even to a person known to be an officer of the organization. Similarly, the records of an airline ticket reservation system can be audited to procure passenger lists of all flights taken by a surveillance suspect, and the passenger lists could be compared with a list of the known members of an organization. *See* text accompanying notes 103-04 *supra*.

321. The Supreme Court has not been very demanding in applying the state action requirement in associational privacy cases, however. In *NAACP v. Alabama*, the Court reversed a civil contempt judgment that had been entered against the NAACP for refusing to reveal "the names and addresses of all its Alabama members and agents" as required by state law. The Court rejected the argument that any repression following from disclosure would be the result of action by private parties. The "crucial factor," in the Court's view, was "the interplay of governmental and private action, for it is only after the initial exertion of state power [in demanding the list] that private action takes hold." The NAACP had shown that "on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." 357 U.S. at 462-63. Dicta in Shelton v. Tucker, 364 U.S. 479, 486-87 (1960), indicates that the "private pressure" to be avoided is not merely the kind that follows from widespread publication of membership lists, but rather may be found in the actions of those who have economic power over the member of an unpopular group:

> Even if there were no disclosure to the general public, the pressure upon a teacher to avoid any ties which might displease those who control his professional destiny would be constant and heavy. Public exposure, bringing with it the possibility of public pressures upon school boards to discharge teachers who belong to unpopular or minority organizations, would simply operate to widen and aggravate the impairment of constitutional liberty.

the principle that a person is entitled to confidentiality in his institutional and human relationships may provide a keystone for placing computerized information systems under effective legislative or administrative controls that go beyond the minimal level of protection that can presently be afforded by the courts through the Constitution and tort litigation.

Closely related to the right of associational privacy is another judicially recognized individual interest—the right to possess ideas and beliefs free from governmental intrusion. As the Supreme Court recently stated in *Schneider v. Smith*,[322] first amendment guarantees and the concept of associational privacy "create a preserve where the views of the individual are made inviolate. This is the philosophy of Jefferson that 'the opinions of men are not the object of civil government, nor under its jurisdiction . . . .' "[323]

As is true of associational privacy, the information-handling capacity of the modern technologies poses a special threat to privacy of ideas and beliefs. Computers provide governmental and nongovernmental institutions with increased ability to store, retrieve, and analyze an individual's opinions as reflected in psychological tests, attitude surveys, machine-assisted instruction, and simulations. These and other techniques for securing subjective data are sufficiently subtle that the individual may not even suspect that his basic beliefs are being scrutinized or that his responses will be preserved and examined by people beyond his immediate ken. Preservation of the fruits of this type of data surveillance also threatens another personal interest that some courts have recognized—the individual's ability to make a fresh start and escape from past errors when there is no overriding public interest in the preservation and chronologically remote disclosure of the information.[324]

The judicial recognition of freedom of association and belief is part of a tradition that is even more basic to the nation's philosoph-

322. 390 U.S. 17 (1968).

323. 390 U.S. at 25. In a concurring opinion, Justice Fortas stated: "No agency may be permitted to require of a person, subject to heavy penalty, sworn essays as to his 'attitude toward the form of Government in the United States' . . . ." 390 U.S. at 27.

324. *See, e.g.*, Melvin v. Reid, 112 Cal. App. 285, 292, 297 P. 91, 93 (1931); *cf.* Comment, *The Right of Privacy: Normative-Descriptive Confusion in the Defense of Newsworthiness*, 30 U. CHI. L. REV. 722, 728-30 (1963); Address by Arthur J. Goldberg, The Owen J. Roberts Memorial Lecture: Can We Afford Freedom?, Feb. 20, 1969, at 9; note 117 *supra* and accompanying text.

Several state courts have recognized equitable relief against the maintenance of a plaintiff's picture in a police rogues' gallery or the dissemination of copies to other law enforcement agencies. *See, e.g.*, Itzkovitch v. Whitaker, 117 La. 707, 42 S. 228 (1906). *See also* State *ex rel.* Mavity v. Tyndall, 224 Ind. 364, 66 N.E.2d 755 (1946); State *ex rel.* Reed v. Harris, 348 Mo. 426, 153 S.W.2d 834 (1941). *But cf.* Hodgeman v. Olsen, 86 Wash. 615, 150 P. 1122 (1915).

ical fabric—the conception of government as an institution of limited powers that is obliged to meet a heavy burden of justification when it undertakes a program or course of action that will inhibit the freedom of its citizens. As Justice Douglas remarked in his opinion for the Court in *Schneider*: "The purpose of the Constitution and Bill of Rights, unlike more recent models promoting a welfare state, was to take government off the backs of people."[325] This attitude certainly is reflected in the spate of Supreme Court decisions recognizing various "zones of privacy."[326]

It is axiomatic that the power conveyed by widespread surveillance or information control can constrict individual freedom, and pressures that lead in that direction must be resisted. Arguments or supplications couched in terms of governmental economy or gains in administrative efficiency cannot justify every demand for greater power to extract, manipulate, store, and disseminate personal data. In the past these very objectives have been advanced and then rejected as justifications for universal fingerprinting[327] or passports for travel within the country.[328] By way of contrast there is the example of the Chinese Communist Party's attempt to register and monitor every household in China.[329]

Today, however, the accelerating development of technology and the almost exponential expansion of the ability to manipulate personal information in variegated ways may be altering the balance between the individual citizen and those institutions in society that seek to exercise control over him. The individual has little ability to protect himself against governmental and private snoopers who can employ sophisticated electronic surveillance devices to monitor

---

325. 390 U.S. at 25.

326. *See, e.g.*, Stanley v. Georgia, 37 U.S.L.W. 4315, 4317 (April 8, 1969); Mancusi v. De Forte, 392 U.S. 364 (1968); Katz v. United States, 389 U.S. 347, 360-61 (1967); Berger v. New York, 388 U.S. 41, 57 (1967); Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

327. *See, e.g.*, United States v. Kalish, 271 F. Supp. 968, 970 (D.P.R. 1967):

> There can be no denying of the efficacy of fingerprint information, photographs, and other means of identification in the apprehension of criminals and fugitives. . . . When arrested, an accused does not have a constitutional right of privacy that outweighs the necessity of protecting society and the accumulation of this data. . . .
>
> However, when an accused is acquitted of the crime or when he is discharged without conviction, no public good is accomplished by the retention of criminal identification records. . . . His privacy and personal dignity is [*sic*] invaded as long as the Justice Department retains "criminal" identification records, "criminal" arrest [records], fingerprints and a rogue's gallery photograph.

See also McGovern v. Van Riper, 137 N.J. Eq. 24, 43 A.2d 514 (1945); note 324 *supra*.

328. *Cf.* Aptheker v. Secretary of State, 387 U.S. 500 (1964); Edwards v. California, 314 U.S. 160 (1941).

329. *See generally* J. Cohen, THE CRIMINAL PROCESS IN THE PEOPLE'S REPUBLIC OF CHINA, 1949-1963, at 19-20, 106-08 (1968).

his activities and obtain information about him.[330] More substantial legal safeguards than those currently available are required merely to maintain the status quo in the privacy field. The Supreme Court appears to have recognized this in recent electronic eavesdropping cases; it has employed expansive general principles to protect a person's legitimate expectations concerning personal privacy.[331] In the process, the Court has used the traditional constitutional restraints on search and seizure of tangible objects to restrict governmental acquisition of personal information.[332]

The need to accommodate existing legal doctrine to meet the excesses of a new communications medium is hardly a novel or revolutionary idea. Indeed, our current theories of privacy emerged from a recognition that the mass media possess unique abilities to harm the individual. As Dean Bloustein has observed:

330. Josephson, Book Review, 15 UCLA L. REV. 1586, 1596 (1968):

> It may be fair to say that the law need not prevent the disclosure of information about another, where the speaker himself has not manifested sufficient concern in its disclosure to safeguard against its dissemination. This view would justify the leeway given to field-glass snoops and naked-ear eavesdroppers. Both types of intruders may be frustrated by simple precautions and the burden of self-protection is not a heavy one. Where electronic surveillance and undercover spies are involved, however, the individual may be truly incapable of coping with the threat to his privacy other than by refusing to talk.

331. *See* Katz v. United States, 389 U.S. 347, 352 (1967), a case involving a police wiretap on a public telephone:

> No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.

See also Note, *From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection*, 43 N.Y.U. L. REV. 968, 981 (1968):

> [T]he *Katz* decision has pointed the way towards a complete reorientation in the analysis of problems relating to governmental intrusion into individuals' private affairs. Rather than relying on an interpretation of the nature and legitimacy of the Government's searching activity, the Court's holding was based solely on the individual's expectation of privacy. . . . It follows that even inadvertent, nonpurposeful government activity may constitute an "unreasonable search" if it unearths nonpublic information legitimately within the personal dominion of the aggrieved party.

332. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353 (1967) ("[W]e have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.' "); Berger v. New York, 388 U.S. 41 (1967). *See also* Warden v. Hayden, 387 U.S. 294, 304 (1967); Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order"*, 67 MICH. L. REV. 455, 475-76 (1969) ("Privacy is invaded at the point when the information in [testimonial communications like conversations and letters] is obtained by one not entitled to it, and this can easily be by aural or visual perception. . . . Where privacy is invaded by seeing or listening, the search and seizure are identical and simultaneous . . . ."); Note, *supra* note 331, at 974 ("The essence of a search is the gathering of nonpublic information; this is as effectively accomplished by the reception of visual stimuli as by actual, physical penetration . . . ."). *But see* the strong dissents of Justice Black in *Katz*, 389 U.S. at 364-74, and *Berger*, 388 U.S. at 78-81, concluding that the fourth amendment applies only to tangible property.

> [T]he small town gossip did not begin to touch human pride and dignity in the way metropolitan newspaper gossip mongering does. Resources of isolation, retribution, retraction and correction were very often available against the gossip but are not available to anywhere near the same degree, against the newspaper report. . . . Gossip arose and circulated among neighbors, some of whom would know and love or sympathize with the person talked about. . . .
>
> . . . A newspaper report, however, is spread about as part of a commercial enterprise among masses of people unknown to the subject of the report and on this account it assumes an imperious and unyielding influence. Finally . . . the newspaper tends to be treated as the very fount of truth and accuracy, and tends to command open and unquestioning recognition of what it reports.
>
> Thus, only with the emergence of newspapers and other mass means of communication did degradation of personality by the public disclosure of private intimacies become a legally significant reality.[333]

Computerized information-handling elevates these difficulties of context and interpretation to a new order of magnitude. The computer printout is less likely to reflect or reveal the bias or the selectivity of the information gatherer than is the newspaper article or television report.[334] Similarly, if the newspaper is viewed as a "fount of truth and authenticity," the computer projects an infallible and omniscent image across the mind of the average American, despite its occasional and well-publicized foibles. Consequently, the probability that an apparently disinterested account or report will be accepted as true—a consideration that disturbed Justice Harlan in his concurring opinion in *Time, Inc. v. Hill*[335]—seems much more substantial when the report is based on a computerized dossier than when it appears in a newspaper article or a television newscast. Most dangerous of all, perhaps, is the fact that computerized information-handling is a low-visibility operation. An individual may never learn that a dossier exists or have any real knowledge of what is in it. If he does know of its existence, he is not likely to receive

333. Bloustein, *Privacy As an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 984 (1964). *See also* Ludwig, *"Peace of Mind in 48 Pieces vs. Uniform Rights of Privacy*, 32 MINN. L. REV. 734, 748-50 (1948), in which the author argues that the scope of privilege recognized in actions for invasion of privacy has varied according to the characteristics of the medium of publication.

334. Karst, *"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342, 350 (1966): "Just as every truth is a partial truth, every statement of fact is at least partly an evaluation. The courts' abiding inability to separate 'fact' from 'opinion' is inherent in the use of language to represent things." *See also* Silver, *Privacy and the First Amendment*, 34 FORDHAM L. REV. 553, 566 (1966).

335. 385 U.S. 374, 409 (1967): "The public is less likely to view with normal skepticism what is written about [the plaintiff] because it is not accustomed to seeing his name in the press and expects only a disinterested report."

notice that an erroneous or misleading entry has been made in his file, or that details of his life have been revealed to people who have no colorable need to know them. Thus, citizens generally have no opportunity to correct or augment the contents of their files or control their use. Decisions affecting their personal destinies, may be made on the basis of unseen data from unknown sources having untested reliability.

But beyond these apprehensions concerning the dangers to particular individuals, the unregulated computerization of personalized information may have a numbing effect on the value of privacy as a societal norm and may debilitate the citizen's conception of the government as a benevolent institution. As in the case of electronic surveillance, the climate or atmosphere of suspicion engendered by an accumulation of invasions of privacy is of far greater concern than the direct harm caused by the incidents themselves.[336] In a dissenting opinion in *Lopez v. United States*,[337] Justice Brennan drew a distinction between informers and informers who carry concealed recording or transmitting devices. He was concerned about the special risks to which individuals are subjected when law enforcement agencies use electronic surveillance devices, and, in turn, about the implications that these risks have for society as a whole:

> It is not an undue risk to . . . compel [people] to use discretion in choosing their auditors, to make damaging disclosures only to persons whose character and motives may be trusted. But the risk which . . . today's decision impose[s] is of a different order. It is a risk that third parties, whether mechanical auditors . . . or human transcribers of mechanical transmissions . . . —third parties who cannot be shut out of a conversation as conventional eavesdroppers can be, merely by a lowering of voices, or withdrawing to a private place—may give independent evidence of any conversation. There is only one way to guard against such a risk, and that is to keep one's mouth shut on all occasions.[338]

Another observer has stated: "Even quite reasonable surveillance practices which should be permissible in themselves, may in the aggregate form be the basis of a terribly oppressive society."[339] This

336. *See, e.g.*, Osborn v. United States, 385 U.S. 323, 343 (1966) (Justice Douglas, dissenting):

> [T]he privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.

See also note 309 *supra*.

337. 373 U.S. 427 (1963).

338. 373 U.S. at 450.

339. Josephson, *supra* note 330, at 1599.

seems to be one of the lessons to be learned from the popular outcry concerning the National Data Center, some of the Census Bureau's questions, and the congressional hearings on credit bureaus.[340]

Unfortunately, the existing tort remedies seem geared to the activities of private mass communications media. The existing common-law structure therefore does not appear readily transferable to regulate the use of personal information by computer networks whose privacy-invading activities are far more subtle than those that traditionally have confronted the courts. The deficiencies of current doctrine will become increasingly apparent as public and private sector data systems continue to integrate. Thus, if the individual is to retain any meaningful control over decisions affecting his life and if society is to avoid becoming enveloped in an Orwellian miasma, the law must adjust and impose limitations and responsibilities upon the proprietors of systems that process personal information. If it fails to do this, these data managers inevitably will wield an increasing measure of power as a greater proportion of each individual's life history is recorded, centralized, and made available on computer networks.

VI. The Handling of Personal Information by the Federal Government: Current Practice

In seeking guidance for developing an adequate system of legal principles to regulate the flow of personal information in society, it is appropriate to examine the most comprehensive contemporary statutory and administrative framework concerning data transfers—the body of rules controlling the federal government's power to acquire and disseminate information. It is especially appropriate to undertake such an analysis if, as concluded in the preceding section, the common-law remedies are inadequate to meet the new challenges. Inasmuch as certain aspects of the federal experience provide insights into the special problems created by information interchange between the private and public sectors and among the federal government and other units of government, the following discussion also is intended to indicate some of the consequences of the national computer networks which are on the horizon.

340. *See generally Hearings on 1970 Census Questions Before the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. (1966); *House Hearings on the Computer and Invasion of Privacy; Senate Hearings on Computer Privacy; House Hearings on Commercial Credit Bureaus; Senate Hearings on Credit Bureaus; Hearings on Retail Credit Company.*

A. *Confidentiality—The Census Bureau Model*

The Bureau of the Census long has been one of the federal government's chief data gatherers. The decennial census has evolved from the simple "enumeration" of the populace described in the Constitution[341] to a comprehensive survey seeking numerous items of data. Citizens are now required to answer questions about their health, employment, finances, and even the number of bathrooms in their homes.[342] Several of the questions on recent censuses have been included at the request of social planners from both governmental and nongovernmental institutions, as well as industry groups desirous of procuring information that will aid in making marketing decisions.

Information for the census is extracted under threat of criminal penalties,[343] and, on the few occasions when the propriety of census techniques has been questioned in the courts, the Bureau's broad discretion has been upheld.[344] In recent years, however, the symbiotic relationship between the Census Bureau's seemingly insatiable appetite for personal information and the Damoclean sword of criminal sanctions has engendered an increasing number of complaints from the public, with resulting criticism in Congress.[345] A proposal to demand data on religious affiliations was a special target of the critics,[346] and that line of inquiry was eliminated from the

---

341. U.S. CONSTITUTION, art. 1, § 2.

342. *See generally Hearings on 1970 Census Questions Before the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. (1966).

343. 13 U.S.C. §§ 221-224 (1964).

344. *See, e.g.*, United States v. Rickenbacker, 309 F.2d 462, 463-64 (2d Cir. 1962), *cert. denied*, 371 U.S. 962 (1963):

> The questions contained in the household questionnaire related to important federal concerns, such as housing, labor, and health, and were not unduly broad or sweeping in their scope. The fact that some public opinion research experts might regard the size of the household questionnaire "sample" as larger than necessary to obtain an accurate result does not support a conclusion that the census was arbitrary or in violation of the Fourth Amendment.

Cf. United States v. Moriarity, 106 F. 886, 890-92 (C.C.S.D.N.Y. 1901).

345. *See* note 347 and text accompanying notes 527-32 *infra*. *See also* Rickenbacker, *The Fourth House*, NATL. REV., May 21, 1960, at 325. The author has had occasion to examine some of the mail received by Senator Ervin and the Subcommittee on Constitutional Rights on the subject of the census and governmental questionnaires. It indicates a strong concern over the loss of individual privacy and growing governmental intrusiveness. The staff of Congressman Jackson Betts of Ohio, a leader in the census reform movement in the House, reports the same phenomenon. *See also* Detroit News, March 23, 1969, at 8A, col. 1: "Congressmen report receiving large volumes of mail from constituents demanding census reform legislation. Similar reactions are being received by the news media from persons who want to thwart any invasion of their privacy . . . ."

346. *See, e.g., Hearings on 1970 Census Questions Before the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. 70 (1966) (statement of Morris B.

1970 census. But the dissatisfaction runs deeper and a number of bills have been introduced in Congress that would sharply limit the kinds of questions that respondents are legally required to answer.[347] In April 1969 the Senate Subcommittee on Constitutional Rights, chaired by Senator Ervin, held broad hearings on the status and the possible development of a theory to protect citizens from abusive inquiries by the government.[348]

Notwithstanding the recent criticisms, it generally is agreed that the Census Bureau has an unequalled record among federal agencies in preserving the confidentiality of personal information.[349] In fact, the Census Bureau's enviable history frequently has been cited by advocates of a National Data Center as indicative of the type of security that can be achieved by a statistical organization.[350]

The basic confidentiality provisions of the Census Act impose three prohibitions on Census Bureau employees. They may incur criminal penalties[351] if they

> (1) use the information furnished under the provisions of . . . [the Act] for any purpose other than the statistical purposes for which it is supplied; or
> (2) make any publication whereby the data furnished by any par-

Abram, President, American Jewish Committee); *id.* at 3 (statement of Representative Cornelius Gallagher). *See also id.* at 45-46 (statement of the Most Reverend Paul F. Tanner, General Secretary, National Catholic Welfare Conference):

> Many commercial and welfare interests can be served by statistics about religious affiliation. In industrial and commercial circles it is well known that markets are influenced by the religious affiliation of prospective customers. Market analyses . . . would be more complete—and better suited to the needs of the citizenry—if they incorporated projections based on statistics on religious affiliations.

347. *See, e.g.*, H.R. 20, 91st Cong., 1st Sess. (1969), which would limit criminal penalties to refusals to answer questions involving name and address, relationship to head of household, sex, date of birth, marital status, and visitors in the home at the time of the census. *See also* S. 494, 90th Cong., 1st Sess. (1969); 113 CONG. REC. H16,231-32 (June 19, 1967).

348. These hearings have not been published as of this writing. Among the witnesses were three law professors, including the author, and a number of citizens deemed "representative of thousands from every walk of life who have complained to Congress about unwarranted invasion of their personal privacy and about increased harassment by government agencies in their everlasting quests for information." Office of the Senate Constitutional Rights Subcommittee, press release, April 14, 1969.

349. *See, e.g.*, Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 218-19 (1968). In testimony before the House Subcommittee on Census and Statistics on May 8, 1969, Congressman Cornelius E. Gallagher revealed that the Census Bureau resisted pressure to disclose the names of all Japanese-Americans following the outbreak of World War II.

350. *See, e.g., House Hearings on the Computer and Invasion of Privacy* 51-56; *Hearings on 1970 Census Questions Before the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. 27-28 (1966).

351. Maximum penalties of $1000 fine and two years' imprisonment for wrongful disclosure of information by employees are set forth in 13 U.S.C. § 214 (1964).

> ticular establishment or individual under this title can be identified; or
> (3) permit anyone other than the sworn officers and employees of the Department or bureau or agency thereof to examine the individual reports.[352]

There have been a few instances in which these commandments have been violated. In 1963, for example, the Census Bureau reportedly provided the American Medical Association with a "statistical" list of 188 doctors residing in Illinois. The list was broken down into more than two dozen income categories, and each category was further subdivided by medical specialty and area of residence.[353] It also is likely that there is a fair amount of data disclosure at the information-gathering level by the large corps of people employed to carry out the Bureau's periodic canvassing.[354] This type of abuse may be reduced by wider use of direct mail techniques.

One basic infirmity in the Census Act restrictions is their ambiguity, which makes consistent application difficult. The classification of information as "statistical" within the meaning of subdivision (1), rather than as "identifying" or "surveillance," will depend in large measure on how the information is presented and what can be inferred from it by a user who is intimately familiar with the subject matter of the underlying question. It also may be unrealistic to require Census Bureau employees to make hypothetical judgments about whether or not a user will be able to determine the identity of respondents from a particular tabulation. The task of making a present judgment about a possible future use is bound to become more difficult as computer analysis techniques become more refined. Moreover, the Bureau's burden of making these judgments will increase because requests to release data in small aggregates of respondent units rather than large tabulations are certain to proliferate as a result of the trend toward computer analysis of "microdata" in the social sciences.[355]

Pressure for the relaxation of Census' confidentiality restrictions has come from other sources. In *St. Regis Paper Co. v. United States*,[356] the Supreme Court held that the confidentiality provisions of the Census Act did not prevent other branches of the government from compelling a respondent to produce file copies of reports that

352. 13 U.S.C. § 9(a) (1964).
353. Hirsch, *The Punchcard Snoopers*, THE NATION, Oct. 16, 1967, at 369.
354. *See* Miller, *On Proposals and Requirements for Solution*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 224, 230 (1968).
355. *See* pt. II.C. *supra*.
356. 368 U.S. 208 (1961).

it had given to the Bureau. The Court reasoned that the rights granted by the statute were enforceable only against the Census officials receiving the information, and did not attach to the information itself. Fortunately, the *St. Regis* case was legislatively overruled in 1962,[357] and retained copies of census reports are now immune from subpoena.

A number of disturbing questions raised by the case remain, however. For one thing, *St. Regis* can be interpreted as supporting the proposition that, in spite of the collecting agency's pledge of confidentiality, a copy of any report supplied to the Government is amenable to compulsory process in the absence of a specific statute exempting it.[358] Moreover, if the Census Act's confidentiality restrictions are enforceable only against officials authorized to gather the information initially, it is conceivable that the statutory prohibition cannot be enforced against a third party who lawfully obtains information from the Bureau and then proceeds to misuse the data.

In any event, the protection afforded by the legislative resolution of the *St. Regis* affair may prove to be more apparent than real. It does not prevent any interested agency from framing a questionnaire asking questions that appear on a census survey, thereby compromising the latter's confidentiality. Moreover, many agencies use the ploy of having the Census Bureau conduct surveys for them.[359] This technique enables the inquiring agency to procure

357. 13 U.S.C. § 9(a)(3) (1964).

358. 368 U.S. at 218:

> Congress did not prohibit the use of the reports *per se* but merely restricted their use while in the hands of those persons receiving them, *i.e.*, the government officials. Indeed, when Congress has intended like reports not to be subject to compulsory process it has said so.

359. A list furnished the author by Senator Ervin's office shows that in a period of approximately two years the Census Bureau performed surveys for over twenty federal, state, and local governmental organizations. In many instances the surveys were taken weekly, monthly, or annually. It is difficult to determine how many respondents were involved; the figure 6,000,000 seems conservative.

A perusal of some of the questionnaires reveals them to be lengthy and, on occasion, intrusive. A document entitled Longitudinal Retirement History Survey, collected by the Census Bureau for the Department of Health, Education, and Welfare, is almost twice as long as the 1970 census. It is being sent to a sample group of recent retirees who are receiving social security benefits. The survey apparently is a response to a recommendation by the Advisory Council on Social Security that data be collected on people who come on the benefit rolls before age sixty-five. Some of its inquiries, in addition to numerous probing interrogatories about the respondent's finances and past employment, include:

> What have you been doing in the last four weeks to find work?
> When you retire, do you expect to live here or somewhere else? Where?
> Taking things all together, would you say you're very happy, pretty happy, or not too happy these days?
> Do you have any artificial dentures?
> Is there some kind of care or treatment that you have put off even though you may still need it? What is this care or treatment for?

the desired data directly and in the precise form it deems necessary. At the same time, it gets the benefit of the quasicoercive demeanor of an official Census Bureau questionnaire.[360] Furthermore, once the collected data is transferred to the agency that requested the survey,[361] the excellent record of the Census Bureau becomes irrelevant. At this point the requesting agency has the capacity to use and disseminate the data in any way that its officials and employees feel is appropriate. Most of the data turned over by Census will be in the form of computer tapes, and this type of transfer has special implications, which are discussed in the next section of this Article.[362]

Another potential deficiency in the Census Act is the provision granting the Secretary of the Department of Commerce discretionary authority to "furnish to Governors of States . . . courts of record, *and individuals,* data for genealogical and other proper purposes, from the population, agriculture, and housing schedules,"[363] subject to the palliative that "[i]n no case shall information furnished . . . be used to the detriment of the persons to whom such information relates."[364] This grant of authority operates as an ill-defined excep-

Do you (or your spouse) see or telephone your parent(s) as often as once a week?
What is the total number of gifts that you . . . give to individuals per year . . . ?
How many different newspapers do you receive and buy regularly?
About how often do you . . . go to a barber shop or beauty salon?
What were you doing most of last week?

Senator Ervin has introduced a bill designed to remedy intrusive federal data-gathering activities. S. 1791, 91st Cong., 1st Sess. (1969). The bill was the focal point of the April 1969 hearings of the Subcommittee on Constitutional Rights. *See* note 348 *supra. See also* text accompanying notes 544-45 *infra.*

360. Although most of the surveys conducted for other agencies by the Census Bureau are voluntary, that fact often is not indicated on the documents. A recent voluntary home survey questionnaire was boldly marked: "This Form Should Be Completed And Returned Whether You Are A Renter Or A Homeowner, Whether You Live In A One-Family Home, Or A House With Two Or More Families, An Apartment, Or Any Other Type Of Building." This approach apparently is typical. In addition, respondents who do not reply are sent follow-up letters (occasionally by certified mail) or receive personal visits.

361. The Census Bureau normally codes and edits the data, sends one copy to the requesting agency, and retains the raw data and one copy of the coded data. See Survey of New Beneficiaries: Report Compiled in Response to Senator Ervin's Letter of Feb. 28, 1969, at 3 (prepared by Robert M. Ball, Commissioner of Social Security) (copy on file with the *Michigan Law Review*).

362. *See* pt. VI.B. *infra.*

363. 13 U.S.C. § 8(a) (1964) (emphasis added). *See also id.* at § 8(b): "The Secretary may furnish transcripts or copies of tables and other census records and make special statistical compilations and surveys for State or local officials, private concerns, or individuals upon the payment of the actual, or estimated cost of such work." Section 8(b) also permits the furnishing of census data, but seems limited to statistical and aggregate material.

364. 13 U.S.C. § 8(c) (1964). The prohibition on detrimental use extends only to material appearing in the three censuses enumerated in section 8(a). St. Regis Paper Co. v. United States, 368 U.S. 208, 215 (1961).

tion to the prohibitions in the confidentiality section.[365] The quantum of protection provided by the vague standard of "detriment to the individual" seems scant; it can be vitiated all too easily by a strict judicial interpretation. Indeed, in one state case "detriment" was construed to mean that the subject of the data must be deprived of something that is lawfully his[366]—a test that appears impossible to satisfy except under the most limited circumstances.

The most serious limitation on confidentiality restrictions of the type governing the Census Bureau, however, is not the scheme's potential ineffectiveness as a means of deterring wrongful disclosures by agency personnel. Rather, it is the fact that information transactions are engaged in without giving notice and an opportunity to be heard to the citizen whose files are subject to the risk of wrongful disclosure or disclosure under the statutory provision described in the preceding paragraph. This is coupled with a total failure to deal with the problem of how an individual can correct erroneous entries or add ameliorating information to the contents of a potentially damaging file.

Admittedly, the absence of procedural safeguards has not had catastrophic consequences in the past, primarily because the Census Bureau has operated on the basis of aggregate data and has restricted itself to relatively bland statistical endeavors. But the twin pressures of increased information-gathering and widespread detailed multivariate analysis will be felt not only by Census but by all information-handling agencies. As a result, fissures in the existing structure for privacy protection are almost certain to develop.

B. *Transfers of Information Among Federal Agencies*

As has been pointed out earlier,[367] the proliferation of large time-sharing computer systems and the existing cost levels are motivating

365. 13 U.S.C. § 9(a) (1964). The primary utilization of this exception seems to be by individuals procuring data from earlier censuses about themselves, especially for proof of age in connection with Social Security, Medicare, and other benefits. *See Hearings on the 1970 Census Questions Before the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. 29 (1966) (statement of Dr. A. Ross Eckler, Director, Bureau of the Census).

366. In Edwards v. Edwards, 239 S.C. 85, 121 S.E.2d 432 (1961), the defendants in an inheritance dispute contended that the plaintiffs' use of census records as evidence was detrimental to their interests. The South Carolina Supreme Court rejected this construction of the Act:

> The use of such information to the detriment of those to whom it relates does not mean detriment in the sense of a financial loss flowing from establishing the truth in a Court of law. If plaintiff is the . . . brother of defendants, he is entitled to an equal share and they have not been deprived of anything that was lawfully theirs but only that which they had no lawful right to claim as theirs.

239 S.C. at 91, 121 S.E.2d at 435.

367. *See* pt. III.B. *supra*.

information managers to share bodies of data in which they have a common interest. Within the federal government, this tendency is legitimized by a statute granting the Director of the Bureau of the Budget power to "require any Federal agency to make available to any other Federal agency any information which it has obtained from any person."[368] This authority can be exercised, however, only if at least one of the following conditions is met: (1) the information consists of statistical summaries, (2) it is not confidential at the time of transfer, (3) the persons who supplied the information have consented to its release, or (4) the transferee agency has power to collect the information itself.[369] Moreover, transferred information is subject to the same confidentiality restrictions that protected it in the originating agency, and any employee of the transferee agency who violates these restrictions is subject to the same penalties that apply to employees of the transferor organization.[370]

These provisions are logical enough on their face and seem to present little direct threat to privacy.[371] However, as is true of much of the existing regulatory scheme, they were conceived with the model of a manual transfer of manila folders in mind. Thus, they may prove to be quite difficult to apply in the context of frequent large-scale transfers of information among compatible agency computer systems. Computerized information can be transferred either by manually exchanging it in stored form—a reel of magnetic tape or a magnetic disc—or by feeding it directly from one computer memory unit to another through a machine interface. Both procedures permit the data to be duplicated by the transferee unit so that the original can remain with the collecting agency. The transferred information often will not carry any indication of its source, particularly if it is used by the borrower on a random-access basis or is amalgamated with other data or transmogrified in some other fashion.

In short, the indicia of the process of transferring computerized data are so evanescent that there does not appear to be any effective way to insure that the limitations on the Bureau of the Budget's statutory authority are honored. Although it is feasible for the trans-

368. 44 U.S.C. § 422(e) (Supp. III, 1965-1967). This power is subject to several exceptions, the most notable of which encompasses "the obtaining or releasing of information by the Internal Revenue Service." *Id.* The term "Federal agency" is defined by 44 U.S.C § 426(a) (Supp. III, 1965-1967) to include "any executive department, commission, independent establishment, corporation owned or controlled by the United States, board, bureau, division, service, office, authority, or administration in the executive branch of the Government . . . ."

369. 44 U.S.C. § 423(b) (Supp. III, 1965-1967).

370. 44 U.S.C. § 423(a) (Supp. III, 1965-1967).

371. The exception for the respondent's consent to release of information can be easily abused, of course. *See* pt. V.C. *supra.*

feree machine to be programmed to indicate the source whenever part of the transferred data is generated as output, the cost of the process might exceed any savings gained by sharing the data. And in cases in which the borrowed information is integrated with other data, the process might not even be feasible except in the most general way. Moreover, it is unrealistic to assume that middle- and low-level administrators are familiar with the disparate standards of confidentiality and penalties for violations that are in force in all of the possible transferor organizations. Of course, it is technologically possible (although a dubious use of computer capacity) to program all potential transferor computers so that they will provide this information with each bit of data they transfer. Then, in the style of some majestic Wagnerian prologue, each transferee computer would print out the rules and regulations applicable to the use of any borrowed information that is to be retrieved. Whether or not they would be read or followed is another matter.

At some point, surely, the basic assumption underlying the statutory transfer restrictions on the Budget Bureau—that privacy can be protected by aggregating confidentiality requirements—must break down by virtue of its sheer complexity. The House Committee on Government Operations examined an aggregation scheme as a method of protecting privacy in the context of a data center consisting of information from thirty to forty federal agencies. The committee rejected this system as impractical:

> Each agency would have numerous bureaus and other subdivisions. For each of these hundreds of bureaus there would have to be developed a complicated set of standards whereby every type of report would have to be evaluated.
>
> . . . [E]ach of the hundreds of bureaus would have to rate every type of information it possesses separately for all other bureaus that might request the information.[372]

The obvious alternative to an aggregation scheme, a single scale of confidentiality that can be used to rate every report received by the Government, also was rejected. The committee was of the opinion that the imposition of a uniform scale would obscure the fact that "the sensitivity of a given document is not intrinsic, but varies with the relationship between the agency gathering the data and the agency receiving it."[373]

372. PRIVACY AND THE NATIONAL DATA BANK CONCEPT 14-15.

373. *Id.* at 15. The Committee went on to give the following example: "[A] person giving his income for the HUD housing survey would have his confidence violated if this income figure were to be given to the Internal Revenue Service, but not if it were given to the Bureau of the Census for aggregate purposes."

Resolution of the dilemma posed by the deficiencies of both systems is essential if a rational scheme of confidentiality is to be developed. As will be discussed more fully in a later section,[374] the answer may lie in proper application of the technology itself. Hierarchical storage techniques, privacy systems built into the hardware and software, and use of cryptography principles—all supported by recast legislative and administrative regulations—may provide the necessary protective mix. Consequently, a number of studies and experimental information-sharing projects must be undertaken before the intricacies of maintaining confidentiality of personal information that moves on an interagency basis can be appreciated. Unfortunately, there is substantial danger that the present trend toward data transfers will continue unabated, with yesterday's aggregated confidentiality restrictions[375] providing a shield against information infiltration that is as porous as McNamara's Vietnam Wall.

C. *Federal-State-Local Transfers of Information*

The trend toward data-sharing within the federal government has been paralleled by the development of numerous data centers at the regional,[376] state,[377] and local[378] levels. There has also been in-

374. *See* pt. VII.A. *infra.*

375. An excellent example of the disregard for confidentiality within the federal government arising from cavalier data transfers is the wide latitude permitted in the disclosure of income tax returns; *see* Treas. Reg. § 301.6103(a)—1(f) (1965):

> [I]f the head of an executive department . . . or of any other establishment of the Federal Government, desires to inspect, or to have some other officer or employee of his department or establishment inspect, a return . . . in connection with some matter officially before him, the inspection may, in the discretion of the Secretary of the Treasury or the Commissioner of Internal Revenue or the delegate of either, be permitted upon written application . . . .

See also Treas. Reg. §§ 301.6103(a)-1(e) (1960); 301.6103(a)-1(g) (1960); 301.6103(a)-100-107 (1961).

In United States v. Costello, 255 F.2d 876, 822-84 (2d Cir.), *cert. denied*, 357 U.S. 937, *rehearing denied*, 358 U.S. 858 (1958), the defendant was prosecuted for income tax evasion. The prosecutor asked an Internal Revenue agent to inspect the tax returns of the veniremen on the jury panel, and to provide a summary of events in their history of dealings with the IRS which might tend to make them unfavorably disposed toward the prosecution. This list was used as a basis for peremptory challenges, and, in spite of the fact that no comparable information was available to the defendant, the court held that this was permissible under the statute and applicable regulations.

376. *See, e.g., Senate Hearings on Computer Privacy* 49-66 (plan for a regional economic data bank for the St. Louis region).

377. *See Project—The Computerization of Government Files: What Impact on the Individual?*, 15 UCLA L. REV. 1371, 1401-10 (1968) (proposals for a state data-processing system in California). *See generally Hearings on Government Electronic Data Processing Systems Before the Subcomm. on Census and Statistics of the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. 231-36 (1966) (statement of Dr. Thomas C. Rowan, Vice President, Systems Development Corporation); Pennsylvania Senate Bill No. 239 (1969) (state police computerized data bank).

378. *See, e.g., A City Where Computers Will Know About Everybody*, U.S. NEWS & WORLD REP., May 15, 1967, at 78 (New Haven, Connecticut); *Senate Hearings on Computer Privacy*, pt. 2, at 303-25 (Washington, D.C.).

creasing pressure to establish interfaces for the transmission of data between these centers and the federal government. In some respects, the sharing of information among different levels of government, and perhaps even with the private sector, is more threatening to individual privacy than the transmission of data within the federal government. In the first place, multilevel systems of this type are bound to increase the potential audience for sensitive data. In addition, local information handlers may be more likely to be inefficient, insensitive, or animated by malice or idle curiosity about the content of the data than are their federal counterparts. In many cases they are in a better position to harm individual citizens through misuse of personal information than relatively remote federal officials. Moreover, the difficulties of interpreting noncomparable bodies of information are likely to arise in more extreme form when data centers that have been designed to meet the particular needs of different levels of government later are patched together to effect data transfers.[379]

In spite of these concerns, programs already are in existence that provide for the sharing of personal data between the federal government and the states. For example, section 6103 of the Internal Revenue Code grants access to federal income tax returns to state officers charged with the collection of any state tax.[380] The treasury regulations under this section also open federal estate and gift tax returns to states that are willing to reciprocate by allowing the federal government to peruse their tax records.[381] Over forty states have entered "agreements of cooperation" with the Internal Revenue Service,[382]

379. *Cf. Hearings on Data Processing Management* 24-25 (statement of Phillip S. Hughes, Deputy Director of the Bureau of the Budget):

> The incompatibility that continues to exist among equipment and software remains a serious obstacle in making the most effective and efficient use of our vast ADP resources. This problem is assuming even greater significance in view of the accelerated trend toward the development of systems that involve the exchange of data in machine-processable form among many different computers. This trend is illustrated by the growing interchange of information among Federal, State, and local governments, between the private sector and governmental agencies, and within major segments of Government and industry.

380. INT. REV. CODE of 1954, § 6103(b)(2):

> All income returns filed with respect to the taxes imposed by chapters 1, 2, 3, and 6 . . . shall be open to inspection by any official body, or commission, lawfully charged with the administration of any State tax law, if the inspection is for the purpose of such administration or for the purpose of obtaining information to be furnished to local taxing authorities . . . . The inspection shall be permitted only upon written request of the governor of such State . . . .

Cf. Rev. Rul. 54-598, 1954-2 CUM. BULL. 121. *See generally* Clurman & Provorny, *Publicity and Inspection of Federal Tax Returns*, 46 TAXES 144 (1968).

381. Treas. Reg. § 301.6103(a)-1(d) (1965).

382. CCH 1968 STAND. FED. TAX REP. ¶ 5209.576.

and more than twenty-five of these have begun exchanging magnetic tapes with the federal government.[383]

Although the administrative and revenue advantages of tax information interchange are obvious, the fact remains that they are being achieved at the expense of exposing financial data concerning our citizens to a wider group of people—in many cases to a wider group than the taxpayer ever anticipated would be privy to it. Abandonment of the program is not being suggested; an evaluation of the privacy-protecting procedures that are being employed does seem appropriate, however. A tax return in the wrong hands can result in great damage to an individual and, in certain circumstances, elements of organized crime or unscrupulous political operatives would be very interested in seeing selected tax returns. They undoubtedly would be willing to pay handsomely for that privilege, and this makes the maximum statutory penalty of 1,000 dollars fine and one year imprisonment for wrongful disclosure[384] seem dangerously ineffective as a deterrent.

Comparable threats to personal privacy are inherent in the development of "integrated information systems" for law enforcement agencies. This is a technique that has been advocated to counteract the difficulties that the police encounter in dealing with a highly mobile criminal population. The Federal Bureau of Investigation has established a National Crime Information Center, which eventually will enable the states and many of the large cities to have immediate access to computerized files of stolen property and wanted persons.[385] Although application of the new technologies to public-record information of this sort does not pose a significant independent threat to personal privacy, it is obvious that a wide variety of information is useful in law enforcement. Thus, pressures to include more extensive data in the system are almost certain to increase.[386]

383. CONG. REC. E2656 (daily ed. Apr. 3, 1968).

384. INT. REV. CODE of 1954, § 7213. This section also provides that federal employees convicted of wrongful disclosure are to be discharged from their jobs.

385. TASK FORCE REPORT: SCIENCE AND TECHNOLOGY 72-74.

386. The TASK FORCE REPORT: SCIENCE AND TECHNOLOGY 72 suggests fifteen general categories of information for inclusion in police intelligence systems, including state motor vehicle registrations, sex and narcotics offenders, and known criminal associates. John de J. Pemberton, Jr., the Executive Director of the American Civil Liberties Union, has expressed apprehension that a different kind of information could find its way into intelligence files:

> Our . . . concern regarding the proposed FBI Crime Information Center is that it will be the repository not just for crime information . . . but for other types of information not at all relevant to [the] prevention and detection of crime. It is said that other Federal investigative agencies will be invited to feed whatever information they choose into the huge reservoir that the national network of com-

Realistically, the National Crime Information Center has to be viewed as the initial element of a broader crime information network that eventually may link all of the nation's law enforcement agencies into a single data system. New York, which is probably the leader among the states in computerizing police records, already has in operation the essential features of a system built around a single computer center in which the various state and local law enforcement agencies store and retrieve data through remote-access terminals.[387] This system could easily be linked both to the FBI's center, and, in the other direction, to police station houses and individual patrol cars.[388]

The same pressures that are leading to information integration among different levels of government may lead to even more expansive systems. In today's climate of student activism and public and governmental reactivism, it is not unreasonable to believe that interfaces between law enforcement and educational data centers are feasible. After all, the Justice Department is obligated to enforce recent federal legislation concerning students who engage in disruptive campus activities,[389] and proposals for comparable state legislation are becoming increasingly fashionable.[390] The process would be exedited for all concerned if data collected by the FBI, the Justice Department, local law enforcement agencies, and the universities could be coordinated and distributed to the interested organizations. But the risks to the individual are enormous.

A refined sifting process to insure that damaging information is not allowed to flow unverified and uncontrolled among local, state, and federal organizations is needed. Unfortunately, the designers and advocates of integrated information systems have been more concerned with making data available than they have been with

puters will store and retrieve. Data concerning a person's political beliefs and associations, gathered by various Federal security agencies, thus will become part of the crime data bank. The implications are obvious: every local police official will be able to learn with facility not only whether a suspect has a criminal record, a proper disclosure, but also whether he has at all deviated from his community's political or social norms, a highly improper disclosure which threatens the enjoyment of first amendment protections.

House Hearings on the Computer and Invasion of Privacy 182-83.

387. For a description of the New York State Identification and Intelligence System, *see House Hearings on the Computer and Invasion of Privacy* 146-81; *cf.* TASK FORCE REPORT: SCIENCE AND TECHNOLOGY 69, 160.

388. TASK FORCE REPORT: SCIENCE AND TECHNOLOGY 35-36. New York City currently is using a system of computer-assisted dispatching of patrol cars, called "SPRINT" (Special Police Radio Inquiry Network). N.Y. Times, Dec. 29, 1967, § 7, at 53, col. 1.

389. *See, e.g.*, Pub. L. 90-550 (1968); Pub. L. 90-575, § 504(a) (1968).

390. *See, e.g.*, H. 815, 75th Gen. Ass. of the State of Missouri; H. 92 (Minnesota Legislature, introduced Jan. 15, 1969); H. 1138, 1st Sess., 32d Legislature of the State of Oklahoma.

safeguarding individual privacy.[391] Although the objectives of these planners cannot be faulted, their inability to define the proper parameters of their task can be.

D. *The Federal Government and the Public—The Freedom of Information Act*

The disclosure of information gathered by the federal government to private individuals and organizations creates its own threats to personal privacy. In many cases, the information held by the government has been extracted from the individual under a statutory mandate or through the use of subtle forms of coercion.[392] Nonetheless, if any of this vast store of personal data finds its way into one of the mass media, the broad implications of *Time, Inc. v. Hill*[393] and other first amendment cases indicate that it can be used with virtual impunity. The problem is not simply the press. Employers, creditors, business rivals, and a multitude of others having an "interest" in a particular individual also have occasion to seek information from the files of the federal government.

The past balance between the Government and the public has been altered radically by the enactment in 1967 of the Freedom of Information Act,[394] a relatively short piece of legislation that requires the

---

391. For example, the TASK FORCE REPORT: SCIENCE AND TECHNOLOGY 74-75 devoted a page and a half to the problem of individual privacy and concluded, "This problem still needs much more study, analysis and judgment."

The vulnerability of computerized crime information systems is illustrated by the following account of difficulties in the New York State Identification and Intelligence System:

> The reluctance of law enforcement agencies to share information on organized crime may pose fatal problems for a state plan to develop a central computerized source of information about criminals.
>
> . . . .
>
> "When it gets right down to it," [a] state official said, "I just don't know whether [New York County District Attorney Frank S.] Hogan is going to let N.Y.S.I.I.S. see the sensitive kind of stuff he's got in his files, especially when there's a possibility it might fall into the hands of a corrupt sheriff or police chief at the other end of the state."

N.Y. Times, Jan. 15, 1968, § 1, at 27, col. 4.

392. *See* pt. V.C. *supra.*

393. For a discussion of the impact of *Hill* and related cases, *see* pt. V.B. *supra.*

394. 5 U.S.C. § 552 (Supp. III, 1965-1967). *See generally* Davis, *The Information Act: A Preliminary Analysis*, 34 U. CHI. L. REV. 761 (1967); Paul, *Access to Rules and Records of Federal Agencies: The Freedom of Information Act*, 42 L.A. BAR BULL. 459 (1967); Sky, *Agency Implementation of the Freedom of Information Act*, 20 ADMIN. L. REV. 445 (1968); Sobeloff, *The New Freedom of Information Act: What It Means to Tax Practitioners*, 27 J. TAXATION 130 (1967); Note, *The Freedom of Information Act: Access to Law*, 36 FORDHAM L. REV. 765 (1968); Recent Statute, 80 HARV. L. REV. 909 (1967); Note, *The Information Act: Judicial Enforcement of the Records Provision*, 54 VA. L. REV. 466 (1968).

The Act does not apply to records maintained by the federal courts. Cook v. Willingham, 400 F.2d 885 (10th Cir. 1968).

disclosure, upon request, of broad categories of information held by governmental agencies. The purpose of the statute is to insure that the public has access to enough information to enable it to scrutinize the activities of federal administrators, thereby providing a theoretical check on abuse. In the process of fulfilling this function, however, the Act is certain to have a profound effect upon an individual's capacity to prevent the circulation of information that he has divulged to the Government under various federal reporting programs.[395]

The conflict between the public's right to know and the individual's right to have some control over the flow of personal information held by the Government is extremely difficult to resolve, and it is doubtful that new legislation—even if it contained significantly more detail than the Freedom of Information Act—could offer more than general guidelines for handling the kaleidoscopic factual problems that will arise. Realistically viewed, however, the Information Act, perhaps unthinkingly, has partially resolved this conflict by establishing a statutory policy favoring disclosure of governmental records. In essence, it reverses the traditional presumption in favor of personal privacy, and places the burden on the information-holding agency to find a specific statutory ground for refusing to honor a request for disclosure.[396] In some instances the Act not only has shifted the burden of proof, it apparently has increased it as well. The most important statutory exemption from disclosure for purposes of the present discussion immunizes "personnel and medical files and similar files the disclosure of which would constitute a *clearly unwarranted* invasion of privacy."[397]

---

395. The fundamental conflict between these two objectives is perhaps best illustrated by the following excerpt from Statement of President Johnson on Signing Public Law 89-487 (the Freedom of Information Act) on July 7, 1966, reprinted in UNITED STATES DEPARTMENT OF JUSTICE, THE ATTORNEY GENERAL'S MEMORANDUM ON THE PUBLIC INFORMATION SECTION OF THE ADMINISTRATIVE PROCEDURE ACT ii (1967) [hereinafter ATTORNEY GENERAL'S MEMO]:

> A citizen must be able in confidence to complain to his Government and to provide information . . . .
>
> Fairness to individuals also requires that information accumulated in personnel files be protected from disclosure . . . .
>
> . . . .
>
> I have always believed that freedom of information is so vital that only the national security, not the desire of public officials or private citizens, should determine when it must be restricted.

396. The Act "does not authorize withholding of information . . . except as specifically stated" in nine exceptions. 5 U.S.C. § 552(c) (Supp. III, 1965-1967). *See* Benson v. General Servs. Administration, 289 F. Supp. 590 (W.D. Wash. 1968). *See also* § 552(a)(3).

397. 5 U.S.C. § 552(b) (Supp. III, 1965-1967). Professor Davis, *supra* note 394, at 798, has argued with considerable logic that this provision forces the government official who has custody of a requested document to commit "an invasion of personal privacy

The Information Act also has greatly expanded the class of persons who can compel disclosure[398] by conferring standing on "any person,"[399] a standard that one commentator suggests may preclude the courts from attempting to strike a balance between the privacy interests threatened on the one hand, and the importance of access to the information on the other.[400] Although the Act permits anyone to compel disclosure judicially, it does not provide standing or assure notice, either of a request for information from an agency or of a judicial proceeding to compel an agency to honor a request, to the party whose interest is most clearly in jeopardy when disclosure of personal information is sought—the individual who is the subject of the data.[401] It is doubtful that reliance on bureaucratic inertia,

---

and it even requires an unwarranted invasion of personal privacy so long as it is not 'clearly unwarranted.' " Perhaps this is one situation in which the triumph of bureaucratic inertia over nice legalistic distinctions will prove beneficial. It is hard to imagine a low-level bureaucrat engaging in the type of sophisticated analysis suggested by Professor Davis. However, it also is disturbing to remember that these same officials will be making the initial determination of whether or not release of a given document constitutes an invasion of privacy—a question that few legal scholars would analyze the same way. But again Professor Davis: "The terms 'personnel and medical files,' 'similar files,' and 'clearly unwarranted invasion of personal privacy' are all reasonably clear standards . . . ." *Id.*

398. 5 U.S.C. § 552(a)(3) (Supp. III, 1965-1967) grants the federal district courts jurisdiction to enjoin the agency from withholding records or to order the production of records withheld. An action brought under this section is to take precedence on the docket over all matters except those the court considers to be of greater importance.

399. 5 U.S.C. § 552(a)(3) (Supp. III, 1965-1967); *see* Skolnick v. Parsons, 397 F.2d 523 (7th Cir. 1968).

400. Davis, *supra* note 394, at 765-66. *See also* Recent Statute, 80 HARV. L. REV. 909, 911 (1967):

> [A]gency records will be equally available to litigants, newspapers, and officious inquirers, unless the courts interpret "any person" restrictively to mean "any person with a legitimate interest." Such an interpretation arguably would actually help to expand the area of publicly available information, on the theory that if information were equally available to any person, the courts would hesitate to order disclosure of information to persons with a particularly strong need because the same or similar information would have to be made available to everyone. However, the purpose of the Act, as shown by the legislative history, would seem to preclude such an interpretation of "any person."

Notwithstanding the legislative history, the ATTORNEY GENERAL'S MEMO 28 concludes that a restrictive reading of "any person" is defensible. According to the Memorandum, the district court in a trial de novo under the Act can "exercise the traditional discretion of a court of equity" and weigh factors such as "the purposes and needs of the plaintiff, the burdens involved, and the importance to the public interest of the Government's reason for nondisclosure." Another route to the same result is a variable interpretation of the standard "clearly unwarranted invasion of privacy" described in note 397 *supra* and accompanying text: "Some regulations . . . provid[e] that the exemption will not apply to disclosures to certain classes of persons, on the assumption that release to such persons either would not be an invasion of privacy or would be justified by some public interest." Note, *Freedom of Information: The Statute and the Regulations*, 56 GEO. L.J. 18, 45 (1967).

401. *See* ATTORNEY GENERAL'S MEMO 28: "Following the statutory plan, the district court would presumably issue an order directed to the agency, which, under the language of the statute, is the only party defendant." The Memorandum did not discuss

obstinacy, or traditional administrative reluctance to disclose the contents of files to the public are adequate substitutes for giving the person whose privacy is threatened the right to participate in the process. A statutory scheme that ignores a supposedly basic societal norm such as the right to privacy by requiring a demonstration that disclosure "would constitute a clearly unwarranted invasion of privacy" and then fails to provide a mechanism for giving notice to the person most interested in discharging that burden gives the impression of having been sketched by a surrealistic draftsman.

Because the Information Act may have a drastic impact on prevailing standards of privacy, the scope of the exceptions permitting information to be withheld is crucial. Unfortunately, the language of these provisions ranges from the obscure to the opaque, and has moved Professor Kenneth Culp Davis to proclaim that the Act is "a shabby product indeed."[402] The statute is not even consistent in describing the units of information that may be withheld. The introductory sentence in the exemption section provides that the subdivisions are inapplicable to *"matters,"*[403] which would seem to indicate that the agencies are able to withhold individual items of information. This interpretation also appears consistent with the discretionary power to delete identifying details, which is given earlier in the Act.[404] Yet, several of the most significant exceptions are phrased in terms of "files," "memorandums," or "letters," so that it is possible to read the statute as exempting the release of all information in a given "file" if it fits the statutory categorization.[405] These constructions are conjectural, however, and the inescapable conclusion is that it is not clear whether the statutory exemptions apply to individual bits of information, specific documents, or entire files, or

the possibility that the party whose privacy was threatened by disclosure might be able to intervene in the action under Fed. R. Civ. P. 24. However, it is conceivable that the threat to privacy would be sufficient to confer that right. According to rule 24(a)(2), the test is whether or not "the applicant claims an interest relating to the property or transaction which is the subject of the action and he is so situated that the disposition of the action may as a practical matter impair or impede his ability to protect that interest . . . ." The real problem, of course, is lack of notice to the party whose personal data is being sought. Even when the agency refuses to release the data and is made the defendant in a court proceeding, 5 U.S.C. § 552(a)(3) (Supp. III, 1965-1967) provides that the action shall "take precedence on the docket over all other causes," and hence the data subject is quite likely to be presented with a *fait accompli.*

402. Davis, *supra* note 394, at 807.

403. 5 U.S.C. § 552(b) (Supp. III, 1965-1967).

404. 5 U.S.C. § 552(a)(2) (Supp. III, 1965-1967): "To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction."

405. *See generally* Davis, *supra* note 394, at 797-99.

whether synoptic or raw data will be treated differently than collated or evaluated information.

These interpretive difficulties are compounded in the context of computerized records. Of what relevance are words such as "files," "memorandums," "letters," and "matters," when the storage medium is a stack of tabulating cards, a reel of magnetic tape, or a disc? Does the Act envision the turning over of a tape or permitting the requesting party to duplicate it? If either is the case, it might enable the recipient to subject the data to highly detailed computer analysis that would reveal relationships and permit the drawing of inferences about people that would not be possible with less sophisticated methods. Another question is whether or not the Information Act obliges an agency to process all the data in its files on a given subject or to integrate its information with accessible data elsewhere within the Government. Is it possible that a person requesting disclosure of the data available on someone else has a right to have that data collated from the far reaches of the federal information system and printed out for him in dossier style?[406]

Perhaps the most confusing statutory exemption deals with "trade secrets and commercial or financial information obtained from a person and privileged or confidential,"[407] a provision which, as the *Attorney General's Memorandum* on the Act admits, is "susceptible of several readings, none of which is entirely satisfactory."[408] Even the legislative history of this section is less than pellucid, but it seems to indicate that Congress intended to exempt all privileged information, trade secrets, and information obtained by the government under a pledge or reasonable expectation of confidentiality.[409]

406. The rather arbitrary interpretations advanced by the Attorney General's Memorandum do little to alleviate the confusion. For example, 5 U.S.C. § 552(b)(6) (Supp. III, 1965-1967) exempts "matters that are . . . personnel and medical files *and similar files* the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" (emphasis added). The Memorandum concludes that this language encompasses all material contained in personnel and medical files, and "all private or personal *information contained in other files* which, if disclosed to the public, would constitute a clearly unwarranted invasion of . . . privacy." ATTORNEY GENERAL'S MEMO 36 (emphasis added).

The courts seem reluctant to impose any significant burden of search on the agencies; *see, e.g.*, Bristol Meyers Co. v. FTC, 284 F. Supp. 745 (D.D.C. 1968).

407. 5 U.S.C. § 552(b)(4) (Supp. III, 1965-1967).

408. ATTORNEY GENERAL'S MEMO 32. *See also* Davis, *supra* note 394, at 802-03, in which the author contends that a literal construction of this provision leads to the conclusion that "[t]he Act is a nullity with respect to all commercial or financial information, and with respect to all non-commercial and non-financial information which is privileged or confidential" (emphasis removed).

409. S. REP. NO. 813, CLARIFYING AND PROTECTING THE RIGHT OF THE PUBLIC TO INFORMATION, AND FOR OTHER PURPOSES, 89th Cong., 1st Sess. 9 (1965): "[Exemption four] is necessary to protect the confidentiality of information which . . . would customarily not be released to the public by the person from whom it was obtained. . . .

This interpretation, together with the statutory exception for "matters . . . specifically exempted from disclosure by statute,"[410] carves out a substantial area of immunity from disclosure; in effect, it superimposes the confusing structure of the Freedom of Information Act upon the existing morass of confidentiality statutes and regulations. This construction of the exemption also creates an intriguing dilemma. It is supported by the notion that if personal information that has been extracted under a pledge of confidentiality is not exempted from disclosure under the Information Act, the citizen's trust in the Government will have been betrayed. The fear, of course, is that people will be deterred from furnishing candid or voluntary reports in the future. On the other hand, if each agency's pledge of confidentiality is honored, then each may be able to immunize many of its records and activities from public scrutiny by the simple expedient of pledging confidentiality for all information gathered from the public.[411]

Since the Freedom of Information Act has so many theoretical and linguistic shortcomings, the manner in which the Act is administered by the agencies will determine how the conflict between the individual's right to privacy and the public's need to know is resolved.[412] Although it is too early to make a confident assessment of

---

It would . . . include information customarily subject to the doctor-patient, lawyer-client, lender-borrower, and other such privileges." The House Report is substantially similar, and also states that the exemption includes "information which is given to an agency in confidence, since a citizen must be able to confide in his Government. Moreover, where the Government has obligated itself in good faith not to disclose documents or information which it receives, it should be able to honor such obligations." H.R. REP. NO. 1497, CLARIFYING AND PROTECTING THE RIGHT OF THE PUBLIC TO INFORMATION, 89th Cong., 2d Sess. 10 (1966). *See also* Benson v. General Servs. Administration, 289 F. Supp. 590 (W.D. Wash. 1968). At present, there are nearly 100 statutes regulating access to information held by the Government. H.R. REP. NO. 1497, *supra*, at 10. *See also* ATTORNEY GENERAL'S MEMO 31-32.

Another problem is whether or not the exemption abrogates the doctrine of executive privilege. *See* Recent Statute, 80 HARV. L. REV. 909, 912 (1967). *Compare* Cooney v. Sun Shipbuilding & Drydock Co., 288 F. Supp. 708, 714 (E.D. Pa. 1968) ("[A] claim of executive privilege is validly made only by the head of the executive department or administrative agency involved, after actual personal consideration by that officer."), *with* Epstein v. Resor, 296 F. Supp. 214 (N.D. Cal. 1969) (grant of an executive privilege delegable within the Department of the Army upheld). Both of these cases were decided under the Freedom of Information Act.

410. 5 U.S.C. § 552(b)(3) (Supp. III, 1965-1967).

411. In Note, *Freedom of Information: The Statute and the Regulations*, 56 GEO. L.J. 18, 37 (1967), this possibility is described as "one of the greatest loopholes in the bill."

412. *Cf.* STAFF OF THE SUBCOMM. ON ADMINISTRATIVE PRACTICE AND PROCEDURE OF THE SENATE COMM. ON THE JUDICIARY, 90th Cong., 2d Sess., THE FREEDOM OF INFORMATION ACT (TEN MONTHS' REVIEW) 1 (Comm. Print, 1968):

> The usefulness of the act . . . will not depend on court decisions alone. The act called for a change in attitude, and hence, the success or failure of the act depends on the sound judgment and faithful execution of the law bv agency officials. The record of the agencies in this regard is far from clear.

the Act's impact on personal privacy, there is some basis for optimism. Apparently, many of the agencies affected by the Act are developing regulations for administrative appeals from initial decisions refusing disclosure.[413] This procedure should bring the hard cases before a relatively high-level official who is more likely to be attuned to the privacy implications of disclosure than is the custodian of the document. These administrators also are less likely to be pressured into releasing the requested data by the threat of litigation. Of course, the Act's goal of rapid and easy disclosure might be defeated by interjecting an administrative appeal that must be exhausted before the judicial remedy becomes available. This certainly would be true if ministerial personnel adopt a general policy of "bucking it upstairs" whenever confronted with a request for disclosure. However, the reported cases thus far indicate that the principal users of the Information Act are not the representatives of the mass media,[414] who had lobbied for its enactment,[415] but private litigants invoking the Act as a supplement to the discovery rules,[416] parties threatened by administrative action,[417] and companies interested in contracting with the Government.[418] In these situations, at least, it does not seem that the public's need to know will suffer unduly if administrators proceed with caution and err on the side of protecting privacy.

Although agency regulations along these lines will help, they cannot overcome all of the linguistic and philosophical inharmony between the Freedom of Information Act and the needs of individual privacy in the computer age. The statute simply ignores the implications of increased governmental data collection and transmis-

---

413. This procedure was apparently contemplated by Congress. *See* ATTORNEY GENERAL'S MEMO 28; H.R. REP. No. 1497, *supra* note 409, at 9. For an example of regulations governing such administrative appeals, *see* 15 C.F.R. § 60.11 (1968) (Census Bureau); 14 C.F.R. §§ 1206.800-.805 (1968) (National Aeronautics and Space Administration).

414. *See* N.Y. Times, June 10, 1968, § 1, at 22, col. 4:

> Senator Long, chairman of the Senate Administrative Practice and Procedure subcommittee, said in a statement he was surprised that the news media had not taken greater advantage of the remedies provided by the act.
>
> "I feel certain that if more people were aware of the act, especially newsmen, we would see more demands for information being made on the agencies," he said.

See also Wall St. J., Oct. 23, 1968, at 1, col. 1.

415. Davis, *supra* note 394, at 803.

416. *See, e.g.*, Cooney v. Sun Shipbuilding & Drydock Co., 288 F. Supp. 708 (E.D. Pa. 1968); Clement Bros. Co. v. National Labor Relations Bd., 282 F. Supp. 540 (N.D. Ga. 1968); Barceloneta Shoe Corp. v. Compton, 271 F. Supp. 591 (D.P.R. 1967).

417. *See, e.g.*, Bristol-Meyers Co. v. FTC, 284 F. Supp. 745 (D.D.C. 1968); American Mail Line, Ltd. v. Gulik, 37 U.S.L.W. 2497 (D.C. Cir., Feb. 17, 1969); Tuchinsky v. Selective Serv. Sys., 294 F. Supp. 803 (N.D. Ill. 1969); *cf.* Martin v. Neuschel, 396 F.2d 759 (3d Cir. 1968).

418. *See, e.g.*, Benson v. General Servs. Administration, 289 F. Supp. 590 (W.D. Wash. 1968).

sion resulting from the capacities of the new technology. In the event a National Data Center with interfaces with state, local, and private centers is established, the potential applications of the Act stagger the mind. This problem has yet to be subjected to a rational analysis. Also unnoticed thus far is the nexus between the Information Act and the Supreme Court's decision in *Hill.*[419] Considering the two in tandem, the Freedom of Information Act gives the public in general—and the mass communications media in particular—a statutory right of access to a large segment of the constantly expanding and deepening store of personal information held by the federal government, and *Hill* may permit the cavalier use of this data by the mass communications media by presaging the elimination of the restraint of any duty of reasonable care in a broad range of situations. The juxtaposition of the Act and a broad judicial conception of the first amendment is likely to have startling and significant effects.

E. *Information in Transit—Wiretapping and the Crime Control Act*

As a result of the enactment of title III of the Omnibus Crime Control and Safe Streets Act of 1968,[420] the nation's law enforcement officers now have extensive statutory authority to intercept communications.[421] Despite its recent enactment and the insights that developed out of the contemporaneous public debate over the National Data Center, the Crime Control Act in many ways is a technological anachronism. Even though a substantial and rapidly increasing proportion of the transmissions carried by the nation's communications networks involve data in digital form,[422] the Act is framed almost

419. *See* text accompanying notes 280-89 *supra.*

420. 82 Stat. 197 (1968) [hereinafter Act]. Ironically, large portions of title III of the Act were taken from the proposed Right of Privacy Act of 1967, S. 928, 90th Cong., 1st Sess. (1967), which led one senator to observe: "Title III, in the form proposed by the administration as S. 928, was properly described as the Right to Privacy Act. As accepted by the committee [and ultimately enacted], Title III is more appropriately described as the End to Privacy Act." S. REP. No. 1097, 90th Cong., 2d Sess. 182 (1968) [hereinafter S. REP. No. 1097] (individual views of Senator Hiram Fong). *See generally* Theoharis & Meyer, *The "National Security" Justification for Electronic Eavesdropping: An Elusive Exception,* 14 WAYNE L. REV. 749 (1968).

421. For a discussion of the vast number of state and federal crimes that will support a grant of eavesdropping authority under title III, *see* Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order",* 67 MICH. L. REV. 455, 481-82 (1969). *See also id.* at 486-95.

422. Less than five per cent of the total communications channel milage currently consists of data communications. UNIVAC Brief at H&I-2. However, the annual volume of data communications is doubling every two years, Comments of Microwave Communications, Inc., at 3 (March 5, 1968) (submitted in connection with *In re* Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities, FCC Doc. No. 16,979), and an official of the American

entirely in terms of voice communications.[423] As a consequence, its application to digital data transmissions is uncertain at best. At worst the Crime Control Act may be construed to permit privacy-invading interceptions that apparently were not contemplated by its draftsmen.

Much of the interpretive difficulty stems from the fact that the Act does not define "communications." However, numerous cases decided under section 605 of the Communications Act,[424] many of which are referred to in the legislative history of title III of the Crime Control Act, indicate that the term may apply only to transmissions of information from one person to another.[425] Thus, the term might not extend to eavesdropping on machine responses to a remote user's inquiry or to the direct transfer of data from one computer to another.[426] This construction would leave data communications without the protections against wiretapping that are embodied in the federal act; there would be protection only to the extent that

---

Telephone and Telegraph Company has predicted that it will not be long until the volume of information carried by data communication will exceed that carried by voice transmissions. UNIVAC Brief at H&I-3 to H&I-5.

423. An excellent example is the definition of "intercept" given in section 2510(4) of the Act: "the *aural* acquisition of the contents of any wire or oral communication through the use of any . . . device" (emphasis added). Unless the word "aural" is given a strained construction, the Act does not seem to be applicable to a tap of the communications lines of a time-sharing system when the tap is linked to another computer that will print out the intercepted data or display it visually. The absurdity of such a result is emphasized by the fact that some computers are able to respond orally. The IBM 7770 Audio Response Unit, for example, "allows the computer to give oral answers to questions by use of a pre-recorded vocabulary." International Business Machines Co. news release, June 29, 1967. The quality and use of this oral response capability undoubtedly will increase.

424. 47 U.S.C. § 605 (1964). Section 605 was amended by section 803 of the Crime Control Act.

425. *E.g.*, Rathbun v. United States, 355 U.S. 107 (1957); Goldstein v. United States, 316 U.S. 144 (1942); Nardone v. United States, 308 U.S. 338 (1939); Weiss v. United States, 308 U.S. 321 (1939); Nardone v. United States, 302 U.S. 379 (1937). *See also* note 426 *infra*.

426. United States v. Dote, 371 F.2d 176, 180 (7th Cir. 1966):

> The *dial* telephone system does not generally require human intervention to connect two telephones. The telephone company was not therefore the intended recipient of the signal. The "intended recipient" was the telephone of another subscriber . . . . Ultimately, the intended human recipient of the signal was the subscriber called.

Cf. S. REP. No. 1097, at 90:

> Other forms of surveillance are not within the proposed legislation. . . . An examination of telephone company records by law enforcement agents . . . would be lawful because it would not be an "interception." (*United States v. Russo*, 250 F. Supp. 55 (E.D. Pa. 1966)). The proposed legislation is not designed to prevent the tracing of phone calls. The use of a "pen register," for example, would be permissible. But see *United States v. Dote*, 371 F.2d 176 (7th 1966). The proposed legislation is intended to protect the privacy of the communication itself and not the means of communication.

See also Goldstein v. United States, 316 U.S. 114 (1942).

state legislation affords some relief[427] and the fourth amendment proscribes governmental activity in conjunction with a criminal prosecution.[428] From a privacy perspective, therefore, it actually would be better to bring computer communications under the limited safeguards of the Act.

Common sense undoubtedly will prevent a horse-and-buggy construction of the Crime Control Act and the courts can be expected to extend its terms to data transmissions. But this may be easier said than done in several contexts. Significant and troublesome problems will arise in connection with the Act's grant of authority to eavesdrop on a transmission when one of the parties to the communication gives his consent.[429] It is unclear who the "parties" to a computer transmission are, particularly in the case of a time-sharing system in which a user may have access to data deposited by some but not necessarily all of the other users. The provision at least suggests that an authorized user may permit law enforcement officials to gain access to any part of the computer's memory bank that is accessible through his terminal. But who are the "parties" when the communication simply involves a machine-to-machine transfer of information?

Another source of difficulty is the section of the Act allowing eavesdropping on an "extension telephone."[430] This provision has broader application than the reference to that mundane instrumentality would suggest because the term encompasses all equipment "furnished to the subscriber or user by a communications common carrier . . . and being used by the subscriber or user in the ordinary course of its business."[431] Thus, if the input-output devices of a remote-access computer system, such as the increasingly common touch-tone telephone, are supplied by the telephone company—a situation that is not unlikely in view of the extensive control that the communications carriers have over the equipment that can be linked to their network[432]—police access to one carrier-owned output

427. The conflict between state and federal wiretapping laws has long been a difficult problem. *See, e.g.*, Lee v. Florida, 392 U.S. 378 (1968); Pugach v. Dollinger, 277 F.2d 739 (2d Cir. 1960), *aff'd per curiam*, 365 U.S. 458 (1961); Recent Development, *Inadmissibility of Wiretap Evidence in State Courts*, 1968 DUKE L.J. 1008. *See generally* Berger v. New York, 388 U.S. 41, 45-49 (1967).

428. *See generally* Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967); Schwartz, *supra* note 421.

429. Act § 2511(2)(c).

430. *See generally* Schwartz, *supra* note 421, at 495-96.

431. Act § 2510(5)(a)(i).

432. The telephone carriers' ability to control "foreign attachments"—the linking of customer-supplied equipment to the national telephone network—currently is a subject of heated controversy. A series of recent decisions has sharply limited the telephone companies' monopoly over transmitting devices; *see In re* American Tel. &

device[433] of a computerized credit bureau system would permit extensive eavesdropping that is unregulated by even the lenient standards of the Crime Control Act.

Nor is there any doubt that police forces will be in a position to take advantage of any permissive construction the courts may give to the Act. As noted earlier,[434] the telephone companies are beginning to convert voice transmissions from analog to digital form, which means that the law enforcement agencies will need to have the equipment and expertise necessary to intercept digital communications in order to carry on traditional tapping activities.

Title III of the Crime Control Act, as is true of many federal statutes governing information transfers,[435] provides only a narrow grant of standing to protest the illicit acquisition of personal information. The remedy of suppressing illegally seized eavesdropping evidence[436] extends only to an "aggrieved person," a term that is defined as "a party to any intercepted . . . communication or a person against whom the interception was directed."[437] The first portion of the quoted clause again requires a construction of the word "party." According to the legislative history of the passage, the provision will not safeguard a person who was the *subject* of an illegally seized communication that originates or terminates at a computer data center containing individualized personal information.[438] The section authorizing civil damages makes this limitation even clearer, stating that the remedy is available only to a person "whose wire or oral communication is intercepted, disclosed, or used" in violation of the Act.[439]

Denying a remedy to the party who is most affected by disclosure is objectionable when normal telephone conversations are in-

---

Tel. Co., 15 F.C.C.2d 605 (1968) ("Foreign Atatchment" tariff revisions in AT&T Tariff, FCC Nos. 259, 260, 263); *In re* Use of Carterfone Device in Message Toll Telephone Service, 13 F.C.C.2d 420 (1968). However, it seems clear that the communications carriers will still supply a substantial number of the devices used in data transmissions.

433. One example of an essential carrier-supplied communications device which may be vulnerable to eavesdropping is described in IBM Brief I-69: "A modem (modulation/demodulation device) is generally required to convert data signals into a form suitable for transmission. Since modems are included within the foreign attachment provisions, they must be furnished by the carriers if they are to be used with a public exchange service."

434. *See* notes 85-86 *supra* and accompanying text.

435. *See* pt. VI.A.-E. *supra.*

436. Act § 2518(10).

437. Act § 2510(11).

438. S. REP. No. 1097, at 91, 163, 173.

439. Act § 2520.

volved;[440] in the context of the interception of transmissions of extensive computerized dossiers and other forms of personal data, it becomes totally offensive, especially in light of system operators' tendency to cooperate with the police.[441] Conceivably, a court could be persuaded that the statute's standing provision was framed with only voice communication in mind and therefore should not be extended to data communication. A distinction between voice and data communication for standing purposes might be drawn in terms of their qualitative difference[442] and the system operator's relative lack of interest in protecting the data subject, his allegiance being to the system user. Inasmuch as the Crime Control Act's limitation on standing is based on the desire to minimize the exclusion of reliable evidence in criminal cases,[443] it should not be extended to civil litigation—especially damage actions to remedy improper interception and use of data communications. Of course, in the unlikely event that the operative passages of the Act are construed to apply only to person-to-person communications, then the individual who is the subject of intercepted data might not be barred by the statutory limitations on standing. This would afford little succor to the data subject, however, since the cases involving standing to protest against wiretapping and eavesdropping in a situation not governed by statute have been extremely restrictive.[444]

The legislative history of the second portion of the standing clause—"person against whom the interception was directed"—is rather sparse,[445] but a reference to *Jones v. United States*[446] indicates that it probably was taken from the following passage in the opinion in that case:

---

440. *See* Schwartz, *supra* note 421, at 484-86.

441. *See, e.g.*, notes 104, 228 *supra* and accompanying text.

442. *See* text accompanying notes 450-52 *infra*.

443. *See* On Lee v. United States, 343 U.S. 747, 755 (1952); Pitler, *"The Fruit of the Poisonous Tree" Revisited and Shepardized*, 56 CALIF. L. REV. 579, 586-88 (1968).

444. In Alderman v. United States, 37 U.S.L.W. 4189 (March 10, 1969), the Supreme Court held that under the fourth amendment a party who was merely the subject of an illegally seized conversation does not have standing to suppress evidence taken from the illegal interception.

445. S. REP. No. 1097, at 91, merely states that the language "is intended to reflect existing law" and cites several cases.

446. 362 U.S. 257 (1960). The legislative history also cites Mancusi v. De Forte, 392 U.S. 364 (1968), which the Supreme Court had not decided when the Senate Report was written. In *Mancusi*, the Supreme Court held that since the papers seized at the petitioner's office were the property of his employer, his claim of standing to suppress the fruits of the search would have to be based on the language of the fourth amendment proclaiming the "right of the people to be secure in their . . . houses." 392 U.S. at 367. The court then cited *Jones* and concluded that the "capacity to claim the protection of the Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion." 392 U.S. at 368.

> In order to qualify as a "person aggrieved by an unlawful search and seizure" one must have been a victim of a search and seizure, one against whom the search was directed, as distinguished from one who claims prejudice only through the use of evidence gathered as a consequence of a search or seizure directed at someone else. . . . The restrictions upon searches and seizures were obviously designed for protection against official invasion of privacy and the security of property. They are not exclusionary provisions against the admission of kinds of evidence deemed inherently unreliable or prejudicial. The exclusion in federal trials of evidence otherwise competent but gathered by federal officials in violation of the Fourth Amendment is a means for making effective the protection of privacy.[447]

The Supreme Court's language seems to give standing to anyone who has been the victim of an invasion of privacy, which, if carried over to the Crime Control Act, would afford the data subject an opportunity to vindicate his rights. Although Justice Fortas construed the *Jones* passage in this fashion in his dissenting opinion in *Alderman v. United States*,[448] a majority of the Court took a constrictive view of its earlier language in *Jones*; they limited standing to those who were parties to the conversation and those with a special interest in the premises on which the violation took place.[449] Since the decision in *Alderman* followed the enactment of the Crime Control Act, that case's reconstruction of the *Jones* language does not necessarily furnish the standard for interpreting the words "person against whom the interception was directed." Obviously, however, there is every likelihood that the federal courts will adhere to the Supreme Court's narrow view of standing, although a distinction between voice and data interceptions should be urged.

The preceding discussion admittedly is highly episodic and superficial. The newness of the legislative scheme and the uncertain movements of the technology caution against more than a tentative presentation at this time. The specific problems chosen for description merely highlight a fundamental shortcoming of title III of the Crime Control Act. By virtually ignoring data communications and the

447. 362 U.S. at 261.

448. 37 U.S.L.W. 4189, 4198 (March 10, 1969) (footnote omitted):

> It is my position that this quotation [from *Jones*, containing the language "one against whom the search was directed"], read in light of the Court's rejection of property concepts, requires that we include within the category of those who may object to the introduction of illegal evidence "one against whom the search was directed." Such a person is surely "the victim of an invasion of privacy" and a "person aggrieved," even though it is not his property that was searched or seized. . . . The Government violates his rights when it seeks to deprive him of his rights by unlawfully seizing evidence in the course of an investigation of him and using it against him at trial.

449. 37 U.S.L.W. at 4192-93.

new computer technology, the Act makes it possible for law enforcement agencies to treat these increasingly important information transfers as if they were nothing more than telephone conversations. This failure to differentiate between types of communications displays either a lack of awareness of recent developments in communications or a degree of disingenuousness on the part of the draftsmen. Given the preoccupation with voice communication at the time the legislation was enacted, its imprecise language probably is attributable to the former.

The differences between voice and data communications are marked. Days of continuous wiretapping[450] may be necessary to obtain a significant amount of information from telephone conversations, and even then the "evidence" often will consist of soft, hearsay narratives. Unlike the normal telephone flow, however, a data communications circuit may be in virtually continuous high-speed operation, transmitting extensive bodies of information that have been purged of trivial or extraneous matter and contain a high degree of hard, record data.[451] In many instances this information will have been extracted under the coercive force of a criminal statute, a governmental ukase, or as a precondition of receiving some social or financial benefit. Data transmissions also are more likely than telephone conversations to contain privileged or confidential data. These differences in character between wiretapping on voice communications and data communications in turn are dwarfed by the possibility of law officers using dial-access devices to extract data directly from a variety of public and private computer centers and networks. If the Crime Control Act is construed to permit the seizure of vast quantities of computerized information on the basis of routine ex parte applications[452]—without affording any mode of redress to the data subject—a major battle in the struggle to preserve individual privacy will have been lost. Rather than subjecting the field of electronic data transmission to the gauntlet of judicial construction of the inapposite language of the present Act, fresh legislative consideration of the subject seems desirable.

450. Act § 2518(5).

451. Conceivably, a tap on a trunk line connecting a primary and a backup central unit of a computer system could result in interception of the entire store of data present in the system. *Cf.* UNIVAC Brief at H&I-8 to H&I-9:

> In a highly critical real-time operation, the effects of computer breakdown are catastrophic. Therefore, in such operations, standby facilities are kept available. If a computer fails, it may instantly be drained of its crucial contents, both data and programs, and these transferred to the standby computer where operations are continued practically without interruption.

452. For a discussion of the weaknesses in the judicial supervision provided by the Act, *see* Schwartz, *supra* note 421, at 483-86.

VII. Safeguarding the Privacy of Computerized Information

The present legal structure, at both the state and federal levels, appears to be virtually unprepared to cope with the threats to privacy that rapidly are becoming a part of our computerized age. The fragmented, ad hoc approach that has been taken to informational privacy problems is disheartening, for it simply aggravates the existing system's unsuitability for solving the problems raised by the computer. The result is confusion concerning the scope of protection afforded by various common-law doctrines and legislative provisions, and, quite frequently, uncertainty regarding the source of law applicable to a particular invasion of privacy. Moreover, isolated public responses to individual threats—as exemplified by the debate over the proposed National Data Center—may draw an undue amount of attention. With public concern focused on relatively narrow problems, there is a substantial risk that many legitimate social interests relating to privacy and the free dissemination of information will be ignored or left to the mercies of interested administrators. As argued at an earlier stage of this Article,[453] a broad conceptual framework is necessary to achieve a rational balance between the often competing objectives of preserving personal privacy and maximizing the benefits of efficiency inhering in the new technologies. In order to come to grips with this task more effectively, it is desirable to consider the range of privacy-protecting safeguards that are technologically and practically feasible for use in conjunction with a modern information system.

A. *Technological Methods of Protection—The Quest for Security*

The problem of insuring the physical security of computerized information thus far has received little more than passing mention in most commentaries,[454] even though improvements in security methods are a prerequisite to the effective use of several types of large multiple-access systems.[455] In point of fact, a variety of mechan-

453. *See* pt. IV.C. *supra.*

454. In 1966, computer expert Paul Baran testified: "As one who has for many years been interested in the problems of preserving privacy in interconnected computer-communications systems, I have been unable to find [a] large body of literature [on security devices] . . . ." *Hearings on 1970 Census Questions* 5.

455. *See, e.g.*, Kramer & Livingston, *Cashing In on the Checkless Society*, 45 Harv. Bus. Rev., Sept.-Oct. 1967, at 141, 143, in which it is suggested that two of the major technical problems preventing the implementation of a "checkless-cashless society" based on computer systems are "[c]hoosing and applying a numbering to identify sys-

ical techniques have been developed, others presently are possible, and additional schemes undoubtedly will become feasible in the future.

Since many security devices and procedures of varying cost, complexity, and effectiveness may be available, the choice of an appropriate protective system will depend upon a prior determination of how much storage and transmission security the particular data base deserves and who should be allowed access to it. This often will be a difficult task, not only because opinions on the subject will diverge but also because information of differing degrees of sensitivity usually will be stored in the same complex system and various groups of people will have to be able to reach different parts of the data.[456] In addition, it often will be hard to perceive the nature and dimension of future challenges to security since there will be changes in the character of the information and its attractiveness to snoopers over time.

If the data stored in a given system is deemed sensitive enough to create a credible threat of eavesdropping on radiations from the equipment, the physical surroundings of the central processor and the remote terminals probably can be protected with shielding materials.[457] A related technique might be desirable for the stored data as well.[458] In the case of remote-access systems, protection against wiretapping can be achieved by using "scramblers" to garble the data before transmission, and installing complementary devices in the authorized terminals to reconstitute the signal.[459] If scrambling or

---

tem users" and "[p]erfecting security protection systems and devices for preventing accidental or fraudulent transactions." *Cf.* Baran, *supra* note 454, at 6:

> The safeguards built into the present generation of time-shared systems all suffer the defect of requiring the assumption of the complete integrity of too many persons connected with the computer installation. Can you think of any general-purpose, time-shared computer systems that are presently approved to handle governmental classified data?

456. *Cf.* Ware, *Security and Privacy: Similarities and Differences*, 30 AFIPS CONFERENCE PROCEEDINGS 287 (1967), indicating that the problem of privacy protection is greater than military secrecy—the military has discreet categories of confidential, secret, and top secret, and a unitary organization accepting those categories. *See also* text accompanying notes 461-64 *infra*.

457. *See, e.g.*, UNIVAC Brief at J-22 to J-23:

> One solution is to shield the entire building which houses the central site with a special form of metalized paper barrier. In addition to this or by itself, depending on the degree of security required, the computer may be provided with a shielding of copper screening. Or, the more vital portions of the equipment may be protected by the use of circuit suppressors and selective filters. . . . They are capable of providing a high level of protection against electronic surveillance.

458. A. WESTIN, PRIVACY AND FREEDOM 324 (1967); Petersen & Turn, *System Implications of Information Privacy*, 30 AFIPS CONFERENCE PROCEEDINGS 291, 294-95 (1967).

459. *Senate Hearings on Computer Privacy* 78 (statement of the author); UNIVAC

encoding of data is necessary, the number of people with access to the cryptography principles must be limited and the code keys changed periodically.[460] Coding has a number of tangential advantages from the privacy perspective, including verifying the source of an inquiry or input into the data center and, in complex systems, allowing different types of information having variant levels of sensitivity to be processed accordingly.

At least one other approach is available to meet the problem of preserving the integrity of the data by controlling access to certain portions of the files. In many cases this can be accomplished by storing the data hierarchically on the basis of its level of content sensitivity. To a degree, this type of protection can be built into the hardware and software of the central processor. The working storage of a time-sharing system can be "partitioned" so that each user's "worker programs" have access only to a limited area of the computer's memory.[461] To support this procedure, the monitor or control program can be designed with a series of "privileged instructions" that provide the only possible means of altering the monitor program.[462] If any user's worker program attempts to alter the monitor program and invade a portion of the memory that is "off limits" to it, the monitor program can inform the system's supervisory personnel and shut down the offending terminal.[463] The effectiveness of this procedure can be tested by periodically checking a master copy of the monitor program against the one that is in operation in order to detect any alterations.[464] The monitor program's efficacy in protecting against unauthorized disclosure can be verified further by using a diagnostic program designed to make periodic attempts to deceive the monitor.[465] The monitor program also can be designed

---

Brief at J-22: "This kind of protection can be provided in several degrees ranging from quite simple, which an expert would not find difficult to decipher, to the almost unbreakable."

460. It may not be worth the effort or expense to develop completely break-proof codes. Sufficient scrambling or coding to make it uneconomic for an eavesdropper to attempt to intercept computer transmissions probably is enough. Alternatively, if information is arranged and stored on a hierarchical basis according to sensitivity or accessibility, the most efficient procedure may be to use codes of different degrees of complexity. The subject of computer cryptography is discussed in Baran, On Distributed Communications: IX Security, Secrecy, and Tamper-Free Considerations, Rand Corporation Memorandum RM-3765-PR (1964).

461. *See* IBM Brief at I-68.

462. *See generally* Graham, *Protection in an Information Processing Utility*, 11 COMMUNICATIONS OF THE ACM 365 (1968).

463. UNIVAC Brief at J-28.

464. IBM Brief at I-69 to I-70.

465. UNIVAC Brief at J-27; IBM Brief at I-70.

to clear the working memory of the computer after each user has finished running his program and thereby eliminate the risk that any residual data will be left accessible to a subsequent user.[466]

Another important security function that a privacy-oriented monitor program must perform is the identification of all users and terminals attempting to gain access to the files. One workable method of identifying terminals is a "call-back" system, which requires a user at a remote console to key in a terminal identification code as a precondition to entering any of the files. The computer then shuts down the terminal, checks its files to see if the code number is correct,[467] and reopens the terminal if everything is in order.[468] Presumably this function could be performed automatically by building a device into the terminal that would emit a unique identifying signal as a preface to each communication.

Call-back systems have their limitations, however. A security system based upon the identification of terminals determines only whether or not the terminal is an authorized member of the system; it provides no assurance that the person at the terminal's console has a right to be there. Nor does a call-back system necessarily incorporate guidance as to what portion of the files that particular terminal should be given access. There is no doubt that a greater degree of security is achieved by a system that decides whether to grant or deny access on the basis of user, rather than terminal, identification. Unfortunately, the problems of constructing an effective system of this type are quite extensive.

Magnetically coded identification cards, even those designed to receive new invisible magnetic code numbers after each transmission,[469] can be lost, stolen, or transferred, as can a code number that is assigned to each user. These schemes not only are vulnerable to the risk that people will enter the system who have no authorization whatsoever, but they also can be compromised by the exchange of cards and numbers by authorized personnel when the access keys open up different portions of the data store or allow different users to reach different information nodes on a network. "Fail-safe" systems, which require several users to insert their keys in a terminal before certain files will be made available,[470] will provide greater secu-

466. IBM Brief at I-68 to I-69.
467. IBM Brief at I-65.
468. UNIVAC Brief at J-23 to J-24.
469. *See* Kramer & Livingston, *supra* note 455, at 144.
470. IBM Brief at I-64 to I-65:

> One presently available terminal (used in the banking industry) has three locks and keys. Two keys are used to enable tellers to unlock the terminal to gain access to the system for routine transactions. A third key is available only to man-

rity than single keys or cards by making it necessary for the snooper to subvert a larger group of persons in order to gain access. Another possibility is closed-circuit television between the terminal and the central processor permitting visual identification of the user,[471] but this would be a relatively costly and cumbersome procedure. In the long run, the most promising method of assuring accurate user identification may be automatic scanning of fingerprints or voiceprints; however, this is not technically feasible at the present time.[472] Perfection of this technique—perhaps coupled with an "answer-back" system that requires the user to respond to a request to input some additional unpredictable identifying data in order to preclude the use of a record of another user's identifying input[473]—would provide a high degree of security.

Whatever technical safeguards are deemed appropriate for particular computer systems, they undoubtedly will be most efficient and economical if they are incorporated into the original design of the hardware and software than if they are added subsequently.[474] In many cases, however, this is not being done currently, and it probably will not be done in the near future unless computer manufacturers and users begin to think systematically about problems of privacy. From a pragmatic perspective, it must be recognized that the more elaborate technical safeguards are likely to be relatively expensive to design and implement. One expert has predicted that security routines in time-sharing systems will occupy up to twenty per cent of the computer's memory capacity.[475] It therefore is unrealistic to expect profit-conscious businessmen or government administrators laboring under limited budgets to undertake expensive measures to protect privacy out of self-interest or benevolence. "Encouragement" through industry or official regulation may well be necessary.

---

agerial personnel. It permits the terminal to be used for opening, closing, auditing and summary transactions.

See also A. WESTIN, *supra* note 458, at 324.

471. IBM Brief at I-66.

472. UNIVAC Brief at J-25. *See also Computer Encoding of Fingerprints*, 93 SCIENCE NEWS 494 (1968). Community Systems Foundation is now testing a system that identifies users by a combination of physical characteristics and responses to questions asked the user. Further details are unavailable at this time.

473. *Cf. Senate Hearings on Computer Privacy* 78 n. 9 (statement of the author).

474. Computer expert Paul Baran concludes in *House Hearings on the Computer and Invasion of Privacy* 126 that "[t]he best time for applying fundamental safeguards is during initial system design. 'Patchups' at a later date may be relatively less effective compared to a good initial design that includes an awareness of the existence and importance of the problem."

475. Behrens, *Computers and Security*, 91 SCIENCE NEWS 532 (1967).

B. *Administrative Methods of Improving Security*

Technical safeguards for a computer system must be supported by a series of workable procedural controls designed to prevent careless or intrusive personnel from bypassing the security devices. These administrative rules must be comprehensible to all personnel who have access to the system and they should be accompanied by realistic penalties. In short, administrative procedures are a necessary part of an over-all "protective philosophy," but they will prove effective only if they are understood by all people connected with the system;[476] the willingness to abide by these regulations should be a basic attribute of personnel selected to work in the system. Only careful employment practices and gentle indoctrination can develop a cadre of systems operators who are sensitive to privacy considerations.

A log listing every user of the data, the files he examined, and all significant events that take place within the central processor should be maintained.[477] This log can be kept either by the operator of the central processer, by the machine itself, or by both.[478] It should be audited periodically by security experts for signs of abuse and in order to evaluate the effectiveness of the entire protection program. Individuals whose personal data is stored in a system should have access to the audit from time to time. They should also, as has been suggested, have access to the data itself, so that they can retain a modicum of control over both the dissemination and the accuracy of the stored information relating to them.[479] The cost of granting access for these purposes is certain to be substantial, particularly if the system is obliged to mail printouts to everyone on whom it maintains data,[480] although in the case of information maintained by the Government, the printout could be included in one of the periodic communications sent to most citizens. To the cost of giving individuals notice of the contents of their files must be added the expense of handling the flow of petty squabbles that might result from the procedure. Moreover, some loss in the value of certain types of data might result from its disclosure to the subject. Nonetheless, the right of an individual to be protected against governmental or private dissemination of erroneous or sensitive information about him

476. *See* Peters, *Security Considerations in a Multi-Programmed Computer System*, 30 AFIPS CONFERENCE PROCEEDINGS 283, 284 (1967).

477. *Senate Hearings on Computer Privacy* 78 (statement of the author); A. WESTIN, PRIVACY AND FREEDOM 324 (1967); Peters, *supra* note 476, at 284.

478. Peters, *supra* note 476, at 284.

479. *Senate Hearings on Computer Privacy* 77 (statement of the author); Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 219 (1968).

480. *Senate Hearings on Computer Privacy* 77 (statement of the author).

is so important that some price may have to be paid to preserve it. Perhaps an appropriate compromise would be to inform individuals when their files are first opened, and then to designate particular times and places for them to examine their records, either in person or through remote terminals, and to lodge any protest they might have concerning inaccuracies or improper disseminations.[481] Inconvenience and expense undoubtedly would prevent some people from taking advantage of this opportunity, but a relatively small number of successful challenges at least would serve to point out procedural and technical defects in the system's security and to sensitize its personnel to the privacy question.

Computer experts seem to disagree on another important administrative aspect of security: the question of whether or not the personnel operating the central processor should have any detailed knowledge about the design of the monitor program. One school of thought argues that knowledge of the monitor program's intricacies should be limited to as small a group as possible. Under this scheme, the operators of the central processor never are told how the monitor program works, and the program's designers are prevented from gaining access to the monitor unless there is a need to make changes or improvements in it.[482] The detractors of this approach believe that it is desirable to have someone continuously on duty at the central processor who is thoroughly familiar with the security procedures and the principal weaknesses of the system.[483] The suitability of either of these methods in a particular situation probably depends upon practical considerations such as the relative costs, the demonstrated dependability and faithfulness of the operating personnel, the sensitivity of the information in the system, and the degree to which the monitor program contains novel features that can best be protected by secrecy.

Any system that contains sensitive data or data that for any reason is attractive to the snooping fraternity should be put under the aegis of personnel who are segregated from those charged with the daily operation of the machines. This group should be trained in the philosophy and techniques of security, and occasionally should act as "devil's advocates" by trying to circumvent the existing precautions in order to assess the system's security.[484] This type of neutral force approach seems especially appropriate in the context

481. *Id.*
482. UNIVAC Brief at J-30 to J-31.
483. Peters, *supra* note 476, at 284.
484. Allen, *Danger Ahead!—Safeguard Your Computer*, 46 HARV. BUS. REV., Nov.-Dec. 1968, at 97, 101; Peters, *supra* note 476, at 285.

of any type of integrated information system in order to protect against hyperactivity on the part of some of the participants.

C. *Controls on Input, Output, and Storage*

Perhaps the most critical set of regulations governing the operation of data centers are those prescribing the information that may be included in or obtained from the system and the types of manipulations that may be performed on the data store. No technological or administrative security measures, however extensive they may be, can assure the complete integrity and privacy of the information contained in a given system. A computer's data store essentially is a file, and whatever has been placed in it can be extracted or altered.[485] Thus, if informational privacy is to be protected, it is crucial to screen data initially to prevent some of it from being placed in the system.

Extremely sensitive personal information—for example, records of mental illness, or inherently "soft" data, such as psychological test results—normally should be excluded from large multiaccess systems,[486] even if the files customarily are stored in a secure area removed from the central processor. Unless there is some definable and compelling reason to include this type of information in a multiaccess system, every effort should be taken to keep it out of the information flow. When highly sensitive or potentially damaging information must be preserved, it should be subjected, as suggested earlier,[487] to special storage and access procedures. In the case of any information of a sensitive character, each individual data subject should be told at the collection stage what uses are to be made of the data and what the extent and character of the group having access to it will be.

Furthermore, all personal information that is put into a large computer system should have to meet rigid standards of accuracy

485. *See Senate Hearings on Computer Privacy* 119 (testimony of Dr. Emanuel R. Piore, Vice President of International Business Machines Corp.); *House Hearings on the Computer and Invasion of Privacy* 128 (testimony of Paul Baran of the RAND Corporation).

486. *See generally* Douglas, *The Computerized Man*, 33 VITAL SPEECHES 700 (1967). At least one bill has been proposed to Congress that would classify certain kinds of information as too sensitive to be collected by government agencies. S. 1035, 90th Cong., 1st Sess. (1967), would make it unlawful for federal administrative agencies to "require or request" from employees information concerning their race or national origin, participation in political organizations, religious or sexual beliefs and practices, and psychological test results. The bill does, however, provide numerous exceptions to these general prohibitions.

487. *See* pt. VII. A. *supra*.

and objectivity.[488] Hearsay and ex parte evaluations, especially when prepared by someone whose position ordinarily does not require preparation of personal reports, should be screened out or carry a special warning when they are retrieved. The scope of present efforts to standardize computer languages and data-collecting methods, which presently are intended to facilitate the movement of data among different systems, should be broadened to develop practices that would help alleviate the risks of misinterpretation inherent in transfers of personal data.[489] Similarly, whenever possible, individuals should be given the right to supplement or explain personal information that is likely to give rise to erroneous or damaging inferences.[490]

A significant percentage of personal information becomes more sensitive as it grows older and is forgotten by the general public; other data atrophies and becomes less important with the passage of time.[491] For example, the record of an isolated past arrest may be extremely damaging if it is dredged up after the subject has made a fresh start, whereas many types of financial data pose less of a threat the more ancient they become. In short, the desirability of preserving different types of recorded personal information should be reevaluated continuously in light of privacy considerations. Computerized information must not be allowed to petrify. Data that is shown to be inaccurate, archaic, or of little probative value should be expunged, reclassified, or its age brought to the attention of users. Computer systems should establish a formal procedure for periodically determining when data is outmoded or should be removed from the file for any of a number of other reasons.

Since it is relatively simple to purge stale data from a computer system,[492] regulations concerning the storage life of various types of

---

488. *See Senate Hearings on Computer Privacy* 77 (statement of the author); Sawyer & Schechter, *Computers, Privacy and the National Data Center: The Responsibility of Social Scientists*, AMERICAN PSYCHOLOGIST, Nov. 1968, at 810, 816.

489. *Cf.* Sawyer & Schechter, *supra* note 488, at 813; Karst, *"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342, 361 (1966).

490. *See* note 565 *infra* and accompanying text. *See also* text accompanying notes 242-44 *supra*.

491. *See, e.g., House Hearings on the Computer and Invasion of Privacy* 278:

> [An official] of the Securities and Exchange Commission expressed the view that corporate concern dealt mainly with current affairs. It was his feeling that, after a period of 5 or 10 years, back data could be exposed to public view without serious objection by respondents. There would be difficulty perhaps in applying such a rule retroactively but a notice to this effect on future collections of data might serve to make the problem less troublesome in the years ahead.

492. *See, e.g., House Hearings on Commercial Credit Bureaus* 89 (testimony of H. C. Jordan, President, Credit Data Company); *cf.* note 70 *supra*.

information should be easier to implement than they would be in a manual filing system. Programming techniques also should be able to prevent the output of data that is damaging because it is incomplete or has not been brought up to date. An arrest record, for example, always should be accompanied by data describing the disposition of the case, whether the party requesting the data asks for it or not.

Other procedures for protecting anonymity can aid system designers in preserving the supposed distinction between statistical data centers and intelligence systems. In some cases, data can be put into the system in small aggregates rather than individualized units; thus, no single person's data could be traced with certainty.[493] When it is essential to identify an individual for purposes of updating the data, some protection can be secured by assigning each respondent an arbitrary identifying number. The data then can be divided into a "substantive deck" for normal statistical use, which would contain the data along with the arbitrary numbers, and an "identification deck," which is needed to link the individual to his code number in order to make a new entry in his data.[494] Modern sampling techniques also make it possible to reach statistically valid results without analyzing the data on every available respondent unit. Thus, it should be possible to deter snoopers by using a random sample selected to make it unlikely that a successful intrusion will yield a dossier on a particular person.[495] This procedure may not always be feasible. In multipurpose statistical centers such as the proposed National Data Center, the objective is to provide one body of data that can be used for a wide variety of analytical projects. This means that the Center's underlying "sample" would have to be large enough to contain data on the different variables needed by numerous researchers pursuing various proj-

493. *Senate Hearings on Computer Privacy* 44 (statement of Charles J. Zwick, Assistant Director of the Bureau of the Budget).

494. *Senate Hearings on Computer Privacy pt. 2,* at 310:

> [W]hile the identification of individuals is essential at the time the information is being incorporated into the [file], once it has been incorporated, the identification becomes irrelevant. It is therefore possible to split the file into two parts: (1) an identification deck which contains only such identifying information as name, date of birth, social security number, and address, together with the identification number; and (2) a substantive deck which contains only the identification number and the accumulated substantive information about the individual . . . . Each deck is kept in locked files.

See also Pemberton, *On the Dangers, Legal Aspects, and Remedies,* in *Symposium—Computers, Data Banks, and Individual Privacy,* 53 MINN. L. REV. 211, 224 (1968).

495. *Senate Hearings on Computer Privacy* 44 (statement of Charles J. Zwick, Assistant Director of the Bureau of the Budget); *Hearings on Government Statistical Programs* 10; Note, *Privacy and Efficient Government: Proposals for a National Data Center,* 82 HARV. L. REV. 400, 413 (1968).

ects.[496] When extensive samples or entire populations are required for a statistical data center, perhaps the most effective protection is an instruction in the control program that allows the computer to output data only in aggregates that contain a sufficient number of individual respondents to make identification of individuals difficult.[497]

D. *Managing the Information Managers*

Effective technical and procedural safeguards, combined with input-output controls, all are critical prerequisites to maintaining the privacy and factual reliability of computerized information. But they are not sufficient by themselves. Even the most sophisticated set of safeguards can be undermined by the people who gain access to the system in one fashion or another.[498] The reports of college students at MIT and elsewhere defeating the monitor protections in time-sharing projects emphasize the reality of this threat.[499]

It would be a mistake to believe that the risks to privacy created by computerization lie exclusively in the misuse of the system by malicious or profit-seeking interlopers. Those who live on intimate terms with the data bases and the technology may prove to be a more dangerous group, even though they may have no interest

---

496. *Cf.* Note, *supra* note 495, at 413-14:

> To facilitate comparative analysis of particular variables, the samples tested for the variables would have to be identical. Where the samples are not identical, correlations of the variables are possible only on a global basis—that is, by finding a third factor which correlates with each of two factors for which different samples have been tested, an analyst can make an indirect correlation between two factors in which he is interested. However, global comparisons constitute the very type of imprecise and unreliable analysis which the data center is intended to obviate.

497. *See, e.g.*, Lozowick, Steiner, & Miller, *Law and Quantitative Multivariate Analysis: An Encounter*, 66 MICH. L. REV. 1641, 1650 n.13 (1968); *cf. House Hearings on the Computer and Invasion of Privacy* 94:

> You can teach the machine to distinguish appropriate inquiries—statistical questions—from inappropriate inquiries—intelligence questions or individual data. . . . You can teach the machine to identify "trick" inquiries—either accidental or purposeful. That is, you can teach the machine to say, "This is a statistical inquiry but it is framed in such a way that the population or group you have defined contains only one individual or less than some specified number of individuals."

498. *See, e.g., Senate Hearings on Computer Privacy* 119 (testimony of Dr. Emanuel R. Piore, Vice President of International Business Machines Corporation):

> Because these [time-sharing] systems permitted many people to use a central computer from their remote locations . . . it has become necessary to exercise control over what a user can do through his terminal.
>
> This control resides, above all, with the men in the room with the central computer—the men who alone can select the operating system, put it into the machine, and start it working.
>
> . . . .
>
> The information stored in a computer is basically a file. Whoever organizes a file can recover anything that he wishes from it.

499. *See* note 75 *supra* and accompanying text.

in the informational content of the material they handle. Thus, the technicians who design and operate computer systems cannot be treated as a Brahmin caste. They already perform many disparate roles, and in the future they are likely to assume managerial functions that range far beyond their technical expertise. In addition to the mundane tasks of collating and disseminating data and overseeing machine operations, programmers and system operators undoubtedly will be called upon to take part in the information analysis and decision-making processes.[500] In many instances this pattern will emerge because the volume and variousness of the data will be too great, the methods of storing and manipulating the information too complex, and the technical language too arcane to enable scientifically naïve executives and public officials to maintain effective control over the structure and activities of their systems. As a result, policy control over data centers may fall into the hands of "computerniks." There is a danger that these people will become so entranced with operating sophisticated machine systems and manipulating large masses of data that they will not be sufficiently sensitive to the question of privacy.[501] This threat will be particularly difficult to control because they are absolutely essential to the effective functioning of the information systems and they cannot be replaced at various critical points in the information-handling process.

Concern about the growing power of computer operators and programmers has led some commentators to suggest that it would be desirable to "professionalize" various jobs in the data-processing industry, so that those who deal with sensitive information would be subject to an enforceable code of professional ethics.[502] This pro-

500. *See, e.g.*, Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 270, 279-80 (1964):

> [G]iven his deeper understanding of how the data are being processed, what assumptions are made about relationships among the data, what constraints must be put on the data in order for the computer to use it [*sic*], it is entirely possible that the programmer may be called upon in difficult cases to enrich the executive's basis for decision making . . . .
>
> . . . The way he arranges the relationships in the information to be processed and the relative emphasis he gives to different items could result in distortions of the "history" of the person and, hence, in the implications of the data.

501. *See* R. BOGUSLAW, THE NEW UTOPIANS 97-98 (paper ed. 1965). *See also Senate Hearings on Computer Privacy* 75 (statement of the author).

502. *See, e.g.*, Karst, *supra* note 489, at 362-63. *See also Professional Conduct in Information Processing*, 11 COMMUNICATIONS OF THE ACM 135 (1968) ("guidelines" adopted by the Council of the Association for Computing Machinery on November 11, 1966):

> 1.1 An ACM member will have proper regard for the health, privacy, safety and general welfare of the public in the performance of his professional duties.
>
> . . . .
>
> 2.1 An ACM member will act in professional matters as a faithful agent or trustee for each employer or client and will not disclose private information belonging to any present or former employer or client without his consent.

posal has several beneficial features. At this comparatively embryonic stage of the technology, it is doubtful that legislation or even administrative regulation could provide a set of principles that would be adequate to govern the wide variety of situations in which computer personnel will be called upon to manipulate or analyze personal data.[503] The inculcation of a sensitivity or professional commitment to the values of personal privacy and the dignity of the individual may provide a far more effective long-term check on the custodians of personal information. Moreover, it may be that the basic philosophical question—what are the duties and responsibilities of those who handle personal information affecting their fellow man—is as much an ethical dilemma as it is a legal issue. If so, perhaps it is best left for regulation by the practitioners of the art in the first instance.[504]

Unfortunately, there seem to be equally good reasons why the professionalization of computer personnel is an unrealistic solution to the privacy problem, at least at the present time. Computer programming and operation, system design and analysis, and most of the other occupations relating to the new technology are very young and rapidly expanding[505] vocations that lack well-developed traditions. It is questionable whether this atmosphere is congenial to effective self-regulation or the adoption of a code of ethics that almost

---

503. *Cf.* PRIVACY AND BEHAVIORAL RESEARCH 7:

> Legislation to assure appropriate recognition of the rights of human subjects [in behavioral science experiments] is neither necessary nor desirable if scientists and sponsoring institutions fully discharge their responsibilities in accommodating to the claim of privacy. Because of its relative inflexibility, legislation cannot meet the challenge of the subtle and sensitive conflict of values under consideration, nor can it aid in the wise, individualized decisionmaking which is required to assure optimum protection of subjects together with the fullest effectiveness of research.

504. *Cf. id.* at 14:

> The values held by an individual or a society are, and must be, in competition since no single value can be absolute. . . . Thus the conflict between the claim of the individual to his privacy and the needs of society to become better aware of human characteristics is no rare or isolated phenomenon.
>
> In each instance of conflict, the decision must rest on the totality of all the relevant issues and the result will vary from one occasion to another, and from one setting to another depending on the context within which the issue arises. . . . No general rule can be formulated to apply in each situation . . . .

505. *See, e.g., Hearings on Data Processing Management* 149:

> [A National Science Foundation] survey found that 120,000 undergraduates and 29,000 graduate students received some computer training during 1964-65. In addition, approximately 4,000 undergraduates and 1,300 graduate majors in "computer science" were estimated to have been enrolled in 1964-65. By 1968-69, it is estimated these enrollments for these majors will have increased fourfold. An estimated 226 degree programs in computer science or related areas were being offered in the fall of 1966 and an additional 331 were reported planned by 1969.

See generally PRESIDENT'S SCIENCE ADVISORY COMMITTEE, COMPUTERS IN HIGHER EDUCATION (1967), reprinted in *Hearings on Data Processing Management* 255-337.

certainly would require circumscription of particular activities and the development of a well-defined set of socially oriented attitudes.

Unlike the physician or lawyer, the computer operator does not deal directly with the people whose life histories he processes. The data subject is not present to engage his sympathies and serve as a reminder that the operator's conduct has an important impact on human beings. To the contrary, in most cases the immediate object of his sense of professional obligation is to the system that employs him, and he often ascribes anthropomorphic qualities to that system. Thus, he may find it difficult to visualize himself as the protector of an amorphous agglomeration of individuals whose computerized files happen to fall within his jurisdiction, and whose actual existence may be evidenced only by a string of binary digits or a sequence of magnetic impulses. Again, this environment is not conducive to enlightened self-restraint.

Finally, it is possible that the emerging class of data managers is imbued with values that are fundamentally incompatible with a commitment to the preservation of individual privacy. According to this theory, computer designers and operators—as a subspecies of modern technological man—are devoted to a scientific quest for efficiency, even if it comes at the expense of humanistic values; individuals are viewed as little more than operating units that must be made to act predictably and function properly within a well-designed system.[506] This judgment undoubtedly is too harsh and ignores the many knowledgeable and socially concerned people who have helped give birth to the new technology and who are advancing its growth today. But it is plausible enough to caution those responsible for establishing and enforcing public policy that they must exercise continuing vigilance over the information managers rather than abdicate responsibility to them.

An alternative method of reducing the risks created by careless, insensitive, or dishonest personnel is to encourage those professions that are the beneficiaries of computerized data to develop ethical standards governing their own collection, use, and dissemination of personal information.[507] Obviously, this method has certain inherent

506. R. BOGUSLAW, *supra* note 501, at 97-98, 202-04.

507. *See* Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1205, 1218 (1966); PRIVACY AND BEHAVIORAL RESEARCH 28-29:

> The scientific associations in the behavioral sciences are custodians of and spokesmen for the values of their scientific disciplines. . . .
>
> It is obvious that the Federal Government cannot and should not prescribe a set of moral principles. Likewise, we cannot expect each man to develop de novo his own set of ethical principles without the guidance of those who have already experienced the ethical conflicts that are involved in behavioral research. It is

limitations. The computer is so flexible a device, and personal information is employed for so many purposes, that comprehensive user self-regulation seems unrealistic, which means that this approach probably could reach only a relatively small proportion of potential abuses. Moreover, as suggested earlier,[508] the most effective privacy protection scheme is one that minimizes the amount of potentially dangerous material that is collected and preserved; a regulatory scheme that focuses on the end use of the data by governmental or private systems might be a case of too little, too late. Uniformity also would be difficult to achieve because of the diffuseness of the user groups. One suggested list of users includes "doctors, lawyers, accountants, journalists, sociologists, political scientists, historians and anthropologists."[509] It seems doubtful that any two of these occupations would have similar views on how much or what kinds of protection an individual should have against misuse or widespread dissemination of intimate personal facts. The professions, at least those listed above, also are likely to be primarily concerned with statistical analyses, and therefore any scheme that regulates them might leave the bulk of the intelligence or surveillance uses that are most inimical to personal privacy unregulated. Nor will all of these professional groups have the resources, technological experience, or motivation to develop and enforce privacy-protecting codes on their own initiative. If professional self-regulation is to have any meaningful impact, it seems necessary to provide some measure of central coordination and an overarching apparatus for channeling the benefits of current research and thinking on privacy to all user groups.

Notwithstanding these difficulties, professional self-regulation and self-examination undoubtedly will play an important role in the over-all protection scheme. If handled properly, the very lack of traditions or calcified attitudes among the current generation of computer specialists and the inherent diversity of outlook among different user groups might prove to be important assets in preserving individual privacy. But to capitalize on these conditions, the development of professional codes of ethics must be approached as an innovative and experimental process. Furthermore, self-regulation must be viewed as a supplement to, and not a substitute for, policy determinations by other interested societal institutions as to appropriate minimum levels of privacy protection.

---

thus logical to expect that these professional associations . . . will accept the responsibility for establishing ethical principles and guidelines for conduct of research as one of their major purposes.

508. *See* pt. VII.C. *supra.*

509. Westin, *supra* note 507, at 1218.

VIII. The Search for a Legal Framework

Although the threat to personal privacy presented by the new information transfer technologies is substantial and imminent, the preceding section demonstrates that a number of workable technical and procedural safeguards are available and undoubtedly more can be developed if the appropriate private and governmental groups are given sufficient impetus to make the needed adjustments in practice. The central problem is to determine how the legal system can best insure that a proper balance is struck between the traditional libertarian ideals embodied in the concept of privacy and the immense social benefit that computer technology offers. This problem is of a type that has many antecedents. Striking a balance between democracy and technocracy has been a frequent chore in the past and the lawmakers should not shrink from the task.

But the challenge of developing a meaningful level of protection in a computerized age is a formidable one and the law's past record of dealing with emerging technologies is not entirely encouraging. Indeed, the legal system's reluctance to deal coherently and promptly with novel phenomena seems to have been greatest when innovation has occurred in the field of communications. In the past, the importance and vulnerability of first amendment freedoms were ample reason for treating the information media with caution. But the computer's potential as an engine of social change—and human control—indicates that a greater threat to freedom may lie in inaction or continued application of ancient or inapposite doctrine in the face of the growing power of information in contemporary life and the increasing concentration of control over it.

As discussed above,[510] the current patchwork of common-law remedies and statutory regulations is characterized by uncertain application, lack of predictability, frequent inconsistency, unawareness of the ramifications of the new communications media, and an almost total disregard for the individual's right to participate in information transactions that have a profound impact on his life. It is unequal to the task at hand. Even if the common-law privacy remedies were rehabilitated and the constitutional freedoms of association and belief were expanded, it would be unwise to rely exclusively on private actions for damages, restitution, or injunctive relief to protect a citizen from misuse of personal information. The difficulties and imprecision of converting a loss of privacy and related injuries to an individual's personality into monetary damages

510. *See* pts. V, VI *supra*.

make private remedies inadequate. Furthermore, is it even likely that an individual will discover that maligning or inaccurate information has been placed in his dossier or that an improper dissemination of confidential matter has cost him a government position, denied him a promotion, or impaired his commercial, personal, or professional relations with others?

The difficulty of finding an appropriate mode of relief is compounded by the protean character of the computer; it permeates both the public and private sectors and has ramifications that cut across the relevant traditional legal theories. Almost any doctrinal legal response is bound to seem Procrustean or anachronistic. Thus, although a number of ingenious modifications of the existing compartmentalized legal structure have been proposed, no single theory promises to be expansive enough to respond effectively to the computer's multifaceted threat to individual privacy.

A. *Property Theories of Privacy*

Perhaps the most facile approach to safeguarding privacy is the suggestion that control over personal information be considered a property right, vested in the subject of the data and eligible for the full range of constitutional and legal protections that attach to property.[511] Support for this theory can be drawn from the fact that personal data often is treated as a commodity,[512] as well as from

511. A. WESTIN, PRIVACY AND FREEDOM 324-25 (1967), concludes that "personal information, thought of as the right of decision over one's private personality, should be defined as a property right, with all the restraints on interference by public or private authorities and due process guarantees that our law of property has been so skillful in devising." Unfortunately, the author does not offer any enlightenment concerning what he means by "property right." A more metaphysical approach to the same result is offered in Shils, *Privacy and Power*, reprinted in *Senate Hearings on Computer Privacy* 231, 247:

> The "social space" around an individual, the recollection of his past, his conversation, his body and its image, all *belong* to him. . . . He possesses them and is entitled to possess them by virtue of the charisma which is inherent in his existance [*sic*] as an individual soul—as we say nowadays, in his individuality—and which is inherent in his membership in the civil community.

In contexts such as the sale of personal information by credit bureaus, however, it is not the subject of the data but a third party who is selling the data. Thus, recognition of a property right in the subject could not be justified on the theory that the law merely was acknowledging the realities of the marketplace. Moreover, property theory, like the defense of consent in privacy actions, is open to the objections that it is simply a conclusory label and places responsibility on the individual rather than on the organization that wants to use the data, and usually has the leverage to extract it. Credit bureaus, for example, would be no less able to "purchase" property rights than they are presently able to obtain "voluntary" consent to credit investigations. *See* text accompanying notes 248, 315 *supra*.

512. It is true that a few courts have recognized property rights in the names and likenesses of celebrities for advertising purposes, but that situation is much more clearly an arm's length transaction, and is almost wholly devoid of traditional privacy

analogies to recent decisions dealing with search and seizure[513] and the holdings of a few privacy cases.[514] The property theory is also the most direct method of resolving the problem of standing to sue and of eliminating the current ability to deal in the intimate details of a person's life history without his knowledge or consent and with little likelihood of legal liability.

The basic objection to granting a property right in personal information for these purposes is the irrelevancy of property concepts to the values that privacy doctrine seeks to safeguard. The protection of individual privacy is intended to preserve emotional and psychological tranquillity by remedying a damaging publication or dissemination, rather than to define the legal title to or control the exploitation of a commodity.[515] There also are practical reasons to oppose the property rationale. The development of property rights in personal information probably would take place under state law. Yet experience with state-created property rights in literary works and commercial values indicates that confusion, uneven protection, and difficult conflict-of-laws problems are certain to result if the

considerations. *See generally* Haelen Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir.), *cert. denied*, 346 U.S. 816 (1953); Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROB. 203 (1954). *But cf.* Miller v. Commissioner, 299 F.2d 706 (2d Cir. 1962), which demonstrates the range of potential absurdities that could result from treating personal information as property.

513. *See* notes 331-32 *supra* and accompanying text. *But cf.* Alderman v. United States, 37 U.S.L.W. 4189, 4201 (March 10, 1969) (Justice Harlan, concurring and dissenting): "[T]he right to conversational privacy is a personal right, not a property right."

514. *See, e.g.*, Zimmermann v. Wilson, 81 F.2d 847, 848 (3d Cir. 1936), in which an injunction was granted preventing revenue agents from examining bank accounts. The court rejected a contention that the bankers' acquiescence in the search precluded the taxpayers from seeking relief, stating:

> It is Zimmermann and his wife, and not their bankers and brokers, who are the real and aggrieved parties before us. To say that their bank accounts, withdrawals, their loans and collateral deposits, are the property of their bankers and brokers, and the taxpayers have no right or standing to prevent an unreasonable search thereof, is to lose sight of substance and rest on shadow. . . . The bankers and brokers have no interest in contesting the search . . . but, when the notice to produce is served on them, coupled as it is with the assertion that noncompliance with the order will subject [them to criminal penalties], prudence and regard for the banker's own alleged liability . . . all unite to constrain him . . . [to] give the government a searching power of the defendants' affairs which it cannot legally assert against the taxpayers themselves.

See also Brex v. Smith, 146 A. 34, 36 (N.J. Ch. 1929): "There is an implied obligation . . . on the bank, to keep [records of deposits and withdrawals] from scrutiny until compelled by a court of competent jurisdiction to do otherwise. The information contained in the records is certainly a property right." *But cf.* note 525 *infra*.

515. *Cf.* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 200-01 (1890): "[W]here the value of the production is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property, in the common acceptation of that term."

recognition of property rights in a transitory intangible such as personal information is left to the states.[516] Especially in the context of computer transmissions on multistate media, national uniformity is an extremely desirable—and may be an imperative—goal. Along the same lines, it is difficult to perceive how a common-law property theory would solve some of the problems raised by federal data centers. It would be ironic, indeed, if the law governing computer systems unwittingly followed the unsatisfactory pattern that the law of literary property is now struggling to escape.[517] Finally, creation of property rights in personal information might prove to be too inflexible a method of regulating the development of important phases of a technology that still is in its infancy and it might tend to abort attempts to pursue other avenues of legal control. Certainly the creation of a property right in information does not obviate the need to impose technological and procedural restraints on information handlers of the type previously described.[518]

The fact that a property theory of personal information would involve the recognition of rights in an inexhaustible commodity suggests that the enigmatic tort theory of misappropriation may be somewhat more adaptable to the problems of computerized data-processing than a conventional property right would be.[519] The leading case of *International News Service v. Associated Press*,[520] which held the defendant liable for the pirating of wire service news reports prepared by a rival company, indicates that misappropriation is concerned primarily with the relationship of those who are competitors. The Supreme Court concluded that a right existed be-

---

516. *See, e.g.*, Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481, 484-85, 493-95 (3d Cir.), *cert. denied*, 351 U.S. 926 (1956); Ludwig, *"Peace of Mind" in 48 Pieces vs. Uniform Right of Privacy*, 32 MINN. L. REV. 734, 759-62 (1948); Comment, *Copyright Pre-emption and Character Values: The Paladin Case as an Extension of Sears and Compco*, 66 MICH. L. REV. 1018, 1029-31 (1968).

517. *See, e.g.*, S. 543, 91st Cong., 1st Sess. § 301(a) (1969): "On and after January 1, 1971, all rights in the nature of copyright . . . are governed exclusively by this title. Thereafter, no person is entitled to copyright, literary property rights, or any equivalent legal or equitable right under the common law or statutes of any State."

518. *See* pts. VII.A.-C. *supra*.

519. *Developments in the Law—Competitive Torts*, 77 HARV. L. REV. 888, 932 (1964):

> Misappropriation consists not in taking the physical object but in copying or drawing upon the conception or underlying intangible value for the use of the appropriator.
>
> In contrast to tangible property, the significant character of intangibles is their inexhaustibility: any number of persons may exploit or enjoy the intangible at one time . . . . Yet, though the appropriated intangible is not lost to the originator, its market value—largely dependent upon the intangible's scarcity—is lost, or at least diminished.

520. 248 U.S. 215 (1918).

tween the parties, which it described as a "*quasi*-property"[521] interest in obtaining a just return on capital and resources invested in obtaining the news reports.

Misappropriation is an appealing theory because personal data can be viewed as the individual's "sweat of the brow," and arguably whatever value it has must be attributed to the subject's "capital and resources." It also recognizes that relations between particular people can give rise to different rights and liabilities in items of economic value. If that is true of competitors, as was the case in *INS*, there is no reason why it cannot also be true of information subjects on the one hand and information disseminators and users on the other. Moreover, misappropriation has sufficient doctrinal vagueness to accommodate a variety of different policy interests and factual situations.[522] But, as in the case of traditional property theory, misappropriation has been used primarily to vindicate economic rather than emotional or personal values, and, as a creature of state law, it is subject to all of the confusion and inequality of application inherent in using an ad hoc approach to a very complex problem.

B. *Information Trusts and Privacy*

A more innovative legal approach than the recognition of a property right in information calls for the adaptation of a venerable legal device, the trust, to provide the mechanism for protecting

---

521. 248 U.S. at 236. *See also* the dissenting opinion of Justice Brandeis, 248 U.S. at 250:

> An essential element of individual property is the legal right to exclude others from enjoying it. If the property is private, the right of exclusion may be absolute; if the property is affected with a public interest, the right of exclusion is qualified. . . . There are . . . many . . . cases in which courts interfere to prevent curtailment of plaintiff's enjoyment of incorporeal productions, and in which the right to relief is often called a property right, but is such only in a special sense. In those cases, the plaintiff has no absolute right to the protection of his production; he has merely the qualified right to be protected as against the defendant's acts, because of the special relation in which the latter stands or the wrongful method or means employed in acquiring the knowledge or the manner in which it is used.

522. *Cf. Developments in the Law—Competitive Torts*, 77 HARV. L. REV. 888, 946 (1964): "The process of deciding an individual misappropriation case is likely to take place on several levels. The merits of a claim rest chiefly on considerations of incentive, social cost, alternative sources of protection, and the interests of others involved in the exploitation of the intangible."

The continued viability of the misappropriation tort is open to serious question in light of the Supreme Court's decisions in Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225 (1964) and Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234 (1964). *Compare* Pottstown Daily News Publishing Co. v. Pottstown Broadcasting Co., 247 F. Supp. 578 (E.D. Pa. 1965), *with* Columbia Broadcasting Sys. v. De Costa, 377 F.2d 315 (3d Cir.), *cert. denied*, 389 U.S. 1007 (1967). *See also* Comment, *Copyright Pre-emption and Character Values: The Paladin Case As an Extension of Sears and Compco*, 66 MICH. L. REV. 1018, 1027-29 (1968).

privacy from the vicissitudes of modern computer systems. This method currently is being tested by the United Planning Organization (UPO), a body formed to establish a "Social Data File" that integrates information on the administration of a number of welfare programs. The UPO has computerized large bodies of personal information secured from various agencies in the District of Columbia and created a trust, treating the data as a res. Control over the data is vested in a number of independent trustees, whose actions are regulated by an elaborate agreement governing permissible disclosures.[523]

The existence of a watchdog group, which does not have an active interest in exploiting the data in its custody and is circumscribed by clearly defined fiduciary duties, is appealing on its face. However, the trust device is not free from conceptual difficulties. It is a traditional principle that the subject matter of a trust must be a legally enforceable property interest,[524] and the assumption that the UPO is the "owner" of the personal data embodied on the magnetic tapes and punch cards that constitute the trust res seems to be a major feat of question-begging. Much of the data undoubtedly is public record information and incapable of being "owned" by anyone; the residue, if it is property at all, surely ought to belong to the individual to whom it pertains rather than to a group that has possession of one notational version of it. The anomaly is emphasized by the fact that the information in question could be

523. The trust instrument is summarized as follows in *Senate Hearings on Computer Privacy*, pt. 2, at 310-11:

> The property that the UPO now has, data that we have received from public agencies and collected through some of our own programs, will be transferred to three persons who will serve as trustees for the data. . . . They will own and collect the data which constitute the trust estate—subject to the conditions which are specified in the Agreement.
>
> . . . The conditions that would be imposed are several.
>
> First, the trustees must hold the data only for a specified purpose. The Agreement describes this purpose as evaluation of social problems and agency practices in the District of Columbia . . . . This is an aggregate, statistical purpose which does *not* include evaluation of any individual.
>
> Second, the trustees must place the data in the custody of the UPO for its use as long as UPO exists and does not disclaim its right under the Agreement to have custody of the data. . . .
>
> Third, the trustees can only place the data in the custody of UPO . . . if we use it for the purpose described . . . and do not use it to breach the confidentiality of information collected concerning named individuals. . . .
>
> Although the recipient would be permitted to delegate research projects to other persons or organizations, it would be prohibited from placing data identifying individuals by name in anyone else's custody . . . .
>
> Fourth, the trustees cannot transfer their control over the data. . . .
>
> Fifth, the trust is created in perpetuity and is irrevocable.

For the full text of the agreement, *see id.* at 312-17. *See generally* Brooks, *The Role of the Data Bank in UPO* (May 25, 1967) (mimeo).

524. *See, e.g.*, 1 G. G. Bogert & G. T. Bogert, The Law of Trusts and Trustees § 111, at 562-63 (2d ed. 1965); 1 A. Scott, The Law of Trusts §§ 74-77 (3d ed. 1967).

publicly revealed by the subjects of the data or obtained by third persons; thus, the same data theoretically can be "possessed" by everybody in the world without physically disturbing the trust res or impairing its primary value as a research tool.[525] Consequently, the effectiveness of the trust approach seems limited, as a practical matter, to the use of the data by the parties to the trust and provides little or no security to the individual against abuses by other users of the information. Nor does it reach the data-collection phase of the information process, although it is possible to extend the trust concept to every aspect of information-handling. But this is an extremely clumsy and circuitous way of establishing a regulatory scheme. A more philosophical objection to this approach stems from the question whether the law of trusts, which throughout its evolution has been designed primarily to safeguard the economic well-being of beneficiaries, is really the most suitable mechanism for creating and enforcing rules to protect the emotional tranquillity and community status of individuals.

The trust concept also is suspect as a protector of privacy because it is essentially an ex parte creation of the party controlling a particular data base, which means that the terms and conditions of the trust instrument are, within very broad limits, wholly a matter of the discretion or benevolence of the party executing it. The United Planning Organization's trust agreement illustrates this deficiency very clearly, since it creates no enforceable rights in the parties who are, at least in theory, its beneficiaries—the citizens whose personal information has been collected by the governmental agencies that furnished the data.[526] Apart from this problem, which could be ameliorated judicially, the trust approach has the potential of resulting in an even greater lack of uniformity of treatment

525. *Cf.* Pearson v. Dodd, No. 21,910, at 11-12 (D.C. Cir. Feb. 24, 1969), in which plaintiff asserted that photocopying of documents from his files and unauthorized dissemination of the copies invaded his property rights. The court rejected the property theory:

> The question here is not whether appellee had a right to keep his files from prying eyes, but whether the information taken from those files falls under the protection of the law of property, enforceable by a suit for conversion. In our view, it does not. . . . Insofar as we can tell, none of it amounts to literary property, to scientific invention, or to secret plans formulated by appellee for the conduct of commerce. Nor does it appear to be information held in any way for sale by appellee, analogous to the fresh news copy produced by a wire service.
>
> . . . .
>
> Because no conversion of the physical contents of appellee's files took place, . . . the District Court's ruling that appellants are guilty of conversion must be reversed.

526. The trust provision by which the United Planning Organization, the donor-recipient, reserves the power to seek judicial enforcement of the terms of the agreement is set out in *Senate Hearings on Computer Privacy*, pt. 2, at 315.

than the property or misappropriation theories. And, given the conceptual difficulty of applying trust theories to computerized personal information, it seems likely that any judicial scrutiny of a trustee's behavior might degenerate into a highly convoluted doctrinal analysis of trust law or a baroque construction of the language of the trust instrument.

On balance, therefore, the establishment of personal information trusts may be more suited to providing full employment for lawyers than to fashioning a workable balance between the competing interests in the flow of personal information. Far from being a panacea, it is little more than a legalistic, ad hoc attempt to finesse the highly complex problems that should be dealt with directly by information users. At the same time, the trust concept also obfuscates a number of the underlying policy issues. It is a useful expedient for providing a small measure of control over the manipulation of data by particular groups or data systems; in a sense, it is a first step toward creating a professional sensitivity to the value of personal privacy on the part of the information managers and UPO should be commended for developing it. But trust law is unlikely to be the seminal mechanism for solving the privacy problems of the computer age.

C. *Federal Privacy Legislation*

The computer's impact on traditional relationships between individuals and organizations, and the impending emergence of computer technology as a medium of communication with national dimensions, suggest that congressional action to protect privacy values may be both necessary and appropriate. By pre-empting inconsistent state laws and affording protection to individuals in contexts in which none presently exists, Congress could provide a uniform and comprehensive formula for the development of multistate computer systems and at the same time infuse a measure of coherence into the law of privacy. But the uncertain direction of the computer age and the lack of obvious and easy solutions have combined to make the desirability and effectiveness of congressional action still very much a matter of conjecture.

A legislative solution can take a number of different forms. The simplest approach, and certainly an effective method of protecting against misuse of personal information, is to enact statutes prohibiting governmental, and perhaps even nongovernmental, organizations from collecting designated classes of data or, at the least, prohibiting them from using or threatening formal or informal

sanctions to coerce disclosure of the data. An example of this type of legislation is the series of recent bills that would eliminate the existing criminal penalties for failure to answer many of the questions asked by the Census Bureau.[527] Although the scope of the current decennial census ranges far beyond the periodic "enumeration" contemplated by the Constitution,[528] Congress generally has passively acquiesced in administrative determinations of what information should be collected by the Government. To be sure the national government has the power to proliferate the census process as a necessary and proper adjunct to the effective planning of numerous federal programs. But the increasingly elephantine character of the census indicates that middle- and low-level bureaucrats —often in response to pressures exerted by large industrial lobbies or other government administrators[529]—in effect are expanding the contours and the potential application of the criminal sanctions imposed for noncompliance with a census request by determining what questions will be included in it.

As attractive as excision of the sanctions appears to be, other considerations counsel against hasty use of this legislative technique. Even a mild restriction such as removing the *in terrorem* effect of criminal penalties from the census process could have an adverse effect on the federal government's over-all statistical effort. If popular resentment against the spectrum of contemporary privacy invasions and the never-ending stream of governmental and private questionnaires focuses on the census, removing the formal sanctions arguably might precipitate a widespread failure to respond that could impair the statistical validity of surveys that are urgently needed for the analysis of fundamental social problems. The hypothetical character of this observation must be emphasized. Although there is a division of opinion as to whether the elimination of the criminal penalties would skew the results of the census to any ap-

527. *See* note 347 *supra*. Over 100 congressmen have endorsed bills removing these penalties. CONG. REC. H858 (daily ed., Feb. 6, 1969). In the ninetieth Congress, the Senate unanimously passed S. 4092, which was virtually identical to the present bills to eliminate the census sanctions.

528. *See* notes 341-44 *supra* and accompanying text.

529. *See* text accompanying notes 178-81 *supra*. *See also* 115 CONG. REC. H859 (daily ed., Feb. 6, 1969) (remarks of Congressman Betts):

> Large corporations are behind the extensive household utility items such as [census] questions asking if a person has a television, clothes washing machine, dryer, home food freezer, and so forth, and Government officials who have an insatiable appetite to extract more and more facts about the American citizenry have prodded inclusion of dozens of income, marital, housing, and employment subjects. The cozy relationship between the Census Bureau and Federal statistical users has gone beyond the semblance of public service. I believe this is an unwholesome alliance which causes improper expansion of the collection of personal data under threat of fine or imprisonment.

preciable degree,[530] it seems unlikely that a sizeable portion of the population would refuse to honor the census request. For some people the process of responding to interrogatories of this type has taken on a Pavlovian character and for others it simply is a matter of good citizenship. There also seems to be little doubt that more refined sampling techniques are available that would cure any problem that might arise.[531] In addition, elimination of the sanctions would not ameliorate the coercive "follow-up" practices of the Government or the subtle forms of pressure that are at work when a citizen is asked to furnish information to his Government. A veteran receiving a pension is likely to complete a Defense Department questionnaire whether or not his obligation to do so can be enforced by fine or imprisonment.[532] But whatever the intrinsic merits of eliminating the census sanctions, prohibitions on coercive data collection can remedy only some of the more blatant affronts to individual privacy. Most of the dangers of the computer age are far more subtle.

The task of developing legislative safeguards to maintain the privacy of data is more difficult in cases in which the information may be used for varied purposes or must be made available to certain agencies or groups but withheld from any wider circulation than it is when all dissemination can be proscribed. Part of the problem stems from the chameleon-like character of many types of data. As congressional investigations of the proposed National Data Center revealed, the "sensitivity" of information—its potential ability to harm the individual if inaccurate or if improperly disseminated—depends in large measure upon the context in which it was first given, and the context in which it is later used.[533] It will be a rare information system in which all of the data has a uniform level of sensitivity.

As indicated earlier,[534] access regulations, personnel controls, and machine safeguards all are available to develop privacy-protecting systems that can discriminate among different users and differentiate data on the basis of sensitivity. But these techniques

---

530. This point was discussed by several of the witnesses before the Senate Subcommittee on Constitutional Rights during its hearings on S. 1791 in April 1969. *See generally Hearings Before Subcomm. on Census and Statistics of the House Comm. on Post Office and Civil Service*, 90th Cong., 1st Sess. (1967); 114 CONG. REC. H4053-75 (daily ed., May 21, 1968).

531. *Id. See also* 113 CONG. REC. at H13,429-31 (daily ed., Oct. 16, 1967) (remarks by Congressman Betts).

532. *See* text accompanying notes 308-14 *supra*.

533. *See* text accompanying notes 88-100 *supra*.

534. *See* pt. VII *supra*.

are interdependent in the sense that a weakness in one security system will undercut the other protective schemes. Thus, legislation dealing with one aspect of security or one level of sensitivity will not effectively preserve privacy. It seems obvious that a potpourri of legislative controls will be needed; some would establish varying degrees of confidentiality for different kinds of data and others would prescribe the technical and procedural safeguards to be employed by the system, with the safeguards organized hierarchically in terms of different levels of data sensitivity. This type of refined structuring presumably would be predicated on an evaluation of how much "privacy" the data in a given system deserves and a balancing of the damage that can be caused by misuse of the information against the cost and loss of efficiency that would result from implementing various safeguards. This assessment takes on an overwhelmingly complex demeanor if it has to be made in the context of a highly sophisticated network or system that involves data from numerous sources and is used by discrete people, groups, agencies, and organizations for highly disparate purposes.

Since the myriad facets of the privacy problem would be difficult to resolve legislatively even if only a single computer system containing personal information required regulation, it seems unlikely that a single statutory scheme can deal effectively with all computer systems. The limited present experience with data centers and networks and the enormously complex problems of distinguishing between governmental and private systems and determining the extent to which the latter should be federally regulated make the obstacles to drafting comprehensive national legislation virtually insurmountable at the present.

A less ambitious course may be appropriate, however. Perhaps it is not necessary for federal legislation to grapple with the minutiae of the specific methods of protection to be followed by every conceivable computer system. It has been asserted that the Freedom of Information Act is effecting a substantial relaxation of government secrecy even though it hardly could be called a model of clarity or specificity.[535] Since protection of informational privacy always will depend in some measure upon the discretion of the data managers, it may be sufficient to adopt an approach similar to that of the Information Act by providing a set of general legislative guidelines and a philosophical orientation that will encourage the enlightened exercise of that discretion.

But there are several reasons why the Freedom of Information Act is not entirely apposite as a model for federal privacy legislation.

535. *See* text accompanying notes 394-419 *supra*.

To be effective, an informational privacy statute should be as extensive as the applications of computer technology, embracing, at least to some degree, both public and private data centers and taking cognizance of the interactions of these systems. The scope of the Freedom of Information Act, however, is much more limited in the sense that it deals with the disclosure obligations of the individual federal agencies—bodies that at least have similarities of structure and function, and share a basic commitment to the ideals of public service. Moreover, the Information Act attempts to avoid conflicts with other legislation by explicitly deferring to existing restrictions on disclosure.[536] Any attempt at effective privacy legislation should strive to bring some order to the existing welter of conflicting and often meaningless confidentiality statutes, which might necessitate supersession or modification of some aspects of other federal legislation, such as the Federal Reports Act, the Crime Control Act, and the Information Act itself. Finally, the Freedom of Information Act deals with familiar problems and was built upon a history of prior legislation and well-defined administrative practice. Computer technology is essentially a new medium of communication, and, in spite of the recent profusion of books and articles on the subject, very little really is known about its long-range impact on the fabric of our society.

In view of the manifold difficulties of drafting comprehensive privacy legislation, especially in the context of computerized information, it is not surprising that most of the bills that have been introduced in the ninetieth and ninety-first Congresses relating to the subject have had relatively narrow scopes.[537] As mentioned earlier, some of these proposals deal with the information-handling activities of particular agencies, such as the Census Bureau.[538] Other proposals involve attempts to protect certain groups that are vulnerable to privacy invasions; this is true of Senator Ervin's bill relating to government employees.[539] On both the federal and state levels, there has been a flurry of legislative activity in the credit bureau field.[540]

In one of the most ambitious efforts to date, Congressman Koch has introduced a bill which would amend the Freedom of Informa-

536. 5 U.S.C. § 552(b)(3) (Supp. III, 1965-1967).

537. *See, e.g.*, H.R. 7214, 91st Cong., 1st Sess. (1969); H.R. 889, 91st Cong., 1st Sess. (1969); H.R. 20, 91st Cong., 1st Sess. (1969); H.R. 15,627, 90th Cong., 2d Sess. (1968); S. 1035, 90th Cong., 1st Sess. (1967).

538. *See, e.g.*, H.R. 20, 91st Cong., 1st Sess. (1969).

539. S. 782, 91st Cong., 1st Sess. (1969). An earlier version appeared as S. 1035, 90th Cong., 1st Sess. (1967). *See also* S. REP. 534, 90th Cong., 1st Sess. (1967).

540. *See* note 244 *supra*. State legislation would be rendered superfluous by the enactment of the Proxmire Bill, S. 823, 91st Cong., 1st Sess. (1969). *See* notes 241-44 *supra*.

tion Act to require that all agencies maintaining files of personal information give notice to the individual if information concerning him has been procured from any source other than himself.[541] The bill also provides that the agency must open these files to the individual so that he can inspect and copy them.[542] The access provision could perform a valuable function in allowing the individual to detect potentially damaging errors in his files; however, it also subjects an individual to the possibility of coercion by those who want access to any governmental information on him and are in a position to insist upon his procuring a copy.[543] The agency also would be obliged to undertake certain precautions in the handling of the information and to refrain from disclosing personal data without obtaining permission from the individual. There is no doubt that the enactment and enforcement of this bill would have a substantial ameliorative effect on the present information-handling practices of a number of federal agencies; but it would accomplish little on the information-gathering side of the ledger. Realistically, the Koch bill has a difficult road to traverse and passage cannot be predicted with confidence.

Most recently, Senator Ervin has introduced a broadly worded proposal that takes a somewhat novel approach to the subject.[544] It would prohibit the executive agencies and their personnel from requiring any individual to divulge personal information unless the collection of that information could be based upon a constitutional provision and a specific act of Congress. When this is the case, disclosure would be mandatory. The bill also would limit federal data collection on a voluntary basis to those matters specifically authorized by an act of Congress. In this category of inquiries the bill

541. H.R. 7214, 91st Cong., 1st Sess. (1969).

542. *Id.* § 552(a)(5).

543. *Cf.* Annot., *Discovery and Inspection of Income Tax Returns in Actions Between Private Individuals*, 70 A.L.R.2d 240, 242-43, 246-47 (1960):

> By the great weight of authority, state as well as federal, a court in which a civil action is pending may require one party to produce a copy of a federal or state income tax return for inspection by an adverse party under the rules or statutes which deal with discovery procedures.
>
> . . . .
>
> State and federal tax authorities will ordinarily furnish a certified copy of an income tax return to the taxpayer or his agent. . . . And since it is within the power of the taxpayer to obtain a copy of his income tax returns from the government, the court may order him to do so, or to sign a form which in effect designates the attorney for the moving party as an agent to obtain a copy.
>
> . . . .
>
> The fact that the Internal Revenue Code protects the taxpayer against the disclosure of his federal income tax returns by public officials and employees does not give the taxpayer an absolute privilege, and does not prevent a court from ordering that he, rather than public officials or employees, shall produce copies of his returns for inspection and copying by his adversary.

544. S. 1791, 91st Cong., 1st Sess. (1969). Congressman Betts has introduced a comparable bill in the House. H.R. 10,566, 91st Cong., 1st Sess. (1969).

would require the collecting agency to inform the respondent group that disclosure is volitional. The Ervin bill has some faults. There are a few problems of language that might unduly limit or render uncertain its scope of application. Generally these stem from the absence of an adequate definition of either the character of the information or the nature of the data-gathering activities that would be covered by the bill. Moreover, reliance on the Constitution as a limitation on mandatory disclosures might be rendered nugatory by a broad application of the necessary and proper clause. Finally, requiring all voluntary surveys to be predicated on specific acts of Congress might tend to produce a rubber-stamp effect or undue congressional preoccupation with the details of agency surveys. A better approach might be to proscribe all forms of voluntary data-gathering unless the agency can satisfy a series of legislative guidelines or standards.[545] On the whole, however, the bill represents a highly desirable attempt both to limit federal data collection activities to those expressly authorized by Congress and to curtail the use of subtle forms of coercion against individuals.

Although each of the current legislative proposals can be criticized for its lack of scope and the failure of its proponents to investigate the broader implications of informational privacy, the present level of legislative activity is a healthy sign. Furthermore, the cumulative effect of these bills may be quite effective. In any event, beyond the possible integration of the various proposals described above, it simply is unrealistic to expect comprehensive legislation to be proposed at this relatively early date. There is insufficient experience with the computer-privacy phenomenon to permit rational and detailed legislative judgments to be made. Indeed, an attempt to achieve them at this time seems premature and might yield an unmalleable product that would prove to be obsolete shortly after its enactment. Furthermore, the somewhat uncertain future shape and application of the technology and the understandable desire on the part of Congress to refrain from interceding in the operation of nonfederal information systems until the need for doing so becomes clear, makes highly detailed statutory regulation in the immediate future unlikely.

---

545. The prerequisites to conducting a voluntary survey might include: (1) an administrative demonstration of a clear and significant need for the data; (2) a showing that the data has not been secured by other federally conducted surveys; (3) a demonstration that the data is not available through prior state, local, or private information-gathering efforts; (4) a finding that the sampling group is no larger than that necessary to obtain the requisite data base; and (5) an articulated administrative determination that the questions to be asked are not intrusive or violative of individual privacy.

D. *Federal Administrative Regulation*

The present lack of detailed knowledge about the computer's long-term impact indicates that perhaps the problem of how individual privacy should be protected against the excesses of this new medium is more amenable to administrative treatment than to legislative resolution; at least this may be the case for the foreseeable future. Administrative regulation is less immutable than a statute, thus providing sufficient flexibility to permit experimentation and shorter reaction time when new problems present themselves.

1. *The Locus of Regulatory Power*

Assuming the validity of this proposition, it is not immediately apparent where power to regulate should be centered and what form the regulation should take. It seems safe to postulate at the outset that regulatory power should not be entrusted to an agency that has operating responsibilities involving the use of personal information. The debate over the proposed National Data Center and revelations before congressional subcommittees[546] concerning the intrusive activities of the Post Office, the Internal Revenue Service, and the Immigration and Naturalization Service have made it abundantly clear that privacy values often get short shrift if fundamental policy decisions are made by an agency that has a vested interest in gathering and using data.[547] The fact that personnel in various agencies have systematically engaged in mail cover operations, electronic bugging, wiretapping, harassment, and other invasions of privacy demonstrates that governmental officials often become too oriented toward the objectives of their institutions or too vulnerable to pressures from other organizations to be entrusted with responsibility for preserving the privacy of others. Consequently, an administrative approach that completely abdicates regulatory control to each agency and bureau probably is unsatisfactory from a privacy-protection prospective and is likely to produce such tremendous variations in practice that there would be little gain over the existing unstructured situation.[548]

546. *See generally House Hearings on the Computer and Invasion of Privacy*; *Senate Hearings on Computer Privacy*; *Senate Hearings on Computer Privacy*, pt. 2.

547. *See generally Hearings on Constitutional and Administrative Problems of Enforcing Internal Revenue Statutes Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968); *Hearings on Invasion of Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 89th Cong., 1st Sess., pts. 1-3 (1965) (Government Agencies), pt. 4 (1965-1966), 89th Cong., 2d Sess., pt. 5 (1966), pt. 6 (1966) (Telephone Systems).

548. *See* text accompanying notes 164-84 *supra*. It is interesting to note that the Proxmire Bill to regulate credit bureaus, S. 823, 91st Cong., 1st Sess. (1969), proposes to

The question then becomes whether there is any single organization that should be given administrative responsibility for developing a privacy scheme for the federal agencies and perhaps for nonfederal information systems. The Census Bureau and the Bureau of the Budget immediately spring to mind. Even though it has an enviable security record,[549] the Census Bureau has become so indoctrinated with the information acquisition syndrome it is difficult to believe that it could overcome its present function and orientation and develop a balanced regulatory scheme for protecting privacy. As to the Bureau of the Budget, its supervision over federal reporting programs has proven ineffectual from a privacy perspective.[550] This is not surprising in view of the institutional bias that the Budget Bureau's duties create, but it does argue against giving the Bureau further responsibility for preserving privacy. It also is worth noting that both agencies are primarily federally oriented and might not be appropriate institutions to the extent that certain activities of nonfederal systems eventually will have to be brought under federal regulation.

A more promising candidate for receiving regulatory authority is the Federal Communications Commission, which already has recognized the importance of privacy by including the subject as one of the central concerns of its inquiry into computer communications technology.[551] A relatively minor extension of the FCC's statutory jurisdiction would enable it to deal with the full range of computer-privacy problems, including those raised by nonfederal systems.[552] Indeed, this might fruitfully be done as an adjunct to its

---

give the Federal Reserve Board extensive regulatory authority. *See* 115 CONG. REC. S1163-69 (daily ed., Jan. 31, 1969). *See also* notes 241-44 *supra*.

549. *See* Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 218-19 (1968).

550. *See* text accompanying notes 164-72 *supra*.

551. Federal Communications Commission Notice of Inquiry, Docket No. 16,979, reprinted in *Senate Hearings on Computer Privacy* 87.

552. The extent of the FCC's jurisdiction has proved to be a prime subject of controversy in its present inquiry into computer technology (*see* note 551 *supra*). *See, e.g.*, IBM Brief at I-6 to I-7:

> It has been suggested that message switching constitutes a fusion of data processing and communications making separation difficult or impossible. This suggestion results, we believe, from confusion created by the generality of the term "message switching." Message switching has been defined as the technique of receiving a message, storing it until the proper outgoing circuit and station are available, and then retransmitting it towards its destination. The fact that a particular activity constitutes message switching within this definition does not determine whether it should be regulated. It is the *purpose* of the particular message switching that is determinative. In general, message switching occurs in one of the following forms:
>
> (1) As an adjunct to a public transmission service. As such, it is subject to traditional common carrier regulation.
>
> (2) As an adjunct to a private data processing or private communications sys-

present investigation of the threat posed by systems that rely on the common carrier networks.

Entrusting the field of informational privacy to the FCC could prove to be a less than ideal solution, however. There is some possibility that the FCC would find itself torn by an ideological conflict of interest, inasmuch as its primary concern is the efficient exploitation of communications technology. In the context of regulating the telephone system, for example, economic considerations typically have predominated over efforts to insure the confidentiality of communications.[553] And it appears that a similar process is occurring in the FCC's present inquiry into data communications; in the responses filed by various organizations, privacy generally has received only minimal attention in comparison to the questions of whether or not regulation of computer systems is economically desirable.[554] But this may simply reflect the parochialism of the communications industries, rather than the Commission's inability to deal with the privacy problem once it directs its attention to that subject. Perhaps it does indicate that it is unwise to burden the FCC with primary responsibility for regulating a highly complex and multifaceted problem that will take it far outside its traditional bailiwick. Moreover, any attempt at comprehensive regulation would require the FCC to enter areas that would be completely new to it, such as single- and multi-level governmental information systems, computer-manufacturing, and software development, which might represent a potentially unhealthy expansion of its jurisdiction.

It is quite possible that none of the existing federal bureaus, agencies, or departments has enough background or is sufficiently independent—in the sense of not being obligated to various institutional "clients" or committed to values of efficiency or policy objectives that are inconsistent with privacy—to be an effective

tem operated by and for the user. Such private use—not involving service to others—should not be subjected to regulation.

(3) As an adjunct to the furnishing of a data processing service. Message switching that is an incidental part of a data processing service should not be subject to regulation.

553. *See generally Hearings on Invasions of Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 89th Cong., 2d Sess., pt. 5, at 2364-75, 2380-86, pt. 6 (1966). Part 5 of these hearings contains a diverting account, at 2356-58, of five college students who "broke" the telephone system so that they were able to make free long-distance calls for a period of six months and threaten the security of secret defense lines.

554. Semling, *The Computer-Communications Inquiry*, MODERN DATA SYSTEMS, July 1968, at 48-52: "While most respondents [to the FCC inquiry] expressed awareness of [the privacy] problem there was little interest in the need for the FCC to do something about the privacy question. Generally, it was considered an industry problem, both by the manufacturer and user."

guardian of individual privacy. If this is the case, the conclusion is inescapable: regulatory control must be lodged outside the existing administrative channels. As repugnant as it may sound in an era of expanding governmental involvements, it may be necessary to establish a completely independent agency, bureau, or office—perhaps preceded by a Study Commission on Informational Privacy—that can establish policy under broad legislative guidelines in order to insure the privacy of all citizens.[555] The organization might regulate the nature of the information that can be recorded and stored in various systems, enforce a congressional standard of care for insuring the accuracy of recorded information, and direct various types of data centers to employ the latest technological advances to protect themselves against breaches of security.

2. *Functional Aspects of Effective Administrative Control*

Whatever the most desirable locus and structure for administrative control over the privacy aspects of computer systems may be, the subject obviously involves numerous political implications and any proposal would be subjected to the vagaries of the legislative process. Consequently, any attempt to predict the precise contours of the regulatory scheme at this time would be a somewhat sterile exercise. However, there are several obvious attributes that any administrative body would have to possess in order to be an effective guardian of informational privacy.

A governmental organization that undertakes to regulate any significant aspect of a technology as dynamic and pervasive as the computer must be able to draw upon a wide range of expertise. At a minimum, then, the agency charged with this responsibility should be composed of people who are conversant with the scientific and technical disciplines, the business community, the social sciences,

555. Many of the commentators on the proposals to create a National Data Center stress the importance of locating control of the center outside of the existing regulatory framework. *See, e.g.*, Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 404 (1968):

> The proposed data center would be organized within the Executive Office of the President and would be under the control of the "Director of the Federal Statistical System." The Director would have two advisory councils: one to represent the interests of government users, the other to speak for the private users and the public-at-large. The councils would advise the Director on such matters as confidentiality, user needs, and the burden on those providing information. The Office of Statistical Standards would be transferred from the Bureau of the Budget to become a staff office for the Director. The Bureau of the Census would also be placed under his control on a coordinate level with the new data center.

See also Senate Hearings on Computer Privacy 79-80 (statement of the author); Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 219 (1968); Zwick, *A National Data Center*, in ABA SECTION OF INDIVIDUAL RIGHTS AND RESPONSIBILITIES, MONOGRAPH NO. 1, at 33 (1967).

the communications and computer industries, and the law.[556] Obviously, the agency also should maintain a close liaison with other branches of the government in order to inform itself of the information needs of the public-policy makers and to be in a position to recommend needed legislation. One potential model for such an organization is the Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, which was created by the Omnibus Crime Control Act of 1968.[557]

One of the basic duties of the agency, and any study commission that might precede it, should be education, both of the policy makers and the public. At present there seems to be a substantial amount of formless, and to some degree needless, anxiety about the

---

556. *Cf. Senate Hearings on Computer Privacy* 80 n.15 (statement of the author).

557. 82 Stat. 197 (1968):

Sec. 804. (a) There is hereby established a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. . . .

(b) The Commission shall be composed of fifteen members appointed as follows:

(A) Four appointed by the President of the Senate from Members of the Senate;

(B) Four appointed by the Speaker of the House of Representatives from Members of the House of Representatives; and

(C) Seven appointed by the President of the United States from all segments of life in the United States, including lawyers, teachers, artists, businessmen, newspapermen, jurists, policemen, and community leaders, none of whom shall be officers of the executive branch of the Government.

(c) The President of the United States shall designate a Chairman from among the members of the Commission.

. . .

(d) It shall be the duty of the Commission to conduct a comprehensive study and review of the operation of the provisions of this title, in effect on the effective date of this section, to determine the effectiveness of such provisions during the six-year period immediately following the date of their enactment.

(e) (1) . . . the Chairman shall have the power to—(A) appoint and fix the compensation of an Executive Director, and such additional staff personnel as he deems necessary. . . .

(2) . . . the Chairman shall include among his appointment individuals determined by the Chairman to be competent social scientists, lawyers, and law enforcement officers.

. . . .

(g) Each department, agency, and instrumentality of the executive branch of the Government, including independent agencies, is authorized and directed to furnish to the Commission, upon request made by the Chairman, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this section. The Chairman is further authorized to call upon the departments, agencies, and other offices of the several States to furnish such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this section.

(h) The Commission shall make such interim reports as it deems advisable, and it shall make a final report of its findings and recommendations to the President of the United States and to the Congress within the one-year period following the effective date of this subsection. Sixty days after submission of its final report, the Commission shall cease to exist.

Variations on this general theme can be found in *Senate Hearings on Computer Privacy* 41-42; *House Hearings on Commercial Credit Bureaus* 49; PRIVACY AND THE NATIONAL DATA BANK CONCEPT 8-9. *See also* the proposal for a commission to study copyright and the new technologies, in title II of S. 543, 91st Cong., 1st. Sess. (1969).

specter of Big Brother, but very little informed concern of the kind that can be translated into effective governmental action. In furtherance of its educative function, the agency and any antecedent study commission should hold public hearings and symposia on a broad range of subjects, undertake technical and social science research projects, and act as a clearinghouse for information concerning activity in each of the many disciplines that touch upon computer technology or individual privacy. By use of these and other methods, an informational privacy agency could implement a philosophy analogous to that embodied in proposals to create a Technology Assessment Board[558]—the belief that it no longer is sufficient simply to respond to technological threats as they become acute, but that it is necessary to anticipate them and undertake enlightened planning to insure that scientific innovation is used in socially desirable ways.[559]

Another aspect in evolving policy for the computer technology-privacy area would be to grant the agency authority to engage in rulemaking governing the technical features, personnel qualifications, and administrative procedures to be employed by all data centers that deal with substantial quantities of personal information. Defining the scope of this rulemaking power, and any attendant licensing authority, undoubtedly will be one of the most politically sensitive phases of establishing the agency. Controversy certainly will arise over whether or not the agency's activities should extend to systems operated by state and local governments or private interests. Similarly, industrial groups can be expected to oppose attempts to apply privacy protection standards to the manufacturing of computer hardware and transmission equipment as well as to software systems. Although ideally the agency's regulatory power should be broad enough to cover those activities of nonfederal information systems and business concerns that bear on individual privacy, it stands to reason that any rulemaking power probably will be exercised sparingly in these contexts and might have to be more circumscribed than in the case of federal data systems. One can hope that self-regulation and the availability of model systems will obviate

558. H.R. 6698, 90th Cong., 1st Sess. (1967).

559. *See, e.g.*, Daddario, *Technology Assessment—A Legislative View*, 36 GEO. WASH. L. REV. 1044 (1968) ("[T]echnological changes have become so extreme and occur so rapidly that it is incumbent upon us to reverse the process. . . . We cannot any longer let technology run rampant and structure our social environment because of a planning vacuum."); Muskie, *The Role of Congress in Promoting and Controlling Technological Advance*, 36 GEO. WASH. L. REV. 1138 (1968) ("[T]echnological advance per se cannot be considered an unqualified benefit to man. If man is to reap the benefits of technological advance, such advance must be controlled and directed so that it benefits society as a whole.").

the need for a heavy commitment of agency time and effort in the nonfederal arena.

To implement the controls that it ultimately deems appropriate for protecting informational privacy, the new agency should engage in several other types of activity. One method of encouraging compliance is suggested by the extensive press coverage and popular response to congressional hearings on the proposed National Data Center and the credit bureau industry. Apparently there is enough concern for privacy to make the glare of public hearings and pronouncements a realistic avenue of expression to which both governmental and nongovernmental groups often will respond. But it would be illusory to believe that public or private officials are always responsive to press releases or the power of persuasion. Despite the fact that two congressional subcommittees were holding hearings during April 1969 on the propriety of some of the census questions and the desirability of retaining the criminal sanctions for noncompliance, the Census Bureau, apparently with White House approval, ordered the printing of the 1970 census in its present form, although it did reduce the number of people who will receive the long form of the census from fifteen to twelve million.[560] The move was justified with the usual bureaucratic protest that it was "too late" to make changes.[561] More effective would be statutory authority in a single agency to investigate, direct correction, and award appropriate relief for any alleged information abuses brought to its attention by citizens. Through the use of these techniques and its ability to negotiate with the information managers, the agency or commission could play the role of an information ombudsman.[562]

In developing procedures for discharging its role as a privacy protector, the agency should place central reliance on measures that give some level of effective control over personal information to the individual. The lack of this type of involvement may be the most important defect of the existing regime. The quest must be to de-

560. Wall St. J., April 18, 1969, at 1, col. 3.

561. N.Y.L.J., April 2, 1969, at 3, col. 5.

562. *Cf. Hearings on S. 1195 Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. 22 (1968), describing the proposed office of Administrative Ombudsman:

> He can be characterized briefly as a high level officer, with adequate salary and staff, free and independent of both the agencies he may criticize and the power that appoints him, with long tenure of office sufficient to immunize him from the natural pressures concurrent with seeking reappointment, with power to investigate administrative practices on his own motion. He is a unique officer whose sole job is to receive and act on complaints without the necessity for charge to the citizen. He should have the power to subpoena records. He operates informally and expeditiously without formal hearing procedures. His principal corrective weapons are publicity, criticism, persuasion, and reporting.

See generally Davis, *Ombudsmen in America: Officers To Criticize Administrative Action*, 109 U. PA. L. REV. 1057 (1961).

velop procedures that give the individual a voice in the important transactions concerning his personal life history—transactions that often are essentially "private adjudications"[563] and profoundly affect his future economic and social well-being. The law's traditional dedication to ideals of due process indicates that any set of rules regulating the handling of personal information should accord the individual, or someone who will represent his interests adequately, the right to receive notice and an opportunity to be heard before decisions are made concerning the information.[564] The right to be heard should include the ability to rebut damaging evaluations[565] and the right to demand that personal information conform to minimal standards of accuracy.[566] Disputes concerning the exercise of these rights undoubtedly will arise, and the development of an expeditious administrative means of resolving conflicts might be desirable.

---

563. *See House Hearings on the Computer and Invasion of Privacy* 26-27 (testimony of Professor Charles Reich):

> Another source of information that gets into the files is something I would call private adjudications, that is, formal decisions about people that are made outside of the courts. . . . [W]hat validity do these private decisions have? They can be a curse on the individual for the rest of his life, but you may not have any idea whether they are really accurate or not. They may meet no standards of fairness with which we are familiar.

564. *Cf.* the concurring opinion of Justice Black in Joint Anti-Fascist Refugee Committee v. McGrath, 341 U.S. 123, 143 (1951): "Assuming, though I deny, that the Constitution permits the executive officially to determine, list, and publicize individuals and groups as traitors and public enemies, I agree . . . that the Due Process Clause of the Fifth Amendment would bar such condemnation without notice and a fair hearing." *See also House Hearings on the Computer and Invasion of Privacy* 28 (testimony of Professor Charles Reich); *House Hearings on Commercial Credit Bureaus* 14 (testimony of Professor Alan Westin); Creech, *Psychological Testing and Constitutional Rights*, 1966 DUKE L. J. 332, 362-64; H.R. 7214, 91st Cong., 1st Sess. (1969).

565. *See, e.g., Hearings on Commercial Credit Bureaus* 14 (testimony of Professor Alan Westin):

> I would suggest requiring notification to the individual whenever a derogatory public-record item such as an arrest, lawsuit . . . or prosecution was entered in his file. The individual then would have the right to enter an explanation of reasonable length and would be asked to notify the credit bureau of the outcome if the matter were disposed of in any manner that did not produce an official disposition.

See also H.R. 7214, 91st Cong., 1st Sess., § 552a(a) (1969):

> Each agency which shall maintain records concerning any individual which are indexed according to the individual's name and which contain any information obtained from any source other than such individual shall . . .
>
> . . . .
>
> (6) permit an individual to supplement the information contained in his record with any information such individual deems pertinent to his record.

566. *Cf.* Miller, *Invasion of Privacy by Computer*, N.Y.L.J., June 4, 1968, at 4, cols. 6-7:

> First: Any government agency or private individual or firm which gathers personal data from several sources for the purpose of distributing that data to third parties should be required to:
> (a) Give notice to individuals that such data is being collected about them.
> (b) Afford access to the data for the purpose of verification.
> Second: Public authorities should not be authorized to purchase or use equip-

The effectiveness of an information agency designed to protect individual privacy obviously depends upon its ability to avoid becoming a captive of the governmental units and private interests that will have a stake in information networks and systems. The tendency of the so-called independent regulatory agencies to become captives of the industries they supposedly regulate is a disheartening prior history from which to proceed.[567] Perhaps with proper staffing and well-chosen lines of authority, an information agency can achieve the degree of independence needed to perform its watchdog role. The other extreme must be avoided as well. It cannot be permitted to become an island unto itself, populated by technocrats whose conduct is shielded by the alleged omniscience of the machines they manage, neither responsive nor responsible to anyone. Nor can its activities and regulations be permitted to ossify. For the foreseeable future the key to effective activity in the computer-privacy area will be to maintain the flexibility to adjust to changes in the technological and social environment.

IX. Conclusion

> Bureaucracy is the only way to coordinate the complex functions of a modern economy and society and therefore cannot be dismissed with a curse. Yet it is also an enormous potential source of arbitrary, impersonal power which folds, bends, spindles and mutilates individuals but keeps IBM cards immaculate.[568]

It may seem surprising, and perhaps distressing to some, that several of the tentative suggestions offered in this Article as responses to the problem of preserving the modest level of privacy

ment for the purpose of storing and distributing personal data to third parties unless a public necessity is established after public hearings.

See also S. 823, 91st Cong., 1st Sess., § 164(9)(e) (1969) (Proxmire Bill).

Even in the context of the mass circulation media, in which first amendment considerations are clearly strongest, it has been argued that a state still might impose a duty to print retractions or corrections of damaging news items. Barron, *Access to the Press—A New First Amendment Right*, 80 Harv. L. Rev. 1641, 1659 (1967). Further analogical support for a right to correct potentially damaging data items can be found in 39 U.S.C. § 4009 (Supp. III, 1965-1967), which provides that the individual has a right to compel anyone who mails "pandering advertisements" to remove his name from the mailing list.

567. *Cf. House Hearings on the Computer and Invasion of Privacy* 126 (statement of Paul Baran, computer expert for the Rand Corporation):

> [Regulation] is viscerally unsatisfying as it carries with it a built-in loss of freedom. The creation of another government agency peering over one's shoulder contains the possible dangers of bureaucratic delay and arbitrary conclusions based upon inadequate understanding of complex problems.
>
> Historically, Government regulatory agencies start as highly effective bodies but lose momentum as the original personnel leave and their replacements come from the industry being regulated.

For a discussion of these problems in a different context, *see* Bonfield, *Representation for the Poor in Federal Rulemaking*, 67 Mich. L. Rev. 511, 536-545 (1969).

568. M. Harrington, Toward a Democratic Left 144 (1968).

that we presently enjoy against the intrusive capacities of computer technology—a problem that is only beginning to emerge—should entail extensive federal intervention. Perhaps this merely reflects the impact that the computer is having on our society and the way it has permeated the daily affairs of virtually every individual and institution. With considerable justification, modern information-transfer networks have been described as a global electronic equivalent of the biological central nervous system[569] because of their unprecedented ability to interrelate social institutions, to create awareness and responsiveness to human problems, and to provide a massive store of information subject to instant recall.[570] As such, the computer is capable of immense social good, or monumental harm, depending upon how human beings decide to use it. Given the magnitude and significance of this new technology, a response from the national level is necessary.

And if the foregoing discussion seems slightly alarmist in tone, that is so because it is necessary to counteract the fact that "progress is a comfortable disease"[571] and the all-too-often complacent attitude of citizens toward the management of our affairs by astigmatic administrators in government and the private sector. The very real benefits conferred by computer technology may opiate our awareness of the price that is exacted in terms of personal freedom. It also seems desirable to sound the klaxon to arouse a greater awareness of the possibility that the computer is precipitating a realignment in the patterns of societal power and it is becoming increasingly important to decision-making 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 our legal system is how to contain the excesses and channel the benefits of this new form of power. If the concept of personal privacy is fundamental to our democratic tradition of in-

569. *Cf.* M. McLuhan, Understanding Media: The Extensions of Man 304 (paper ed., 1964):

> Any process that approaches instant interrelation of a total field tends to raise itself to the level of conscious awareness, so that computers seem to "think." In fact, they are highly specialized at present, and quite lacking in the full process of interrelation that makes for consciousness. Obviously, they can be made to simulate the process of consciousness, just as our electric global networks now begin to simulate the condition of our central nervous system.

See also Rapoport, *Technological Models of the Nervous System*, in The Modeling of Mind: Computers and Intelligence 25 (paper ed., 1968).

570. *Cf.* Benn, *Where Power Belongs*, The Nation, Aug. 26, 1968, at 136, 137: "Processed information about individuals could be the basis for a police state, and a mass of new safeguards would be required. But on the positive side this information could and should compel government to take account of every single individual in the development of its policy. Just to exist will be to participate."

571. 100 Selected Poems by E. E. cummings 89 (paper ed., Grove Press 1959).

dividual autonomy, and if its preservation is deemed desirable, then the expenditure of some verbal horsepower on its behalf seems justified.

Perhaps the most imperative need at this point in time is a substantial input of human resources to help solve the many privacy problems posed by the new technologies. The experimental laboratories exist—the federal agencies and many private organizations, such as the Interuniversity Communication Council, can provide the necessary structural context in which to test the privacy-protecting capacity of hardware, software, and administrative procedures. The scientific and business communities seem to be awakening—privacy protection techniques appear to be receiving increased attention in both of these fraternities. But is the legal profession ready to come to grips with the ramifications of the computer? Leading professional groups, such as the American Law Institute, the National Conference of Commissioners on Uniform State Laws, and the American Bar Association, must move to the forefront of the effort to develop a legal framework that will secure personal privacy while permitting effective implementation of the new information technologies.

Michigan Law Review

Vol. 67, No. 6 April 1969

Published Monthly, November through June, by the
Law School of the University of Michigan

NOTES

CONTRACTS—CONSIDERATION—Inadequacy of Consideration As a Factor in Determining Unconscionability Under Section 2-302 of the Uniform Commercial Code

Section 2-302 of the Uniform Commercial Code (Code) provides that a court may refuse to enforce all or part of a contract if it finds that the contract, or any part of it, was unconscionable when made.[1] In *American Home Improvement, Inc. v. MacIver*[2] the Supreme Court of New Hampshire apparently held that a price substantially in excess of the value of the goods and services sold was sufficient in itself to constitute unconscionability under this provision of the Code. The high price was at least in part attributable to high time-credit charges, and, as noted by the court, the contract could have been invalidated on the ground that the seller had violated a state law by not disclosing these charges in full.[3] Nevertheless, the language of the opinion leads to the conclusion that the inadequacy of consideration alone constituted unconscionability.[4]

In several other cases[5] striking down contract provisions, it is unclear whether courts viewed inadequacy of consideration as sufficient to make the contract unconscionable within the meaning of section 2-302. Others factors may have been essential to these courts'

1. This section provides:
(1) If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result.
(2) When it is claimed or appears to the court that the contract or any clause thereof may be unconscionable the parties shall be afforded a reasonable opportunity to present evidence as to its commercial setting, purpose and effect to aid the court in making the determination.

2. 105 N.H. 435, 201 A.2d 886 (1964).

3. Under the new Truth in Lending Bill (Consumer Credit Protection Act), 15 U.S.C. § 1601-77 (Supp. IV, 1968), disclosure of credit terms is required in all states. *Id.* § 1631.

4. The court stated that there was "[an] independent reason why the recovery should be barred in the present case because the transaction was unconscionable" and then proceeded to document the disproportionate price. 105 N.H. at 439, 201 A.2d at 888.

5. In addition to the cases discussed in the text, *see* FrostiFresh Corp. v. Reynoso, 52 Misc. 2d 26, 274 N.Y.S.2d 757 (N.Y. Dist. Ct. 1966) (contract calling for excessive credit charges was held to be unconscionable, the court noting that negotiations were conducted in Spanish, while the contract itself, which was not explained to the defendant, was in English); Robinson v. Jefferson Credit Corp., 4 U.C.C. REP. SERV. 15 (N.Y. Sup. Ct. 1967) (defendant, after exacting several fees from the plaintiff, refused to return plaintiff's repossessed car; contract held unconscionable and defendant ordered to return the car); *In re* Elkins-Dell Mfg. Co., Inc., 2 U.C.C. REP. SERV. 1016 (E.D. Pa. 1965); *In re* Dorset Steel Equip. Co., 2 U.C.C. REP. SERV. 1016 (E.D. Pa. 1965) (referee in bankruptcy refused enforcement of two security agreements under section 2-302 because they were too one-sided in favor of creditors).

decisions. In *In re State v. ITM, Inc.*[6] the defendants sold electrical appliances door-to-door, charging extremely high prices and making misrepresentations which were fraudulent under a state statute.[7] The New York trial court stated that the disparity of consideration was equivalent to that in *MacIver* and was sufficient "to clearly render such transactions unconscionable."[8] However, in the same sentence, the court stated that "when the deceptive practices are also considered, there can be no doubt about the unreasonableness and unfairness of these agreements."[9] In another New York case, *Central Budget Corp. v. Sanchez*,[10] plaintiff seller brought suit to enforce a contract for the sale of a 1959 Buick. The buyer's defense was that after the sale he had discovered several mechanical defects and that therefore the contract price was much more than the car was worth. In denying plaintiff's motion for summary judgment, the court noted that "[e]xcessively high prices may constitute unconscionable contractual provisions within the meaning of Section 2-302 UCC."[11] But the court added that defendants should have an opportunity to present evidence as to the over-all purpose and effect of the contract to aid the court in determining whether it is unconscionable.[12] This latter statement arguably implies that unconscionability should not be found solely on the basis of excessive price.

In a recent case, *Jones v. Star Credit Corp.*,[13] a New York trial court relied on section 2-302 to hold that welfare recipients who had paid almost 620 dollars on the installment purchase of a

---

6. 52 Misc. 2d 39, 275 N.Y.S.2d 303 (Sup. Ct. 1966).

7. The defendants violated subsection 12 of section 63 of the Executive Law of New York which provides:

> Whenever any person shall engage in repeated fraudulent or illegal acts or otherwise demonstrate persistent fraud or illegality in the carrying on, conducting or transaction of business, the attorney-general may apply . . . for an order enjoining the continuance of such business activity . . . and the court may award the relief applied for. . . . The word "fraud" or "fraudulent" as used herein shall include any device, scheme, or artifice to defraud and any deception, misrepresentation, concealment, suppression, false pretence, false promise or unconscionable contractual provisions.

N.Y. EXEC. LAW § 63(12) (McKinney Supp. 1968-1969). The court found the defendants' statements to be both false and unconscionable within the meaning of this statute. Defendants also violated section 402(2) of N.Y. PERS. PROP. LAW (McKinney Supp. 1968-1969) which provides that "[a] contract or obligation shall contain the entire agreement of the parties with respect to the goods and services," that promises to the buyer to compensate him for referrals must be in the contract, and that the contract must contain a clause permitting compensation earned to be deducted from the outstanding balance otherwise due under the contract.

8. 52 Misc. 2d at 54, 275 N.Y.S.2d at 321.

9. 52 Misc. 2d at 54, 275 N.Y.S.2d at 321.

10. 4 U.C.C. REP. SERV. 69 (N.Y. City Civil Ct. Rec. 1967).

11. 4 U.C.C. REP. SERV. at 70.

12. 4 U.C.C. REP. SERV. at 70.

13. 37 U.S.L.W. 2549 (N.Y. Sup. Ct., March 21, 1969).

freezer with a maximum retail value of 300 dollars[14] were entitled to keep the appliance in spite of the seller's claim that the purchasers still owed nearly 820 dollars in payments. The judge stated that "[t]here is no reason to doubt . . . that [section 2-302] is intended to encompasss the price term of the agreement."[15] But in phrasing the issue for decision, the court asked "whether or not, under the circumstances of this case, the sale . . . is unconscionable as a matter of law."[16] The court held that it was, but not without discussion of the "circumstances."[17] It stressed the huge disproportion between price and retail value, and stated that this mathematical disparity "carries the greatest weight."[18] Thus, the court did not clear up the uncertainty about whether excessive price alone can constitute unconscionability.

Under the general common law of contracts, inadequacy of consideration by itself was simply no basis for legal relief.[19] Even in equity, relief for excessive price was difficult to obtain. In a few cases courts cancelled contracts solely because of inadequacy of consideration, but in these cases the inadequacy was so great as to "shock the conscience."[20] Equity courts were more willing to grant relief, both affirmative and defensive, when an excessive price was accompanied by other inequitable incidents.[21] In both situations, however, the courts based their decisions on the traditional theories of fraud, mistake, and undue influence, and not on inadequacy of consideration.

An affirmative fair exchange doctrine, known as *laesio enormis*, existed in medieval law and has been incorporated into many civil law codes.[22] These codes authorize recision of contracts of sale when it can be shown that there was disproportionate consideration. A precise mathematical standard is sometimes used to evaluate prices, the courts considering a price "disproportionate" if it is a certain percentage greater than the market value of the item for which it is exchanged.[23] Cases under the Louisiana Civil Code,

14. The plaintiffs' (purchasers') proof at trial of the maximum retail value of the freezer was not controverted by the defendant seller. 37 U.S.L.W. at 2549.

15. 37 U.S.L.W. at 2549, citing FrostiFresh Corp. v. Reynoso, 52 Misc. 2d 26, 274 N.Y.S.2d 757 (Dist. Ct. 1966); *In re* State v. ITM, Inc., 52 Misc. 2d 39, 275 N.Y.S.2d 303 (Sup. Ct. 1966); and American Home Improvement, Inc. v. MacIver, 105 N.H. 435, 201 A.2d 886 (1964).

16. 37 U.S.L.W. at 2549.

17. *See* notes 44-45 *infra* and accompanying text.

18. 37 U.S.L.W. at 2550.

19. 1 A. CORBIN, CONTRACTS §§ 127, 128 (1963 ed).

20. 3 J. POMEROY, EQUITY JURISPRUDENCE § 927, at 634 n.13 (S. Symons, 5th ed. 1941).

21. *Id.* at § 928.

22. 1 A. CORBIN, CONTRACTS § 127, 128 (1963 ed.); 3 J. POMEROY, EQUITY JURISPRUDENCE § 927, at 637 n.18 (S. Symons, 5th ed. 1941). *See* Dawson, *Economic Duress and the Fair Exchange in French and German Law*, (pts. 1 & 2), 11 TUL. L. REV. 345, 364 (1937), (pt. 3) 12 TUL. L. REV. 42 (1937).

23. *See* Dawson, *supra* note 22, at 364-76.

which adopts the civil law principle of *lesion* by providing that a reasonably proportionate price is required to sustain a contract of sale,[24] illustrate that in practice civil-law courts are reluctant to assess price differentials. The Louisiana courts have refused to interfere with merely highly profitable bargains and have demanded gross disproportion between price and market value before they will set contracts aside. In effect, they thereby limit the doctrine of *laesio* so that it operates to invalidate only those contracts which are supported by no more than nominal consideration.[25] Under such a test even the contracts involved in *MacIver* and the other three cases discussed above could have been upheld. However, it is important to recognize that the *laesio* doctrine, whether applied conservatively or liberally, does focus solely on price.

It is doubtful that the Uniform Commercial Code was intended to authorize a shift to the *laesio* approach. Prior to the adoption of section 2-302 by the Commissioners on Uniform State Laws, there was concern that inclusion of such a provision in the Code would interfere with the freedom of a buyer and seller to contract and that judicial investigation of the adequacy of consideration was inconsistent with our competitive economy.[26] Perhaps in reaction to this fear, the official comment to section 2-302 indicates that, at least in the drafters' opinion, the main function of section 2-302 was merely to reaffirm the propriety of judicial scrutiny in areas pre-

24. LA. CIV. CODE ANN. art 2464 (West 1952), which requires that the price not be "out of all proportion of the thing." For an interpretation of this section, *see* Herbert & Lazarus, *Some Problems Regarding Price in the Louisiana Law of Sales*, 4 LA. L. REV. 378, 412-18 (1942). A number of states have adopted statutes which permit courts to use inadequacy of consideration as a basis for the denial of specific performance. *See, e.g.*, CALIF. CIV. CODE § 3391 (West 1954). In such states, while a legal right to relief theoretically exists, at least one study indicates that when equitable relief was denied, no legal relief was in fact forthcoming. *See* Frank & Endicott, *Defenses in Equity and "Legal Rights,"* 14 LA. L. REV. 380 (1954).

25. *See* Brooks v. Broussard, 136 La. 380, 67 S. 65 (1914) (price which equalled at least one-half the value of the property sufficient to support the contract). *See also* Johnson v. Mansfield Hardwood Lumber Co., 143 F. Supp. 826 (D.C. La. 1956). In cases decided under the California statute relating to the denial of specific performance, courts were more willing to assess the inadequacy. For cases holding that consideration was inadequate, *see* Cornblith v. Valentine, 211 Cal. 243, 294 P. 1065 (1930) (price was two-thirds of the value); Wilson v. White, 161 Cal. 453, 119 P. 895 (1911) (discrepancy of 1,000 dollars in 14,000 dollars transaction sufficient where other elements of overreaching appeared); Dessert Seed Co. v. Garbus, 66 Cal. App. 2d 838, 153 P.2d 184 (1944) (price 3,400 dollars, reasonable market value 5,000 dollars); *cf.* Miami Tribe v. United States, 281 F.2d 202 (Ct. Cl. 1960), *cert. denied*, 366 U.S. 924 (1961) (payment of less than one-half market value is unconscionable).

26. *See, e.g.*, Hogan, *The Highways and Some of the Byways in the Sales and Bulk Sales Articles of the U.C.C.*, 48 CORNELL L.Q. 1, 42 (1962); King, *Suggested Changes in the Uniform Commercial Code—Sales*, 33 ORE. L. REV. 113, 116 (1954); Legislation, *Definition and Interpretation of Unconscionable Contracts*, 58 DICK. L. REV. 161 (1954); Note, *Policing Contracts Under the Proposed Commercial Code*, 18 U. CHI. L. REV. 146, 151 (1950); Note, *Section 2-302 of the Uniform Commercial Code: The Consequences of Unconscionability in Sales Contracts*, 63 YALE L.J. 560 (1954).

viously subject to the courts' supervision—for example, limitations on remedies and disclaimers of warranty.[27] The comment asserts that section 2-302 was designed to prevent "oppression and unfair surprise"; it was not intended to change the "allocation of risks because of superior bargaining power,"[28] nor was it designed to protect the foolish from bad bargains. It appears, therefore, that cases like *MacIver* and *Jones*, which apparently equate excessive price with unconscionability, are beyond the intended purview of section 2-302.

Whatever the drafters of the Code may have intended, the cases demonstrate that courts examining contractual arrangements may consider adequacy of consideration an important factor; some courts may go so far as to hold that proof of inadequacy of consideration is enough in itself to establish unconscionability. This recent development raises two major questions: How should a court assess the price charged by the seller to determine whether it is in fact too high for the goods or services offered to the buyer?[29] And, if a court requires other elements than disproportionate price for a showing of unconscionability, what should these other elements be?

A two-step approach can be used to develop a standard for determining whether a seller's price is out of line. The first step is to decide whether a seller's *markup*—the difference between the selling price and the wholesale price of the goods, or his *profit*—the difference between the selling price and the cost of the goods sold (including selling and operating expenses), provides the best measure of the fairness of his price. If markup is used, a seller could legitimately complain that he was denied the same rate of return as other sellers

27. *See, e.g.*, Kansas City Wholesale Grocery Co. v. Weber Packing Corp., 93 Utah 414, 73 P.2d 1272 (1937); Hardy v. General Motors Acceptance Corp., 38 Ga. App. 463, 144 S.E. 327 (1928). *See also* Henningsen v. Bloomfield Motors, Inc., 32 N.J. 358, 161 A.2d 69 (1960); Note, *Unconscionable Contracts Under the U.C.C.*, 109 U. PA. L. REV. 401, 408-15 (1961).

The decision to define unconscionability by reference to those areas in which courts had previously deemed contracts unconscionable—for instance, warranty disclaimers and liquidated damage clauses—is anomalous because the Code deals in detail with what is permissible in these types of clauses. *See* UNIFORM COMMERCIAL CODE §§ 2-316, 2-719 [hereinafter UCC]. Leff, *Unconscionability and the Code—The Emperor's New Clause*, 115 U. PA. L. REV. 485, 516-24 (1967) which suggests that in view of the way the Code regulates such clauses in detail, it is difficult to assume that section 2-302 adds anything in the way of protection from unconscionability. Leff suggests that the reason for the paradox may simply be imprecise drafting.

The only case referred to in the official comment which would support the proposition that inadequacy of consideration should suffice for unconscionability is Campbell Soup Co. v. Wentz, 172 F.2d 80 (3d Cir. 1948). If the drafters intended to incorporate this notion into the Code, it is likely they would have made a more substantial reference to it than a *"cf."* *See* Leff, *supra*, at 530, 538.

28. *See* UCC § 2-302, comment 1.

29. The result in *MacIver* emphasizes the need to develop standards for assessing the fairness of the price. The carrying charge in that case, which the court failed to calculate, was apparently only eighteen per cent. *See* Leff, *supra* note 27, at 549-51,

because he had sales expenses, overhead, bad debts, or other costs which were not reflected in this measure of consideration.[30] Consumers may also be adversely affected by the use of a markup standard. Many sellers provide transportation, installation, or other services free of charge when goods are purchased. Such a seller's price may be relatively high, but it may be the best price obtainable for the combination of goods and services which he provides. If this price is deemed unconscionable, as it might well be under a strict markup standard, the seller will probably eliminate or at least reduce his free services, and this would be to the detriment of consumers. A profit standard, by taking all costs into account, presents a fairer picture of the transaction and thus seems to be a better unit of measurement. The only difficulty with using profit is that different accounting methods will often produce different results, even when individual sales are involved. This difficulty is not insurmountable; in other circumstances, courts have weighed the merits of different accounting systems to determine which best reflects a seller's costs.[31] A similar approach should be used in cases involving claims of unconscionability because of excessive price.

The second important step in analyzing a challenged transaction is to develop a standard of fair profit with which the particular seller's profit can be compared. The simplest standard would be a fixed percentage of profit applicable to all sellers, but this seems to be inconsistent with the ideal of a free market economy regulated by the mechanism of competition.[32] According to this ideal, the emergence of abnormally high profits in a particular market will

30. The usury laws typically set a flat rate which may be charged for the use of money. This approach resembles the use of a markup standard in that costs are not taken into account in computing the rate of interest. The inflexible rate set by the usury laws has been criticized as unreflective of the true costs and risks involved to the lender. *See, e.g.*, F. RYAN, USURY AND USURY LAWS 9-10, 174 (1924).

31. *See* INT. REV. CODE OF 1954, § 446, which requires that taxable income be computed according to an accounting method which clearly reflects a taxpayer's income. "[W]e read 'clearly reflect the income . . .' to mean . . . that income should be reflected with as much accuracy as standard methods of accounting practice permit [rather than merely fairly and honestly]." Caldwell v. Commissioner, 202 F.2d 112, 114-15 (2d Cir. 1953). *See also* Niles Bement-Pond Co. v. United States, 281 U.S. 357 (1930) (an accrual method was required); Kahuku Plantation Co. v. Commissioner, 132 F.2d 671 (9th Cir. 1942) (allowed a hybrid method to be used); Boynton v. Pedrick, 136 F. Supp. 888 (S.D.N.Y. 1954), *aff'd.*, 228 F.2d 745 (2d Cir. 1954); Motors Securities Co., Inc., ¶ 52,316 P-H Tax Ct. Mem. (1952) (tax court held discounts on notes not to be income to an auto finance company in the year of purchase; instead, the court ruled that it was permissible to spread the income over the life of the notes when that practice had been followed for years and income was not distorted); Bellevue Mfg. Co., ¶ 57,094 P-H Tax Ct. Mem. (1957) (tax court required a cash accounting method).

32. *See* P. AREEDA, ANTITRUST ANALYSIS 3-11 (1967); J. BAIN, PRICING DISTRIBUTION AND EMPLOYMENT 5, 65-66, 130 (rev. ed. 1953). *See also* P. SAMUELSON, ECONOMICS 39-57, 778-93 (1967).

attract new entrants into that market.[33] These will be new enterprises or will come from relatively unproductive segments of the economy, and their entry into the market to take advantage of the demand creating the high profits will achieve a desirable allocation of resources.[34] Their arrival is also supposed to drive profits down to a level consistent with the costs and risks of operating in the particular market.[35] Theoretically, judicial precedent prohibiting profits above a certain percentage of the cost of a good would place an artificial limitation on sellers in the market, with the result that new entrants would not be attracted, economic resources would not be correctly allocated, and price competition would not be stimulated. It may be argued that these theories of a free market economy do not conform to the realities of the economic system.[36] However, these theories are embodied in the antitrust laws[37] and in other state and federal statutes,[38] and inconsistent rules should not be promulgated by the courts.[39]

A better test would be to compare a seller's profit to the profits of similarly situated sellers. This would remove the problem of discouraging market entry, because sellers in the market would not be forced to maintain an artificially low price. However, if a court does not make certain that the sellers used for comparison to the challenged seller are indeed similarly situated, its decision may yet be in conflict with the ideal of a free market economy. Some sellers who are more successful than their competitors should be allowed to reap greater profits; they provide additional benefits for consumers and spur their competitors to emulate them. If other sellers in the market do improve their operations in some manner, there will be increased consumer benefits and, because of the resulting increase in competi-

33. *See* P. AREEDA, *supra* note 32, at 3.

34. *Id.* at 11.

35. *Id.* at 4.

36. *See* T. ARNOLD, FOLKLORE OF CAPITALISM (1937). *See also* P. AREEDA, *supra* note 32, at 11.

37. *See* P. AREEDA, *supra* note 32, at 3-4; *see also* A. NEALE, THE ANTITRUST LAWS OF THE UNITED STATES OF AMERICA 29-30 (1966).

38. *See* P. AREEDA, *supra* note 32, at 3.

39. Suggesting that the theories underlying the unconscionability clause of section 2-302 are the same as those underlying antitrust laws and other statutes does not imply that the unconscionability clause is to be administered as extensively as some of those laws are. Obviously, courts are not to police contracts for unconscionable provisions in the same way that the Federal Trade Commission polices contracts, mergers, and other agreements which restrain trade; courts are to determine unconscionability only when a private litigant has raised the issue. Because most buyers do not know of the unconscionability clause and because most losses which occur as a result of unconscionable contract provisions are not costly enough to warrant a court action, the unconscionability clause will not deter unreasonable commercial practices to any great degree. More regulation may be needed in this field; if so, legislatures will have to provide more effective enforcement machinery than section 2-302. For an example of such legislation, *see* the discussion in note 7 *supra*, of the New York statute which authorizes the state attorney general to bring suit when a seller misleads a buyer.

tion, these benefits may well be available at a lower price. Thus, sellers should not be penalized for higher profits if these profits are attributable to excellent business locations, to particularly efficient operations, or to access to a particular class of customers who are willing and able to pay more for their products;[40] competitors should be encouraged to improve their locations and operations and to seek out high-paying customers. Greater profits would also be justified if the seller offers a high-quality or an unusual product or if he provides a better quantitative or qualitative selection of ancillary services than his competitors.

All of these considerations make it clear that great care must be exercised in deciding which sellers in a given market are "similarly situated." A certain fixed percentage of the average profit of similarly situated sellers could be chosen as the dividing line for determining whether a challenged seller's profit is excessive, but this probably would not be desirable. Because of the possibilities of error inherent in determining a seller's profit and in finding comparable sellers, there can be no certainty to the test suggested above. Moreover, applying a fixed standard based on percentage of profit above cost of goods sold would create only the illusion of certainty. Worse, such a test would be inflexible. Courts should not evaluate the seller's price in a vacuum, as they would in effect be doing if they applied a a fixed standard. The judge should ascertain the extent to which the seller's profit exceeds that of his competitors—that much is clear. However, he should weigh this factor in the context of the particular case, requiring less in the way of excess profits for a finding of unconscionability when certain other factors are present. Factors which a court should consider are those which demonstrate, with more force than the mere presence of high prices and profit margins, that the seller intended to take unfair advantage of the buyer. Because of the imprecision involved in comparing prices and profits, courts should be reluctant to declare contracts unconscionable when such circumstances are not present in the case.

The buyer's inability to comprehend the transaction is one factor which could lead to a finding of unconscionability. In *FrostiFresh Corp. v. Reynoso*,[41] a contract calling for excessive credit charges was

---

40. A seller can cultivate high-paying customers as long as he does not restrict other sellers from dealing with those customers:

> As we see it, the laws of the United States do not require that persons engaged in private trade and commerce must deal with everyone. When they do deal they may not discriminate, but they do have the right to choose their customers. The Clayton Act as amended by the Robinson-Patman Act itself provides in section 2(a) "Nothing herein contained shall prevent persons engaged in selling goods, wares, or merchandise in commerce from selecting their own customers in bona fide transactions and not in constraint of trade." Sec. 13(a), Title 15 U.S.C.A.

Chicago Seating Co. v. S. Karper & Bros., 177 F.2d 863, 867 (7th Cir. 1949). *See also* FTC v. Bausch & Lomb, 321 U.S. 707 (1944).

41. 52 Misc. 2d 26, 274 N.Y.S.2d 757 (N.Y. Dist. Ct. 1966).

held unconscionable. The New York court noted that negotiations for the contract were conducted in Spanish, but the contract itself, which was not fully explained to the defendant, was in English.[42] This factual context presents a substantial possibility that the buyer misunderstood the implications of the contract and that he was in fact exploited by the seller. The court was clearly correct in taking it into account. The question arises, however, whether courts should consider less obvious indicia of a buyer's low degree of commercial sophistication, such as his low intelligence level or his lack of knowledge of the seller's business. Courts are justifiably much more likely to consider these relatively subjective indicia of the buyer's knowledge if it is clear that the seller was aware of the buyer's shortcomings and played upon them. In *Williams v. Walker-Thomas Furniture Co.*,[43] for example, the court held two installment contracts unconscionable on the grounds that the seller knew of the buyers' lack of education and poor financial position and yet inserted in each of the contracts an "obscure" provision which allowed the seller in the event of a default, to repossess all items the buyers had previously purchased from him.[44] In *Jones v. Star Credit Corp.*, discussed above, the New York Supreme Court stated that

> a caveat is warranted lest we reduce the import of Section 2-302 solely to a mathematical ratio formula. It may, at times, be that; yet it may also be much more. The very limited financial resources of the purchaser, known to sellers at the time of the sale, is entitled to weight in the balance. Indeed, the value disparity itself leads inevitably to the felt conclusion that knowing advantage was taken of plaintiffs.[45]

Some sales techniques might be sufficient in themselves, or at least when coupled with excess price, to render a contract unconscionable. A seller's failure to disclose an important aspect of the

42. It is not clear that these facts were necessary to the court's decision.

43. 350 F.2d 445 (D.C. Cir. 1965).

44. *See* Note, *Contracts—Enforcement—Unconscionable Installment Sales Contract Is Unenforceable*, 79 HARV. L. REV. 1299 (1965). The court could not base its decision on section 2-302 because the Code was not in effect in the District of Columbia when the contracts in question were made. It held that the rule of section 2-302 was part of the common law of the district, and, alternatively, that it could adopt this rule pursuant to its power to develop the common law of the district. 350 F.2d at 447-48 (D.C. Cir. 1965). The contract provision referred to in *Williams* is commonly called an "add on" clause. Only one state has a statute forbidding such clauses and Maryland specifically allows them. Leff, *Unconscionability and the Code—The Emperor's New Clause*, 115 U. PA. L. REV. 485, 554-55 (1967).

In *Jones*, discussed at notes 13-18 *supra* and accompanying text, the court cited *Walker* for the proposition that "the meaningfulness of choice essential to the making of a contract, can be negated by a gross inequality of bargaining power." 37 U.S.L.W. at 2550.

45. 37 U.S.L.W. 2550 (N.Y. Sup. Ct. March 21, 1969).

transaction to the buyer is one factor which might support a finding of unconscionability. Thus, in *MacIver* the court was probably influenced by the fact that the seller had failed to disclose finance charges.[46] High pressure sales tactics would also be relevant in determining whether a contract is unconscionable. In *In re State v. ITM, Inc.* the court held that the seller's "deceptive practices," in conjunction with disproportionate price, established grounds for a holding of unconscionability.[47] *MacIver* and *In re State v. ITM, Inc.* were relatively easy cases because the sales practices engaged in were defined as illegal under state statutes.[48] In addition to such state legislation, the courts might examine standards of fair dealer activity developed by government agencies devoted to consumer protection[49] and by trade associations. When such criteria for evaluating particular selling tactics are not relevant or available, the courts should probably consider the practices of other sellers. Before accepting dealer practices as evidence, however, courts should make sure that the practices are designed to provide fair treatment for buyers and are not used simply to promote efficiency.[50]

There is, of course, a counterargument that courts should not consider the buyer's degree of commercial sophistication or the seller's business practices, at least when these practices do not violate state or federal statutes. It may be argued that such an approach eliminates the traditional adversary relationship between buyer and seller and institutes an agency relationship in which sellers have a vague duty to warn and to care for buyers. However, since requiring sellers to conform to statutes which define moral business practices does not seem to be harsh or unjustifiable,[51] administrative guides, trade association rules, and accepted dealer practices should be regarded in the same way. Such requirements certainly do not give rise to agency relationships; nor do they impose new duties. Section 2-302 and other provisions of the Code were apparently intended to eliminate the harsh consequences of a completely adversary relationship between buyer and seller, and this purpose can be accomplished only by allowing courts to inquire into sellers' practices and buyers'

46. *See* notes 2-4 *supra* and accompanying text.

47. *See* note 6 *supra* and accompanying text.

48. The statute involved in *MacIver* required disclosure of time-credit charges. The statute involved in *In re* State *v. ITM, Inc.* is quoted in note 7 *supra*. The Federal Trade Commission, for example, issues guidelines for use in examining the fairness of such dealer practices as price advertising, reduction of prices, and retail price comparisons. *See FTC Guides Against Deceptive Pricing*, 16 C.F.R. pt. 233 (1949).

49. For a general discussion of trade associations and professional codes of ethics, *see* J. BRADLEY, THE ROLE OF TRADE ASSOCIATIONS AND PROFESSIONAL BUSINESS SOCIETIES IN AMERICA (1965); G. LAMB, TRADE ASSOCIATIONS LAW AND PRACTICE (1956).

50. For example, it may be common practice to fill in all the blanks on a credit form simply because doing so tends to insure accuracy later.

51. See *In re* State v. ITM, Inc., 52 Misc. 2d 39, 275 N.Y.S.2d 303 (Sup. Ct. 1966).

capabilities.[52] Statutes are helpful in determining which events and circumstances make a contract unconscionable, and more comprehensive legislation is certainly needed in this area. However, considering the infinite variety of contract provisions and selling practices, it is doubtful that legislatures could designate all the activities which a court should consider in assessing the cases which come before it. Furthermore, extremely detailed legislation might prevent courts from weighing different dealer practices in light of the effect they have on purchasers with different intelligence levels and backgrounds. For these reasons courts should look beyond legislation to other prevalent definitions of acceptable business practices in determining unconscionability.

It is more questionable whether courts should follow the precedent set in *Williams* and consider the buyer's financial status and the seller's knowledge of it. A buyer's wealth is not necessarily indicative of his ability to bargain with sellers, although, given facts similar to those in *Jones*, a court may suggest that this is the case. However, a buyer's financial position is relevant to some issues arising in these cases and probably should be considered for that reason. In usury cases it has been observed that poor borrowers often do not question the terms set by lenders because they fear they will be refused loans elsewhere.[53] Some lenders probably take advantage of this state of affairs by charging usurious rates and by imposing other difficult contract terms on borrowers. If the poor borrower is buying goods on an installment basis, the seller-lender has the opportunity to exploit the buyer's fear of being refused credit elsewhere. In an attempt to circumvent the usury laws, he may charge an excessive price for the goods instead of imposing high interest rates. Since the buyer's financial status and the seller's knowledge of it are the determinants of the buyer's vulnerability, courts should examine these factors for the limited purpose of ascertaining whether and to what extent coercion and deception exist.[54] It has been argued

---

52. It is nevertheless true that the drafters of section 2-302 may not have envisioned such inquiries. *See* note 27 *supra* and accompanying text.

Some states have also increased their legislation regulating dealer activities. *See, e.g.*, Maryland Retail Installment Sales Act, MD. ANN. CODE art. 83, §§ 132A-52 (Supp. 1968) [referred to in Williams v. Walker-Thomas Furniture Co., 350 F.2d 445 (D.C. Cir. 1965)]; N.Y. EXEC. LAW § 63(12) (McKinney Supp. 1968-1969); N.Y. PERS. PROP. LAW § 402(2) (McKinney Supp. 1968-1969) [referred to in *In re* State v. ITM, Inc.,. 52 Misc. 2d 39, 275 N.Y.S.2d 303 (Sup. Ct. 1966)].

53. *See In re* William Sylvester Branch, 40 REF. J. 101, 102 (N.D. Tenn. 1966) (mem.).

54. Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 447 (D.C. Cir. 1965):

> Unconscionability has generally been recognized to include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party. Whether a meaningful choice is present in a particular case can only be determined by consideration of all the circumstances surrounding the transaction. In many cases the meaningfulness of the choice is negated by a gross inequality of bargaining power.

that a court's consideration of these factors would confuse the issues and create uncertainty as to the basis for the decision;[55] but this criticism holds true only when the court does not make its limited purpose clear, and thus it seems to be mainly a criticism of judicial writing.

In summary, although the draftsmen of the Code did not intend such results, several recent cases seem to hold that excessive price is enough in itself to constitute unconscionability under section 2-302. Since these decisions stress price as the most important factor in the determination of whether or not a contract is unconscionable, standards should be developed for asserting price. It is submitted that a price should be held sufficiently excessive to render a contract unconscionable if it gives the seller a greater profit than similarly situated sellers ordinarily receive. This test presents the most accurate assessment of the transaction in question and it also conforms to the economic theories incorporated in our antitrust laws and other statutes. However, the courts should not apply an inflexible percentage standard to determine in the abstract whether a seller's profit is excessive; instead, they should evaluate the differential between the seller's profit and that of his competitors in the light of such factors as the buyer's ability to understand the transaction and in light of generally accepted commercial practices. Finally, because of the possibilities of error inherent in assessing price, it is suggested that courts ordinarily should not declare contracts unconscionable if there is no evidence of the seller's overreaching other than the excessive price.

55. The attorney who argued the *Walker-Thomas* case for Mrs. Williams has stated that the infusion of the financial status of the consumer confuses the issues, "creating a degree of uncertainty" around the decision. *See* Skilton & Helstad, *Protection of the Installment Buyer of Goods Under the Uniform Commercial Code*, 65 MICH. L. REV. 1465, 1480 (1967).

RECENT DEVELOPMENTS

CONSTITUTIONAL LAW—Equal Protection—Property Ownership Qualifications on the Right To Vote in Special Municipal Elections—*Cipriano v. City of Houma**

Plaintiff, a resident of Houma, Louisiana, who owned no real property, brought a class action seeking to prevent the city from issuing utility revenue bonds approved by a vote of the property taxpayers at a special election. He argued that the Louisiana statute[1] restricting the right to vote in such elections to property owners[2] was unconstitutional. Plantiff relied on *Harper v. Virginia Board of Elections*,[3] in which the Supreme Court declared that Virginia's required payment of poll taxes for voting in general elections was a violation of the equal protection clause of the fourteenth amendment. *Harper*, he claimed, established that any voter qualification based on property ownership violates the equal protection clause. The three-judge federal district court rejected this argument, one judge dissenting; *held*, the denial to residents who do not own property of the right to vote in municipal elections on the issuance of revenue bonds for public utilities does not violate the equal protection clause of the fourteenth amendment.

In general, there appear to be two types of limitations on the right to vote that are constitutionally permissible. Voter-qualification requirements may be sustained either when they promote intelligent or responsible voting[4] (voting competence) or when they

* 286 F. Supp. 823 (E.D. La. 1968). This case was reversed by the Supreme Court in a unanimous decision on June 16, 1969 while this issue was in the final stage of being printed. N.Y. Times, June 17, 1969, at 57, col. 5.

1. LA. REV. STAT. § 33:4258 (1950), pursuant to LA. CONST. art. 14, § 14(a). In the case of utility revenue bonds, LA. CONST. art. 14, § 14(m) contemplates an optional election, but the section first mentioned above makes it mandatory. If the voters in the special election veto the bond issue, that veto is decisive. If they approve it, final approval must still be given by the local governing body. LA. REV. STAT. §§ 33:4252, 33:4258 (1950). Only the constitutionality of the distinction between property owners and nonproperty owners will be examined here; it should be noted, however, that the Louisiana statutes cited require that bond issues be authorized by a majority of the property taxpayers in "number and amount"—a requirement of doubtful constitutionality in light of the development of, and emphasis on, one man-one vote.

2. The property taxpayer requirement has been interpreted as a property ownership requirement. McFatter v. Beauregard Parish School Bd., 211 La. 443, 30 S.2d 197 (1947); C. ADRIAN & C. PRESS, GOVERNING URBAN AMERICA 90 (3d ed. 1968) ("By property taxpayers are meant property owners, of course").

3. 383 U.S. 663 (1966).

4. In Lassiter v. Northampton County Bd. of Elections, 360 U.S. 45, 51 (1959), the Court upheld North Carolina's literacy requirement, concluding that "[t]he ability to read and write has some relation to standards designed to promote the intelligent use of the ballot." Other qualifications the Court there cited as constitutionally permissible were age, residence, and previous criminal record.

serve to separate persons with a substantial interest in the outcome of an election from others with little or no such interest[5] (interest in the result). If the property ownership qualification in *Cipriano* performs either of these functions, the decision of the district court should be upheld.

Qualifications for voting are traditionally established by the legislature, and thus it might seem that the legislative determination on the questions of voting competence and interest in the election should prevail. A strong presumption of validity normally attaches to legislative enactments,[6] and consequently it is not the function of the judiciary to decide whether the means adopted by the legislature are the best means possible to attain the end sought.[7] Indeed, the court in *Cipriano* relied heavily on the legislature's

There is some indication that restrictions on the states may be even more stringent when a congressional enactment is involved than when the fourteenth amendment alone is involved. In Cardona v. Power, 384 U.S. 672 (1966), the Court found that by force of the supremacy clause and section 4(e) of the Voting Rights Act of 1965, 42 U.S.C. § 1973(e) (Supp. III, 1965-1967), the State of New York's English literacy requirement cannot be enforced against persons legally literate in Spanish by virtue of successful completion of sixth grade in a public school, or in a private school accredited by the Commonwealth of Puerto Rico.

The Court has condemned voter qualifications which bear no demonstrable relation to the promotion of intelligence and responsibility in voting. For instance, in Carrington v. Rash, 380 U.S. 89 (1965), it struck down a provision of the Texas constitution which prohibited any member of the armed forces who moved to Texas from ever voting in that state while still in the armed forces. 380 U.S. at 91-92. In *Harper*, the Court declared the Virginia poll tax unconstitutional saying, "Voter qualifications have no relation . . . to paying . . . this or any other tax." 383 U.S. at 666.

5. The Supreme Court has stressed the basic premise that issues should be decided by a majority of the people concerned. Reynolds v. Sims, 377 U.S. 533 (1964); Wesberry v. Sanders, 376 U.S. 1 (1964); Gray v. Sanders, 372 U.S. 368 (1963); Baker v. Carr, 369 U.S. 186 (1962). As one distinguished observer has concluded, "In all the cases emerges the basic proposition that a majority of the human beings concerned will determine their political and economic fate." A. SUTHERLAND, CONSTITUTIONALISM IN AMERICA 508 (1965).

It is apparent that if a person has no concern with the outcome of an election, it is not a denial of equal protection to deny him the right to vote. However, it will not always be possible to say that a person has no interest whatsoever in the outcome of an election. Rather, the line must be drawn on the ground that certain people have a substantially greater interest in an issue than others, whose interest may be indirect or insubstantial. If this is established, it is not unreasonable or unfair to exclude the latter group from voting on a particular issue. For instance, a resident of Ann Arbor who commutes fifty miles to Detroit to work is undoubtedly affected by and interested in the outcome of the municipal elections in Detroit; however, it is not unconstitutional to deny him the right to vote in those elections. The distinction would have to be drawn on the basis of the fact that property owners as opposed to those who did not own property in Detroit were substantially more interested in the outcome and issues of such general elections, and the latter group had no other interests substantial enough to entitle them to vote.

6. *See, e.g.*, Toombs v. Citizens Bank, 281 U.S. 643, 647 (1930); Home Tel. & Tel. Co. v. City of Los Angeles, 211 U.S. 265 (1908).

7. McLean v. Arkansas, 211 U.S. 539, 547 (1909); *cf.* Allied Stores of Ohio, Inc. v. Bowers, 358 U.S. 522, 527 (1959). *See also* Old Dearborn Distrib. Co. v. Seagram Distillers Corp., 299 U.S. 183 (1936); Standard Oil Co. v. City of Marysville, 279 U.S. 582 (1929); St. Louis Southwestern Ry. v. Board of Directors, 207 F. 338 (8th Cir. 1913).

determination that the property ownership qualification serves as a wise fiscal restraint.[8] However, it is clear that the legislature cannot choose a method that violates the fundamental liberties of individuals if the same end can be achieved without infringing those liberties.[9] In the *Cipriano* situation, there might well be alternative means for promoting fiscal restraint which do not impinge on a number of citizens' right to vote, as the property ownership qualification does. Possible alternatives include such mechanisms as manipulation of debt ceilings, state approval of locally approved bond issues, or the present requirement of the Louisiana statute that final approval of the bond issue be given by the local governing body.[10] If these alternative means are as reasonable and as workable as that of a property ownership requirement, the statutory limitation on the right to vote in *Cipriano* would be unconstitutional.[11]

But even assuming that there are no such reasonable and workable alternatives, the legislative determination is not necessarily conclusive. When the franchise is involved, the normal presumption in favor of the legislature is not as strong as it is in other cases. The Supreme Court has indicated more than once that "any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized."[12] *Harper* and subsequent voting rights cases established that statutorily imposed restrictions on voters run afoul of the equal protection clause if they are "irrational," "arbitrary," or "invidious"[13] or if they are not "reasonable in light of

8. Principal case at 827-28.

9. Shelton v. Tucker, 364 U.S. 479, 488 (1960); *see* Note, *Constitutional Law—Police Power—Michigan Statute Requiring Motorcyclists To Wear Protective Helmets Held Unconstitutional*, 67 MICH. L. REV. 360, 366-67 (1968). This principle is supported by the general rule, stated in People v. Armstrong, 73 Mich. 288, 41 N.W. 275 (1889), that the state may impose restraints on the individual only to the extent which is required or necessary for the protection of public health, safety, or welfare. This seems to imply that if a statutory restriction is not necessary or essential—that is if there is another method to the same end that does not infringe a fundamental right—the restriction is invalid. Note, *supra*, at 366 n.35.

10. *See* note 1 *supra*.

11. *See, e.g.*, Dean Milk Co. v. City of Madison, 340 U.S. 349 (1951), in which the Court stated that a municipality may not discriminate against interstate commerce, even in the exercise of its unquestioned power to protect the health and safety of its people, if reasonable nondiscriminary alternatives, adequate to conserve local interests, are available. *See also* Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 163 (Justice Frankfurter, concurring) (emphasis added):

> The precise nature of the interest that has been adversely affected, the manner in which this was done, the reasons for doing it, *the available alternatives to the procedure that was followed* . . . the balance of hurt complained of and good accomplished—these are some of the considerations that must enter into the judicial judgment.

12. Harper v. Virginia Bd. of Elections, 383 U.S. 663, 667 (1966) [quoting Reynolds v. Sims, 377 U.S. 533, 562 (1964)].

13. Avery v. Midland County, 390 U.S. 474, 484 (1968) (extending the principle of the apportionment cases to local government elections); Harper v. Virginia Bd. of Elections, 383 U.S. 663, 666, 668 (1966).

their purpose."[14] Thus, it is clear that state statutes that affect voting rights will be struck down despite the legislative presumption when they make invidious discriminations, are patently arbitrary, or are irrelevant to the achievement of the state's objective.[15]

Assuming that the courts will take a more active role in assessing legislative restrictions on the franchise, the task of determining whether voter qualification requirements are irrational, invidious, or unreasonable requires a careful evaluation of possible justifications on the basis of voting competence or interest in the election. Obviously, if neither justification appears to be particularly relevant to a given set of circumstances, the restriction is improper.[16] Thus, if the property ownership qualification applied in the principal case can be justified realistically on one of these bases, it would be constitutional and the *Cipriano* decision would be correct.[17]

One justification for a property ownership qualification on voting rights is based on the traditional idea that property ownership is related to voting competence.[18] The historical notion was that such a requirement would promote the intelligent and responsible use of the ballot. In colonial times, "property ownership and payment of taxes [were] the accepted symbols of community membership and interest."[19] Professor Galbraith has stated that "[i]n the New World, as in the Old, it was assumed that power be-

14. Carrington v. Rash, 380 U.S. 89, 93 (1965).

15. McGowan v. Maryland, 366 U.S. 420 (1961); Lassiter v. Northampton County Bd. of Elections, 360 U.S. 45, 50-51 (1959).

16. The court in *Cipriano* appeared to disagree with this analysis. It noted that the standards of voting competence and interest in the result were applicable only in general elections and that they did not apply to special elections such as the one in question. According to this argument, a voter qualification for a special election would not violate the equal protection clause even if it did not meet one of these standards. In proposing this principle, the court relied on Sailors v. Board of Educ., 387 U.S. 105 (1967), in which the scheme for selecting county school board members was challenged. In that case, local school boards were elected by popular vote of the residents of the district; no constitutional question was raised respecting those elections. The constitutional claim was based on the fact that the county board was chosen not by the electors of the county, but by delegates from the local boards, every local school board (irrespective of population, wealth, or other differences) having one vote. The Supreme Court ruled that this scheme was not inconsistent with equal protection and that municipalities could experiment in the selection of members of administrative agencies. The court in *Cipriano* found that the election to approve the issuance of bonds was not a general election but concerned only administrative functions of the municipality, and relied on the distinction made in *Sailors* to approve the property ownership requirement. However, the Court in *Sailors* indicated that "where a State provides for an election of a local official or agency—whether administrative, legislative, or judicial —the requirements of [equal protection] must be met . . . ." 387 U.S. at 111. Although it did not go on to decide what the requirements of equal protection would be if there were to be elections for county school board members, there is no apparent reason for the special-election standard to depart from the criteria applied to general elections.

17. *But see* notes 9 & 11 *supra* and accompanying text.

18. The court in the principal case relied primarily on this justification. Principal case at 827.

19. J. PHILLIPS, MUNICIPAL GOVERNMENT AND ADMINISTRATION IN AMERICA 175 (1960).

longed, as a right, to men who owned land. Democracy, in its modern meaning, began as a system which gave the suffrage to those who had proved their worth by acquiring real property and to no others."[20]

No state today has property qualifications for voting in general elections.[21] Professor Phillips has described the abandonment of such limitations:

> In time [however] leveling influences prevailed, and most Americans refused to accept the contention that there was a necessary relationship between property ownership or payment of taxes and interest in government or capacity to govern. North Carolina, in 1865, was the last state to abolish property ownership as a qualification for voting in state and national elections . . . .[22]

Moreover, even by the end of the 1950's, only a few states required property ownership for voting on bond issues or special assessments.[23] The unanimous abandonment of property ownership as a prerequisite for voting in general elections and its apparently infrequent use as a test for voting in special elections weaken the purely historical justification for its present-day use. The same sort of historical and traditional justification was rejected by the Supreme Court in *Harper* when it was used in defense of the poll tax. Dissenting in that case, Justice Harlan restated the argument:

> It is . . . arguable, indeed it was probably accepted as sound political theory by a large percentage of Americans through most of our history, that people with some property have a deeper stake in community affairs, and are consequently more responsible, more educated, more knowledgeable, more worthy of confidence, than those without means, and that the community and the Nation would be better managed if the franchise were restricted to such citizens.[24]

---

20. J. GALBRAITH, THE NEW INDUSTRIAL STATE 52 (1968).

21. XVII THE COUNCIL OF STATE GOVERNMENTS, THE BOOK OF THE STATES 1968-1969, 30 (1968).

22. J. PHILLIPS, *supra* note 19, at 175.

23. Carville v. McBride, 45 Nev. 305, 202 P. 802 (1922) (state constitution construed to permit cities to impose property requirements in local bond elections); LA. CONST. art. 14, § 14(a); LA. REV. STAT. §§ 33:4252, 33:4258 (1950) (*see* note 1 *supra*); MICH. CONST. art. 2, § 6 (tax-limit increase or bond issue); MONT. CONST. art. IX, § 2 [creation of levy, debt, or liability; construed to apply only to debts or liabilities to be retired by ad valorem taxes in Cottingham v. State Bd. of Examiners, 134 Mont. 1, 328 P.2d 907 (1958)]; NEV. REV. STAT. §§ 387.365-.395 (property owners' veto of approval of school bonds), 539.123 (irrigation district elections) (1967); N.M. CONST. art. IX, § 10 (county elections on borrowing), § 11 (school district elections on borrowing), § 12 (elections to increase municipal indebtedness); S.C. CODE ANN. § 23-62(4) (1962) (alternative to literacy requirement in all elections); TEX. CONST. art. 7, § 3 (certain school taxes), art. 9, §§ 4-9, 11 (certain hospital taxes), art. 16, § 59(c) (certain conservation district bonds); UTAH CONST. art. IV, § 7 (property ownership requirement permissive in elections to create indebtedness or to levy special taxes).

24. 383 U.S. at 685.

Nevertheless, the majority concluded that "[v]oter qualifications have no relation to wealth nor to paying . . . this or any other tax."[25]

Payment of a property tax, or property ownership, when employed as a device to promote the "intelligent" use of the ballot, is an anachronism. Today, there is no reason to believe that property ownership in any way enhances one's ability to exercise intelligent judgment in any election. Property owners are not necessarily better educated than others, and a literacy requirement would be a better device for measuring a potential voter's basic level of education or intelligence than would property ownership. Apart from considerations of education, there is no reason to believe that property owners are per se more responsible or more worthy of confidence than nonproperty owners. With increased mobility throughout our society—manifested especially by the large number of property owners employed by national public and private enterprises—it is by no means clear that property owners as a class have a greater stake in community affairs than those who do not own property.

However, in a case in which the election involves financing by increased property taxes, it might be argued that property owners would indeed be more likely to vote responsibly than those who do not own property. Nevertheless, when it is recognized that the property tax is generally not paid by property owners alone, but is often passed on to tenants,[26] this argument becomes questionable. Without the assumption that property owners alone pay the property tax, there is no fundamental difference between property owners and nonproperty owners that would make the former more likely to vote responsibly in such an election.[27] In short, it

25. 383 U.S. at 666. Whether or not the property tax qualification attacked in the principal case (as opposed to property ownership qualifications generally) is ipso facto unconstitutional by virtue of *Harper* is not clear, although such a conclusion is certainly within a literal reading of the words quoted in the text.

26. When the demand for rental housing is price inelastic, owners of such property will raise rents and pass on the increased tax promptly. D. NETZER, ECONOMICS OF THE PROPERTY TAX. 45-46 (1966). This would be the case especially with respect to multifamily units, owned and maintained for investment purposes; and this is the largest share of rental housing by property value. *See also* C. ADRIAN & C. PRESS, *supra* note 2, at 90: "Contrary to popular misunderstanding, a renter pays just as much in property taxes as an owner, although it is hidden in the rent."

27. There is some suggestion that while there is no economic difference between owners and lessees with respect to payment of property taxes, there may be a psychological difference. C. ADRIAN & C. PRESS, *supra* note 2, at 90. It may be true that property owners have a greater awareness of the burden of financing when the property tax is to be used to finance the improvement or expenditure authorized by an election. Nevertheless, the distinction is merely one of degree, and its magnitude cannot be demonstrated. Moreover, the common practice of landlords of justifying rent increases by virtue of increased property taxes weakens the claim that tenants are less aware of the relevant issues at stake in such an election. It should be noted, however, that the bond issue election in *Cipriano* did not present a case in which the property tax was to be used to finance the improvement. Principal case at 824; Judge Wisdom's dissent at 829; LA.

is impossible to find any significant connection between the ownership of real property and the ability to exercise the franchise intelligently and responsibly.[28] Consequently, any property qualification such as that in *Cipriano* seems to be irrational and arbitrary with respect to voting competence and the legislative presumption in favor of that qualification is thus overcome.[29]

The property ownership requirement might still be justified, however, if it serves to separate citizens with a substantial interest in the outcome of the election from those whose interest is not substantial.[30] If the outcome of an election affects property owners alone, or if it affects them to a substantially greater degree[31] than it does others, a property ownership qualification would not violate the equal protection clause.[32] But it is clear that when the issue at stake in an election affects all citizens in much the same manner and degree, restricting the class of voters to property owners is arbitrary and, therefore, unconstitutional.[33]

This type of analysis has been applied recently. In *Pierce v. Village of Ossining*,[34] a three-judge federal district court held that a restriction of the franchise to "owner[s] of property in the village assessed upon the last preceding assessment-role thereof"[35] was invalid. The issue at stake in the election was whether or not the village should change from a mayoral system to a village-manager system of government. In holding that this classification of voters was arbitrary and had no reasonable relation to proper qualifications for voting, the court declared:

> The proposition on which plaintiffs have been excluded from voting would work a fundamental change in the village government where they live. Whether that change should be made affects all who live in the Village so that denying the franchise to those who do not own real property is an invidious discrimination.[36]

CONST. art. 14, § 14(m). Consequently, any argument as to the greater responsibility of property owners by virtue of their financing of an improvement through the property tax, or their greater awareness of such financing, should have no bearing on the decision in the principal case. *See* text accompanying note 4 *infra*.

28. For a discussion of property ownership as a qualification on the right to hold elective town office and a conclusion that it is impermissible, *see* Landes v. Town of North Hempstead, 20 N.Y.2d 417, 421, 231 N.E.2d 120, 122, 284 N.Y.S.2d 441, 444, (1967). *But cf.* Schweitzer v. Plymouth City Clerk, 381 Mich. 485, 164 N.W.2d 35 (1969).

29. *See* notes 13-15 *supra* and accompanying text.

30. *See* note 5 *supra*.

31. *See* notes 43-45 *infra* and accompanying text.

32. *See* note 5 *supra*.

33. *Id.*

34. 292 F. Supp. 113 (S.D.N.Y. 1968) (unanimous decision by three-judge court).

35. N.Y. VILLAGE LAW § 4-402(b) (McKinney 1966).

36. 292 F. Supp. at 115. *But see* Croen v. Vetrano, 52 Misc. 2d 915, 277 N.Y.S.2d 354 (Sup. Ct. 1967) (sustaining a restriction on the right to vote in referenda on the question of incorporation of a village to owners of real property in the territory involved).

Thus, when all residents of a community have equal concern with an election issue, the fourteenth amendment demands that they have equal voice in the decision.

Conversely, when there is a substantial difference between the interests of various classes of persons and when a reasonable attempt is made to identify those classes which have a substantially greater interest in a particular election, the vote may be constitutionally denied to others.[37] In *Kramer v. Union Free School District No. 15*,[38] a resident of the defendant school district—a twenty-eight year old bachelor living in the home of his parents—launched a fourteenth amendment challenge against the provisions of the New York Education Law[39] which denied him the right to vote in school district elections. The statute provided that only residents who owned taxable real property, their spouses, lessees in the school district (but not their spouses),[40] and parents or guardians of children attending district schools had the right to vote in such elections. The majority of the three-judge federal district court found the statute valid as a reasonable attempt to limit the vote

> to those district residents who, [the legislature] believes, have a direct interest in the administration of the school system because they are either real estate taxpayers (or renters of taxable real estate) and thus carry the burden of paying for a major share of the services provided by the school districts, or because they are directly involved as parents of pupils attending the schools in question.[41]

The interests recognized in the statute as qualifying residents to vote are clearly relevant to the issues presented in the election—electing members to the school board, approval of the budget, and levying taxes on taxable real property in the district to meet the expenses for the coming year.[42] The classes enumerated in the statute have direct and substantial interests in those issues in addi-

37. *See* note 5 *supra* and accompanying text.

38. 282 F. Supp. 70 (E.D.N.Y. 1968) (2-1 decision), *prob. juris. noted*, 393 U.S. 818 (1968) (No. 258). The issue presented on appeal is whether N.Y. EDUC. LAW § 2012 (McKinney 1953) as applied to deny petitioner his right to vote in school district elections violates the equal protection clause or the first amendment as made applicable to the states by the fourteenth. The first amendment issue was not discussed by the lower court.

39. N.Y. EDUC. LAW § 2012 (McKinney 1953).

40. Since *Kramer*, the statute has been amended (effective June 16, 1968) to extend the vote to the spouse of "one who leases, hires or is in possession of a contract of purchase of, real property in such district liable to taxation for school purposes . . . ." N.Y. EDUC. LAW § 2012(3)(a) (McKinney 1969). The constitutionality of the former provision extending the vote to spouses of owners of taxable real property while denying it to spouses of lessees of such property seems doubtful. However, the question was not raised in *Kramer* since the plaintiff had no standing to represent spouses of lessees.

41. 282 F. Supp. at 73.

42. N.Y. EDUC. LAW §§ 2021, 2022 (McKinney 1953).

tion to the general interest—which is all that could be asserted by the plaintiff—in educational policy and in the schools as socio-cultural institutions. Although it cannot be said that the plaintiff was completely unaffected by or disinterested in the issues decided by the school district elections, the substantial difference between his interests and the interests of those eligible to vote indicates that the *Kramer* decision is a sound one.

Another type of election in which the right to vote might be constitutionally restricted to a certain class of citizens—in this case property owners—is a special assessment election on the issue of whether to construct public improvements affecting property in a specific area.[43] Special-assessment financing generally assumes that the property adjacent to certain types of public improvements receives special benefits from the improvements; therefore, it imposes the burden of paying for this kind of improvement upon the owners of adjacent parcels of land.[44] It might be reasonable to restrict the right to vote on whether to construct public projects financed in this way to the same group of property owners.[45] However, if people who did not own property—for example, lessees of real property that was to be specially assessed—were affected in substantially the same way, the property ownership qualification could still be held unconstitutional. It might be argued that although lessees do share to some degree in the benefits and burdens, their interests are not nearly so great as those of the property owners. Factors which might be said to cause this difference in interest are transiency and investment of the property owner in the community in terms of the length of his connection with it and his direct payment of taxes. However, it is doubtful that property ownership is an accurate measure of connection with the

43. Special assessments for public improvements are special charges imposed by law on land to defray the expenses in whole or in part of a local improvement on the theory that the owner of the property has received special benefits from the improvement over and above the benefits accruing to the community in general. *See, e.g.*, Fluckey v. City of Plymouth, 358 Mich. 447, 450, 100 N.W. 2d 486, 489 (1960); County of Westchester v. Town of Harrison, 201 Misc. 211, 215, 114 N.Y.S.2d 492, 497, (Sup. Ct. 1951). This is not to say that there are no benefits outside the group whose property is assessed, but that this group has benefited specially by the enhancement of their property.

No state statute authorizing such a special-assessment election could be found, such assessments normally being made by the local legislative body. *See, e.g.*, M. HOWARD, PRINCIPLES OF PUBLIC FINANCE 298-99 (1940); W. WINTER, THE SPECIAL ASSESSMENT TODAY WITH SPECIAL EMPHASIS ON THE MICHIGAN EXPERIENCE 67-68, 98 (Michigan Governmental Studies, No. 26, 1952). Hence, it is posed here as a hypothetical.

44. *See* note 43 *supra*.

45. Although it is difficult to conceive of a situation in which a municipal improvement in a particular neighborhood would not have some incidental effects on other residents or property in the city, merely incidental beneficiaries with a small and intangible interest need not be allowed to vote. *See* note 5 *supra* and text accompanying notes 37-41 *supra*.

community or concern with the special improvement.[46] It must be reiterated that often lessees effectively pay the property tax[47] and share the benefits of improvements such as improved sewers, wider streets, or community parks; thus, it appears that the interests of lessees and property owners are likely to be identical. Moreover, it may be unrealistic to expect a state or local legislative body to establish adequate guidelines which would take account of all possible variations in the comparative interests of the two classes of residents. It may be impractical, therefore, to attempt to restrict the lessees' franchise so that they can vote only when their interests are exactly equivalent to the interests of property owners. Furthermore, such a determination should not be left entirely to the courts since the establishment of voter qualifications has traditionally been a legislative concern. Thus, it appears that the best course, consistent with both practicality and the equal protection clause, is to extend the franchise to lessees and property owners whenever the interests of the two groups in the burdens and benefits at stake in an election are generally similar.

Although the three-judge federal district court in *Cipriano* did not consider this standard, the case appears to be wrongly de-

46. Transiency may indeed be relevant in determining the degree of one's interest in a public improvement, but the usual method of taking account of this factor is to use a residency requirement. It is more direct and does not encompass considerations which are irrelevant to the concern; consequently, it should be used if the goal is to limit the franchise to those who have a relationship to the community of significant duration.

It might also be argued that one's investment in the community is to be inferred from the length of his connection with it, but again residence would appear to be the relevant consideration rather than the fact of property ownership. *See* Shapiro v. Thompson, 37 U.S.L.W. 4333 (U.S. April 21, 1969). This case stresses the restriction which welfare residence requirements place on the right to travel freely within the United States, 37 U.S.L.W. at 4336-37. It could be argued that residence requirements imposed on the franchise in special assessment elections have a similar effect; however, it seems clear that there is a significant difference in the magnitude of the effect. Perhaps one's participation in civic affairs is more indicative of a concern about the community than any of the foregoing considerations; but there is no necessary relation between such participation and property ownership.

With respect to payment of taxes as a measure of one's investment in the community, both property owners and lessees pay taxes, including the property tax. *See* note 26 *supra* and accompanying text. Although there may be some difference in degree with respect to the latter, such differences are not easily measured since the lessee's payments are merged in his rent. Consequently, any distinctions between property owners and lessees based on differences in degree of payment of property taxes would be administratively impracticable.

There is a difference in investments in the community in that the tenant's rent does not buy a permanent interest in the property. Yet the significance of this difference for the question of the restriction of the vote in special assessment elections is not clear. Public improvements may indeed affect the value of property in either direction. Whether property values increase or decrease, the fact that they are affected makes it doubtful that property owners are in the best position to pass exclusive judgment on the wisdom or desirability of a public improvement that also affects others.

47. *See* note 26 *supra*.

cided when the standard is applied. Property owners have no greater interest in the bond issue election involved in that case than do those residents who do not own property in the community. All residents of the city would benefit in substantially the same way from the construction of the utility, and because the utility was not to be financed by property taxes,[48] property owners would bear no more burden than other residents. Since the burdens and benefits were equal for all, the question was essentially a general one involving the administration of city affairs. And because property owners were no more concerned with or affected by the outcome of the election than were other residents, the property ownership qualification was clearly inconsistent with the demands of equal protection and should be invalidated.

LABOR RELATIONS—Consumer Picketing Under Section 8(b)(4)(ii)(B) of the National Labor Relations Act—*Honolulu Typographical Union, No. 37, I.T.U., A.F.L.-C.I.O. v. NLRB**

When a dispute arose between a local of the International Typographical Union and a Honolulu newspaper, the union proceeded to picket several restaurants which advertised in that newspaper. The pickets carried signs and distributed handbills identifying the dispute and asking potential consumers of the restaurants not "to purchase . . . products advertised in the struck [newspaper]."[1] However, since the restaurants did not advertise individual products but claimed generally that they were good places to eat, the pickets' appeal was, in effect, a request to the public to avoid patronizing those restaurants. The picketed restaurants subsequently instituted proceedings before the National Labor Relations Board claiming that the picketing should be prohibited because it was a secondary boycott which violated section 8(b)(4)(ii)(B) of the National Labor Relations Act (NLRA).[2] The union argued that its actions con-

48. *See* note 27 *supra*.

* 401 F. 2d 952 (D.C. Cir. 1968) [hereinafter principal case].

1. Principal case at 954.

2. 29 U.S.C. § 158(b)(4)(ii)(B) (1964). This section provides in part:

> (b) It shall be an unfair labor practice for a labor organization or its agents—
> . . .
> (4) . . . (ii) to threaten, coerce, or restrain any person engaged in commerce or in an industry affecting commerce, where in either case an object thereof is—
> . . .
> (B) forcing or requiring any person to cease using, selling, handling, transporting or otherwise dealing in the products of any other producer, processor, or manufacturer, or to cease doing business with any other person . . .
> . . .
> . . .

stituted consumer picketing and that therefore they were protected under the United States Supreme Court's decision in *NLRB v. Fruit & Vegetable Packers Warehousemen, Local 760 (Tree Fruits)*.[3] The Board found that the picketing was a violation of the NLRA and issued a cease and desist order against further picketing by the union. The union appealed, and the Court of Appeals for the District of Columbia upheld the NLRB's finding and granted its cross-petition for enforcement of the cease and desist order. The court stated that the pickets' request was aimed at the restaurants' business in general and not at a specific product;[4] thus, the picketing was not protected by the *Tree Fruits* doctrine and was an illegal secondary boycott.[5]

The principal case is concerned generally with the problem of secondary activity by unions, and specifically with the application of a judicially created exception to the general prohibition against such activity. As originally written, section 8(b)(4) was intended to protect neutral employers from becoming involved in disputes between other employers and unions by prohibiting certain union activities.[6] Among the practices forbidden was the traditional secondary boycott which arises when a union in a dispute with a primary employer brings pressure to bear on other employers (secondary employers), through their employees, to cease doing business with the primary.[7] However, the statute did not seek to insulate the primary employer from this indirect pressure; rather, "the gravamen of a secondary boycott is that its sanctions bear, not upon the employer who alone is a party to the dispute, but upon some third party who has no concern in it."[8] In short, Congress intended to prevent those who were only tangentially related from becoming involved.

. . . [N]othing contained in such paragraph shall be construed to prohibit publicity, other than picketing, for the purpose of truthfully advising the public, including customers and members of a labor organization, that a product or products are produced by an employer with whom the labor organization has a primary dispute and are distributed by another employer, as long as such publicity does not have an effect of inducing any individual employed by any person other than the primary employer in the course of his employment to refuse to pick up, deliver, or transport any goods, or not to perform any services, at the employer engaged in such distribution . . . .

3. 377 U.S. 58 (1964). *See* text accompanying notes 13-15 *infra*.

4. Principal case at 954.

5. Principal case at 957.

6. As added by section 303(a) of the Labor Management Relations Act, ch. 120, § 303(a), 61 Stat., 158 (1947), section 8(b)(4) forbade a union to induce "employees of any employer to engage in, a strike or a concerted refusal in the course of their employment." For a discussion of the shortcomings of this approach to the problem of protecting neutral employers against secondary pressures by unions, *see* Aaron, *The Labor-Management Reporting and Disclosure Act of 1959*, 73 HARV. L. REV. 1086, 1112-13 (1960).

7. *See, e.g.*, Aaron, *supra* note 6.

8. International Bhd. of Elec. Workers, Local 501 v. NLRB, 181 F.2d 34, 37 (2d Cir. 1950) (Judge Learned Hand).

The language of the original section 8(b)(4) prohibited unions only from inducing "the employees" of a secondary employer.[9] This construction proved far too narrow, and in 1959, Congress sought to expand the scope of prohibited secondary activity by enacting section 8(b)(4)(ii)(B). This new provision makes it an unfair labor practice for a union "to threaten, coerce, or restrain *any person* engaged in commerce" if its objective is to force him to stop doing business with "any other person."[10] Obviously, this prohibitory language is very broad, but Congress did make a specific exception for truthful publicity, communicated by means *other than picketing*, designed to inform the public that a product of the primary employer is being distributed by secondary employers.[11] According to many commentators, section 8(b)(4)(ii)(B), when viewed in light of this proviso, is intended to operate as a complete ban on consumer picketing.[12] In their view, any attempt by the union to pressure a secondary employer by inducing his customers to stop doing business with him is illegal secondary activity under the NLRA. The effect of such secondary pressure is certainly similar to a union attempt to influence the primary by appealing to the secondary's work force. In both cases, the neutral employer is forced into a dispute which does not directly concern him.

Five years after the 1959 amendments, in *Tree Fruits*,[13] the Supreme Court declared that the ostensibly comprehensive prohibitions of section 8(b)(4)(ii)(B) do not forbid all consumer picketing. In that case, the union's dispute was with a producer of apples, but it chose to picket a retail supermarket which sold the apples as one of many items. The picketing was not specifically aimed at the retailer; it clearly identified the primary employer—the producer —as the union's target and asked only that the consumers refrain from purchasing his apples. The Court held that peaceful secondary picketing of retail stores was not prohibited by section 8(b)(4)(ii)(B) when its sole purpose was to ask consumers not to buy the primary employer's product.[14] The Court found that Congress intended to

9. *See* note 6 *supra*.

10. NLRA, § 8(b)(4)(ii)(B), 29 U.S.C. § 158(b)(4)(ii)(B) (1964). This section is reproduced in note 2 *supra*. *See* note 27 *infra*.

11. *Id.*

12. *E.g.*, Lewis, *Consumer Picketing and the Court—The Questionable Yield of Tree Fruits*, 49 MINN. L. REV. 479, 481 n.6 (1965). *See also* Cox, *The Landrum-Griffin Amendments to the N.L.R.A.*, 44 MINN. L. REV. 257, 274 1959; Aaron, *supra* note 6, at 1114-15.

13. NLRB v. Fruit & Vegetable Packers Warehousemen, Local 760, 377 U.S. 58 (1964).

14. 377 U.S. at 71. It would appear necessary to come within the standard established that the picket signs clearly identify the primary employer (both who he is and that he is the target) and ask only that consumers not buy *his* product. Such a test very closely approximates the language of the proviso to section 8(b)(4), which states that the union does not commit an unlawful secondary boycott if its actions amount only to "truthfully advising the public . . . that a product or products are

distinguish picketing which merely follows the struck product and attempts to persuade consumers not to buy it from picketing which is aimed at preventing all trade with the secondary employer. The majority opinion stated:

> When consumer picketing is employed only to persuade customers not to buy the struck product, the union's appeal is closely confined to the primary dispute. . . . On the other hand, when consumer picketing is employed to persuade customers not to trade at all with the secondary employer, the latter stops buying the struck product, not because of a falling demand, but in response to pressure designed to inflict injury on his business generally. In such a case, the union does more than merely follow the struck product; it creates a separate dispute with the secondary employer.[15]

In the Court's view, then, only that picketing aimed at preventing all trade with the secondary corresponds to the traditional secondary boycott proscribed by section 8(b)(4)(ii)(B).

Despite the Court's rationale in *Tree Fruits*, the decision is difficult to support as a matter of strict statutory interpretation; section 8(b)(4)(ii)(B) and its proviso seem to indicate that all consumer picketing is illegal.[16] In fact, the NLRB's opinion in *Tree Fruits* states that " 'by the literal wording of the proviso . . . as well as through the interpretative gloss placed thereon by its drafters, consumer picketing in front of a secondary establishment is prohibited.' "[17] Thus, the Board held that the picketing in question was illegal. The Board's holding, then, as well as the views of some commentators,[18] indicates that *Tree Fruits* must be regarded as a judicially created exception to the general rule against consumer picketing. Consequently, the decision should be narrowly construed to assure the continuing validity of the general rule.

The *Tree Fruits* case distinguished between picketing one of many products handled by a secondary—a partial boycott—and an attempt to prevent all trade with the secondary—a total boycott. This test is difficult to apply in factual contexts that differ from the situation in *Tree Fruits*. For instance, when the struck product encompasses all or a substantial part of the secondary's business ("one product" cases),[19] consumer picketing of the primary's product at the secondary's place of business may well produce the same pressures on

---

produced by an employer with whom the labor organization has a primary dispute and are distributed by another employer [as long as there are no effects on employees of anyone other than the primary in the course of their employment]."

15. 377 U.S. at 72.

16. *See* text accompanying note 12 *supra*.

17. Fruit & Vegetable Packers, Local 760, 132 N.L.R.B. 1172, 1177 (1961).

18. *See* note 6 *supra*.

19. That is, if he sells only one particular brand of gasoline or one type of car.

the secondary as would the traditional secondary boycott which section 8(b)(4) proscribes.[20]

The principal case presents a somewhat related problem. The picketed restaurants did not advertise a specific product in the struck newspaper; rather, they claimed that they were good places to eat. Picketing the advertised product, therefore, necessarily affected the secondary's entire business.[21] The court applied the *Tree Fruits* doctrine and found the total-partial boycott distinction to be crucial. Picketing, the court stated, is permissible when only a small part of the secondary's business is affected (as in *Tree Fruits*), but impermissible when the "picketing appeal to consumers is expanded to request a total boycott of the secondary seller . . . ."[22] In the latter situation, found to exist in the principal case, the picketing is illegal under section 8(b)(4)(ii)(B).

Although this conclusion is consistent with the *Tree Fruits* rationale, it ignores the conceptual problems involved with extending that rationale to cases in which intangible services rather than products are furnished by the primary. It is suggested that these conceptual problems might be solved by dividing consumer picketing situations into two basic types which could be called "chain" and "merger." *Tree Fruits* and the "one product" situations[23] are examples of chain cases.[24] The struck product of the primary passes to the retailer-secondary (perhaps through middlemen) unchanged. Consequently, it is relatively easy to visualize the product in question as that of the primary, although it is ultimately picketed at the secondary's place of business. The problem with chain cases then becomes one of deciding what portion of the secondary's business must be involved in order to make the picketing a violation under the *Tree Fruits* distinction between total and partial boycotts. This question, although vital for an effective application of the test, has not yet been answered by the Supreme Court.

Cases like the principal case, however, do not fit this chain con-

---

20. The court in the principal case expressly reserved opinion on the "one product" case. Principal case at 956 n.9. The *Tree Fruits* decision did not specifically discuss "one product" cases either. However, the effect in such a case of consumer picketing appears to be indistinguishable from the effect in the principal case. Both fact situations appear closely analogous to a total boycott of the secondary, which, under *Tree Fruits*, would be illegal.

21. The court in the principal case stated:

> [T]he picketing appeal to consumers not to buy "products advertised in the struck . . . [p]ress" was an attempt to cling to a legal concept evolved for another case even though the language patently does not fit the facts of this situation. The only realistic meaning of the appeal is the traditional "do not patronize this establishment.

Principal case at 954.

22. Principal case at 955.

23. *See* text accompanying note 20 *supra*.

24. There may be other chain cases involving more than one product picketed, but the analysis would be the same.

cept, because the product of the primary (intangible services) is not simply passed along to and sold by the secondary in the same form. The picketing, therefore, is not directed at the particular service in question—in the principal case the newspaper advertising—but at the products ultimately produced and sold by the secondary. In order to visualize the primary's product as the one being picketed, resort must be made to a concept such as merger. In the principal case, for instance, since advertising costs contribute to the cost of the secondary's product and ultimately to the price a diner pays for his meal, the advertising might be thought of as "merged" into the secondary's product.[25] The unions would undoubtedly argue that this merger of the primary's product into the secondary's is sufficient to identify the two so as to justify consumer picketing of the secondary's product. It is submitted, however, that such an argument should be rejected. Since the product of the secondary in merger cases is *substantially different* from that of the primary, permitting consumer picketing of the secondary's product does not accord with the *Tree Fruits* rationale. In these situations the union's appeal cannot be said to be "closely confined to the primary dispute." It also seems that this type of picketing "create[s] a separate dispute with the secondary employer."[26] Moreover, in merger cases, since picketing the primary's contribution means picketing the *entire* product sold by the secondary, the appeal of the pickets is aimed directly at the secondary's total business. Therefore, the picketing becomes, in effect, a total boycott of the secondary which, under *Tree Fruits,* clearly violates section 8(b)(4)(ii)(B). At least one recent Board decision is in accord with this analysis.[27]

25. Examples of "merger" cases, in addition to the advertising situation, would be cases in which the primary provided some intangible service or component part that contributed to what the secondary ultimately sold to his customers. For an example of an intangible service other than advertising, *see* Laundry, Dry Cleaning & Dye House Workers International Union, Local 259, 1967 CCH NLRB Dec. ¶ 21,328. *See also* note 27 *infra.*

An example of a component parts type of merger case is Twin City Carpenters District Council & Boot & Shoe Workers Union, Local 527-C, AFL-CIO, 167 N.L.R.B. No. 51, 1968-1 CCH NLRB Dec. ¶ 21,858 (1968). In that case, the union picketed a builder and seller of houses advising that the cabinets being used in the houses were not made by union members, but failing to name the cabinetmaker at whom the pickets were directed. The Board found this activity to be a coercive attempt to get the builder to stop dealing with the cabinetmaker.

26. NLRB v. Fruit & Vegetable Packers Warehousemen, Local 760 (Tree Fruits), 377 U.S. 58, 72 (1964). *See* text accompanying note 15 *supra.*

27. In Laundry, Dry Cleaning & Dye House Workers Intl. Union, Local 259, 1967 CCH NLRB Dec. ¶ 21,328 (1967) the union picketed a restaurant that used a linen service supplied by a laundry with which the union was engaged in a dispute. The restaurant did not sell linen service to its customers, but merely used it in its operations. The Board found that there was not sufficient identification between the picketing and either a primary product or primary employer to render the picketing permissible as an attempt to persuade consumers not to buy a struck product. *See also* Twin Cities Carpenters Dist. Council & Boot & Shoe Workers, Local 527-C, AFL-CIO, 167 N.L.R.B. No. 51, 1968-1 CCH NLRB Dec. ¶ 21,858 (1968).

Under the approach presented above, the *Tree Fruits* rationale might be stated as follows: consumer picketing which acts exclusively on the demand for a struck product of the primary and which does not affect either any other part of the secondary's business or so much of his business as to be a threat to its continuance is not a secondary boycott for purposes of section 8(b)(4). If there are any coercive effects in such chain situations, they are merely incidental or insubstantial. On the other hand, in merger cases it is impossible to act exclusively on the demand for the primary's product without disturbing other business of the secondary. Therefore, in such situations the basic evil of the traditional secondary boycott—pressuring the secondary into a complete cessation of business with the primary—is likely to occur. It is this difference which suggests that the *Tree Fruits* exception should not be extended to merger cases. The principal case recognizes this approach.

The court in the principal case suggested another possible test for determining the legality of consumer picketing. According to that test, the determination would turn on whether the union's picketing subjects the secondary employer to greater pressure or disruption than he would suffer from a successful strike against the primary.[28] In the chain cases, assuming a successful strike against the primary, the unavailability of the primary's product because of that strike would have substantially the same effect as a successful appeal to consumers—the secondary would be unable to sell any of the struck product.[29] In such cases, consumer picketing of the primary's product at the secondary's place of business should be allowed. On the other hand, in the "merger" cases, picketing the secondary would have a substantially greater effect on him than would a strike against the primary. On the facts of the principal case, for example, a successful strike against the newspaper would merely extinguish one source of advertising services and might therefore have little impact on the demand of the secondary's customers for his meals. However, if the union were allowed to picket the advertised product, the secondary would be subjected to much greater pressure affecting his entire business. In the event of a strike, the secondary could merely change advertising outlets, while if picketed he would bear

28. This test was suggested earlier by Lesnick, *The Gravamen of the Secondary Boycott*, 62 COLUM. L. REV. 1363, 1412 (1962). Although Professor Lesnick's focus is limited to "common situs," "roving suits," and "reserved gate" problems, the distinction he suggests seems no less appropriate in determining when secondary picketing should constitute a violation of section 8(b)(4)(ii)(B). Carried to its logical conclusion, however, this test would seem to permit consumer picketing in the total boycott situation when the secondary sells only the struck product (the "one product" case). This demonstrates the weakness of the suggested test and indicates that the "merger" theory would be preferable.

29. Of course, he might get a similar product elsewhere and, therefore, lose nothing.

a considerable risk of losing business. Accordingly, in merger cases consumer picketing of the secondary should be disallowed.

The result in the principal case can be supported on several grounds, as discussed above. It is suggested that the merger-chain analysis is preferable since it eliminates automatically any need to consider the application of *Tree Fruits* once the merger label is attached. But, helpful as this categorization is, it is not a panacea for solving the problems of determining when consumer picketing violates section 8(b)(4). As chain cases approach the one product situation, a difficult line-drawing task awaits the Board and the courts.

RECENT BOOKS

Book Reviews

MR. JUSTICE MURPHY, A POLITICAL BIOGRAPHY. By *J. Woodford Howard.* Princeton, N.J.: Princeton University Press. 1968. Pp. x, 578. $12.50.

Dramatically and unexpectedly, Frank Murphy learned within hours of the death of his predecessor, Justice Pierce Butler, that he would be appointed to the Supreme Court of the United States. On that day, November 16, 1939, there had been a Cabinet meeting at the White House. Desiring to speak privately with President Roosevelt about several routine matters, Attorney General Murphy stayed behind after most of the other Cabinet members departed. In the midst of this discussion with the President, the following episode took place, as described in Murphy's own handwritten notes:

> The Assistant Secretary of Commerce was in the room at the time. He stood looking out the window at the far end of the Cabinet Room. I had drawn a chair—the Secretary of State's chair—near the President's right side. He was in his chair at the head of the table.
>
> In the midst of our chat and when Noble wasn't looking he reached over and whispered in my ear "Do you appreciate the significance of what happened this morning—Justice Butler's death?" In a sense I did but did not want to assume that my name would be considered so I remained silent. Without a moment's delay he now leaned back in his chair and with a handsome grin on his face he chucked his arm full length at me, index finger pointing just under the head of the table over against my arm and whispered "You, you!" I was bewildered not only that he had so briefly come to a conclusion on the subject but also, despite the fact that I am fully aware of his love of surprises, that he would announce it to me in this fashion. "It begins to look like it," he added.
>
> I quietly said to him, "Mr. President, I am of course at your service but expect you to do only what is in the best interest of the Country." Beyond this, I said nothing. I did not indicate that I hoped it was true, that I was pleased with it or that I would reject it. "Think it over for a week and then we will have a visit about it."
>
> My thoughts were not settled on the subject for I honestly knew he could make a better choice for the Supreme Court than myself. My long years of training have made me to a degree proficient and very fond of administrative work. Reform and modernization of government, [and] the selection of discriminating personnel attracted me mightily and for these and other reasons I believe I could serve the nation better off the Court than on it. Be that as it may a Supreme Court Justice was born in the informal and boylike performance recited above. He was in glee throughout the brief episode.

> He loves with some sort of gleeful passion deflating an important and solemn occasion into a normal affair.

Thus was born a Court appointment that was to span more than nine years, an appointment that brought to the Court a man whose judicial talents were both unique and controversial. J. Woodford Howard, professor of political science at Johns Hopkins University, has sought in this "political biography" to bring meaning and understanding to the judicial career of Frank Murphy. And he has done so with the postulate of Jerome Frank in mind:

> The ultimately important influence in the decisions of any judge are the most obscure . . . . They are tied up with intimate experiences which no biographer, however sedulous, is likely to ferret out, and the emotional significance of which no one but the judge, or a psychologist in the closest contact with him, could comprehend . . . . For in the last push, a judge's decisions are the outcome of his entire life history.[1]

While not a psychologist and never an acquaintance of Justice Murphy, Professor Howard has managed to draw a most perceptive and realistic portrait of the Justice. He has come as close as possible, at least for an outside observer, to comprehending the emotional significance of the events in Murphy's life that influenced his work on the Court. This is no hasty tract or superficial biography. It represents thorough research and mature reflection covering more than a decade, starting with the author's doctoral thesis at Princeton under Mason.[2] And he has had the advantage of examining the recently available papers of the Justice, including those of the Court tenure.

The story of Frank Murphy, as sketched by Professor Howard, "resolves itself into an impressive unity . . . a life of unwavering defense of human rights" (p. 496). As a public prosecutor and criminal court judge, as Mayor of Detroit, Governor-General of the Philippines, Governor of Michigan, and then as Attorney General of the United States, Frank Murphy exhibited an amazing consistency of purpose and action in the civil rights arenas. He was an activist in his complete and uncompromising dedication to the basic democratic ideals that most Americans profess but so often ignore. And he brought that activism, that dedication, to his role as Associate Justice of the Supreme Court.

Therein lies the key to the enigma of Frank Murphy—a key that serves to explain a great deal about what have been described as his strengths and his weaknesses as a Justice. During the 1940's, the period of Murphy's service on the bench, the Court was confronted with two

---

1. LAW AND THE MODERN MIND 114-15 (1930).
2. Howard, Frank Murphy: A Liberal's Creed (unpublished doctoral thesis in the Princeton University Library, Department of Politics, Feb. 1959).

major types of civil liberties problems: (1) those generated by wartime controls and restrictions; and (2) those emanating from the awakening of the legal system to the need for greater constitutional and judicial protection of basic human rights. To those tasks, Justice Murphy brought a full measure of understanding and insight. In forceful and colorful language, he gave voice to the libertarian idealism that underlies the Bill of Rights and that came into greater prominence in the subsequent years of the Warren Court. Seldom has the judicial and public conscience of the nation been so eloquently expressed than in the opinions of Murphy during this period, opinions that for the most part were dissenting from or concurring with the results reached by the Court majorities.[3]

So complete was Murphy's commitment to Christian morality and democratic principles that he sometimes appeared to overplay his hand, thereby causing much of his conventional work on the Court to be overshadowed and little appreciated. As Professor Howard has noted, "The essential fact to be grasped about Murphy is that, while he was capable of functioning in conventional terms and did so more often than not, he *chose* different tactics when battling for principles he felt most deeply" (p. 478). From his earlier experiences in public life, Murphy brought to the Court a fighting, evangelical, and emotional approach to civil liberties. It was an approach that sometimes translated complex problems to simpler moral terms and allowed few procedural niceties to stand in the way of giving vent to vigorous constitutional condemnations.

As a result, Justice Murphy completely antagonized those who profess that the legal system is simply a process of calm objective discovery of pre-ordained and immutable principles. He appeared to some observers to use his seat on the Court as a pulpit from which, to use the words of Felix Frankfurter, " 'he exercised the compassionate privileges of a priest when in fact he was only a judge' " (p. 480). He became known as a "lawless" judge who confused the "law" with his own notions of compassion and morality.

Such denigrating comments, perpetuated and echoed throughout the two decades since Murphy's death in 1949, do not find their ultimate refutation in any re-evaluation of Murphy's opinions or in a defense of his vanity or the other personal idiosyncrasies that obviously annoyed some of his fellow men. Rather, that refutation is to be found in the growing recognition that the Supreme Court, in many of its functions, is necessarily a political institution that is

3. *See, e.g.*, In re Yamashita, 327 U.S. 1, 26 (1946); Korematsu v. United States, 323 U.S. 214, 233 (1946); Bridges v. Wixon, 326 U.S. 135, 157 (1945); Steele v. Louisville & Nashville R. Co., 323 U.S. 192, 208 (1944); Falbo v. United States, 320 U.S. 549, 555 (1944); Hirabayashi v. United States, 320 U.S. 81, 109 (1943).

forced to play an activist role in the development of certain constitutional doctrines, whether they be the federalist doctrines of the Marshall Court or the reapportionment concepts of the Warren Court. The Court is something more than an arbiter of conflicting views among lower courts as to the proper interpretation of a tax or jurisdictional statute; it is something more than a vehicle for resolving legal problems through the use of legal logic or the correlation of past precedents. The Supreme Court is also a unique and human institution designed to forge and expand our basic legal and constitutional doctrines to meet men's needs. In so acting, the Court and its members must perforce reflect and apply, in the context of cases and controversies, some of the fundamental notions of public and historical morality.

A natural part of the Court's function in these respects is the individual expression of views by the Justices. Confronted from time to time with some of the most controversial and significant of our nation's social problems, Justices who hold strong views about the legal or constitutional implications of those problems have consistently given expression to their views. On occasion those views can be contained within the limited bounds of a majority opinion. More often, strong views can best and most effectively be set forth in concurring and dissenting opinions. Frank Murphy was thus no pariah in utilizing such means to voice his abhorrence of what he conceived to be invasions of personal freedom. He was not the first nor the last to use his seat on the Court as a "pulpit" to preach his notions of constitutional freedom.

History will doubtless judge Frank Murphy not as a lawless innovator of personalized views but as a dramatic expositor of constitutional ideals. He had an established right to express those views and he will ultimately be judged by the intrinsic merit of what he had to say, rather than by the mere fact or manner of expression. History will also judge him on the merits of his conventional but nonetheless significant contributions to other aspects of the Court's role in the judicial system. Such in-depth studies of the man as that by Professor Howard make it possible for history to make its judgment dispassionately and with all the relevant facts revealed.

When President Roosevelt whispered "You, you" in Frank Murphy's ear on that day in November of 1939 he was perhaps creating a judicial figure of greater stature and more enduring qualities than either could then foresee. Certainly Justice Murphy's final place in judicial history will be more important and significant than that assigned to him by those who cry that he misconceived his function with that of God. The ultimate truths that time alone can establish may well prove that much of what Justice Murphy

so eloquently stated in the 1940's had meaning not only for that period but for all of our constitutional time.

Eugene Gressman,
Member of the Washington, D.C., Bar and former clerk to Justice Murphy.

RIGHTS OF THE PERSON. By *Bernard Schwartz.* New York: Macmillan. 1968. Pp. xi, 1018 (2 vols.) $25.

The publication of *Rights of the Person* marks the completion of Professor Bernard Schwartz's magnum opus, his commentary on the Constitution of the United States.[1] Appropriately enough, these final two volumes focus upon the most recent preoccupations in constitutional law.

Rights of the Person canvasses the hotly contested battlegrounds of constitutional adjudication in our generation: the controversies concerning the position of radical politics in a nation fearful of its security, the meaning of equality for a long-suppressed racial minority, the role of the police and the uses of the criminal process, the position of religion in education and in public life, and the essential institutions of politics itself. Merely to list these issues suggests the difficulty of presenting them meaningfully within the confines of a comprehensive survey. Within the past two decades each of them has become a recognized specialty of scholarship, possessing its own vast literature of historical research, logic-chopping casuistry, contentious propaganda, behavioral impact studies, philosophical punditry about the merits or about the judicial role, and so forth—a torrent of learning in which even the specialist can only hope to paddle his own canoe without capsizing in the rapids. Surely no legal institution has ever been the subject of such continuous observation, analysis, and comment as the United States Supreme Court and its constitutional jurisprudence.

Thus, it is understandable that one picks up an all-embracing review of the Constitution with skeptical curiosity. The appearance of these latest volumes was peculiarly timely in 1968—a year that signaled a major shift in the nation's political mood, marked by the impending end of the "Warren Court" and a revolt against its works in a historical fight over the successor to the Chief Justice. The time

1. A COMMENTARY ON THE CONSTITUTION OF THE UNITED STATES. Part I appeared in two volumes in 1963, under the title THE POWERS OF GOVERNMENT, Part II in one volume, THE RIGHTS OF PROPERTY, in 1965.

may well be ripe for stock-taking, for consolidating some theoretical positions, whether or not the changing of the guard brings a slowing or reversal of the flow of innovation. Still, a general commentary on constitutional "rights of the person" seems at first blush an impossible undertaking. The issues at stake are as ancient as the earliest articulated concerns of civilization, and more universal than the membership of the United Nations. They are timeless themes of philosophy and literature, and they are the daily grist of politics and litigation. An exposition of these issues under our Constitution can be presented as a study in historical evolution, as the ultimate challenge to the contest of reason this country uniquely entrusts to lawyers, or as a grand procession of classic dilemmas—the antinomy which Cardozo stated rather than resolved in his phrase about "ordered liberty." To understand the scope of any guarantee stated in the Constitution, we want to examine its historical origins, the verbal choices its text offers to exegesis, the rhetoric of claims and counterclaims in which it appears, and the social context in which these claims once had, now have, or may someday have validity. To do one of these things well practically excludes doing the others within any reasonable compass, as anyone who teaches constitutional law has learned to his frustration. To undertake a synthesis of these diverse approaches and to apply it to the Constitution as a whole is an impressive ambition.

Fortunately, Professor Schwartz did not let himself be deterred by the false choices of whether to write another history of constitutional adjudications in the Supreme Court, or a philosophical disquisition on human rights, or an annotated encyclopedia of leading cases. These volumes repeat none of these particular forms. Rather, they borrow from each; none is missing entirely, but none is wholly dominant. In less capable hands, so eclectic an approach might produce a disaster of uncritical generalities and superficial popularization. This author's erudition maintains a notable depth of scholarship for the breadth of the topics covered. His books represent a highly personal combination of ingredients. They are a commentary, as they purport to be, but they are also a solidly professional work.

Of course, any choice of ingredients put into the combination creates problems. Commendably, *Rights of the Person* is a commentary on the Constitution, not on the Supreme Court. Too often legal scholarship forgets the difference, or assumes that the Constitution is *only* what the Supreme Court says it is. Professor Schwartz does not enter at length into the learned debates of the Court watchers that stir the academic world. Nevertheless, these books do not, nor could they, often venture beyond the Constitution as law to consider it in action outside courts; for instance, these volumes do not deal with the Constitution as a factor in legislative debate and executive messages, or as a still powerful appeal in public

rhetoric, or as the ultimate touchstone of ideological legitimacy in America. *Rights of the Person* remains a commentary on constitutional *law*, though free of the technical constraints of a legal treatise. Thus, the author illuminates his exposition with frequent judicial quotations without strict concern for the immediate use of the quoted statement in a majority opinion, dissent, or extra-judicial essay, or for its place in an on-going contest of ideas with a competing philosophy. And in finding illustrative examples in cases from many courts, he risks misleading the unwary or nonprofessional reader about the relative weights of citations. In particular, the decisions of state courts on federal constitutional rights, although indisputably a part of our constitutional reality, are still a most unreliable guide to authoritative constitutional law. In a book that undertakes to combine extensive description, accurate exposition, and independent evaluation, these divergent uses of the sources must be kept clear in the reader's mind.

Of course, many pages of exposition also can present only familiar material, without containing any surprising information or novel insights for anyone who is acquainted with constitutional law. That is an unavoidable cost of comprehensiveness; one who undertakes to be encyclopedic cannot be expected to be continuously profound.

What of the substance of Professor Schwartz's Constitution? Much is implicit in the very title of these two volumes. *Rights of the Person* avoids the risk of becoming a mere annotation of the separate clauses as they appear in the Constitution in favor of grouping the constitutional safeguards into "rights" that are related by the interest protected, not by the usual circumstances of their invasion. Thus the protections of personal security through the stages of the criminal or administrative process, from arrest, bail, and fair trial, to habeas corpus, double jeopardy, and legislative attainder, are collected under the heading *Sanctity of the Person* (ch. 15). The next chapter, on privacy, covers conventional searches and inspections as well as electronic surveillance for both criminal and administrative purposes. This discussion is followed by chapters on freedom of expression, the equality principle, and religion. But the fifth amendment privilege against self-incrimination—including the problem of coerced confessions—and the prohibition against cruel or unusual punishments are separated from the rest of criminal procedure and presented along with citizenship and nationality law in a final chapter on *Dignity of the Person*. Here, too, we find the closely circumscribed law of treason, far separated from the other constitutional doctrines which have developed in response to the governmental pursuit of "subversion" that gives us its modern functional equivalent.

The gain in focus and readability achieved by this organization

carries a price. Professor Schwartz has introduced an unacknowledged bias toward seeing the "rights" discussed as something apart from the constitutional text that attempted, so far as the foresight and the language of 1789 and 1866 would permit, to give them legal expression—a form of analysis one would consider a throwback to the "higher law," but for the fact that *Griswold*[2] commands caution in dismissing the recurrence of "natural rights." This bias might have been counterbalanced by inserting reminders, in discussions of the case law, of the constitutional words before the judges for interpretation. But perhaps the implicit "natural rights" flavor is, if not deliberate, at least not uncongenial to the author's thinking. As a matter of fact, this may be as good a place as any to mention—though it seems unbelievable—that I could not find the text of the Constitution of the United States printed anywhere in these two volumes of commentary on that Constitution.

On the substance of the issues, the author's positions defy the Procrustean categories of "liberal," "conservative," "activist," "abstentionist," or whatever. He is emphatic on the importance of enforcing procedural guarantees against government agents of all kinds, in the investigatory as well as in the trial process. A striking contribution, because the problem is so often ignored in the mainstream of the alien and the immigrant, particularly with respect to entry and deportation; these two emphases join, for instance, in a critique of *Abel v. United States*.[3] On the other hand, Professor Schwartz is satisfied to leave wiretapping policy to Congress; and his reasonable apprehension of the irrational and destructive force of mobs, direct action, and organized extremism (he refers more than once to the experience of the Weimar Republic) allows him little sympathy for the constitutional claims of those engaged in picketing and other forms of demonstration, door-to-door canvassing, civil disobedience, group libel, or communism.

The treatment of the first amendment, though painstaking, largely recapitulates conventional wisdom. The author scornfully dismisses the debate on whether the free speech clause states an "absolute" by viewing, and refuting, the claim as one of an "absolute" *right* of speech regardless of circumstances. This analysis is consistent with his own approach, but it fails to examine the more plausible claim that the amendment states an absolute prohibition against any restraints directed *in terms* against speech. Yet we might have been spared much if that approach had been developed in *Gitlow*[4] and after; if it had confined the clear-and-present-danger test (or later versions of it) to the restraint of speech under nonspeech laws, where

2. Griswold v. Connecticut, 381 U.S. 479 (1965).
3. 362 U.S. 217 (1960).
4. Gitlow v. New York, 268 U.S. 652 (1925).

it originated, and had prevented the extension of that test to controls expressly directed at speech rather than deferring to a supposed governmental predetermination of the constitutional necessities.

Moreover, the author's first amendment analysis is obfuscated by a curiously old-fashioned conception of "the police power," as though this were some kind of affirmative grant of a defined authority instead of a name for the residue of all plenary power that is not constitutionally denied to state government. Thus he attempts to explain why, though the first amendment protects only the verbal element in speech, wearing "freedom buttons" is a privileged form of protest but hanging rags on a clothesline is not: the police power can reach the latter but not the former (pp. 396-97). These analytical tools prove equally inadequate in the commentary on obscenity, in Professor Schwartz's jurisprudence as in Justice Brennan's; the discussion begins with the "simple proposition" that the police power includes the *power* to protect public morals, therefore it plainly encompasses the *power* to protect the public against obscenity (p. 314). As this formulation indicates, the search for a "power" before examining a claimed constitutional limitation prejudices the latter. Of course the search is illusory; unlike the Federal Constitution, state constitutions do not grant or delegate lists of powers any more than do the national constitutions of unitary states or the British constitution. But the method of analysis implies the possibility of a "lack of power" *antecedent* to the first amendment claim—a theory for which there can be no federal constitutional source save a reversion to generalized substantive due process. And the needless finding of "power," which focuses on the case *for* control, will likely prejudge the real question of constitutional limitation, which focuses on the case *against* control.[5]

There is another drawback implicit in using the terminology of "rights" of persons rather than that of constitutional limitations on government: it obscures rather than highlights one of the most interesting current phenomena in constitutional law. This is the impending shift from ancient demands for limitations on a govern-

5. If the cited illustrations of the "freedom buttons" and the clothesline display, for example, are to be distinguished by delimiting the reach of a "power" and not only the reach of the first amendment's limitations, then a finding that the "power" falls short would logically apply also to wearing similar buttons without a "freedom" or any other message—that is, it would support a "right" that could not be founded on the first amendment and, by the hypothesis of a prior search for "police power," need not be. These premises create trouble for the analysis of our most recent claims of right in dress, hair styles, and the like (p. 396). They similarly confuse the deduction of the constitutional status of obscenity from the power of the Court of King's Bench to punish Sir Charles Sedley for "making water on the persons below" from a balcony in Covent Garden (p. 314). One would confidently assume that this would not give rise to a first amendment claim even by today's more advanced theoreticians—despite reports of some disputed emission from a hotel window during last summer's political discussions in Chicago.

ment of circumscribed functions to modern demands for affirmative action from a pervasive government. As an eminent comparativist, Professor Schwartz knows the different history, style, and role of the power-limiting Bill of Rights and the concept of judicial review in the Anglo-American tradition, as contrasted with the programmatic social assertions which the Continental tradition enshrines in constitutions as the highest political symbols of past victories and present commitments. When constitutions of the latter tradition assert a right to health, to welfare, to education, to employment, to a fair share of the nation's material goods, they create a standard for the political performance of government that is no more sought to be enforced in courts than is the preamble of the Constitution of the United States. In the present commentary, the author recognizes that similar claims are being pursued at the frontiers of constitutional litigation under the Bill of Rights and the fourteenth amendment; it would have added clarity if this development had been displayed, and if the difficulty of deriving such political claims from what are historically and textually *restraints* on government had been discussed, uncluttered by the ambiguity of "rights."

But if much of the book's wisdom is conventional, it is so from conviction and not from failure to recognize the troublesome questions. The conclusions are stated reasonably, without shouting or preaching. The style matches the content. Much of it necessarily is a parade of declarative sentences reciting holdings and citations, enlivened by an occasional retelling of some significant case. The author is an indefatigable collector of quotations from historic and literary as well as legal sources, but these quotations are scattered through the text as grace notes rather than for the relevance of the source. The subject of constitutional rights is rife with temptation to pontificate in orotund generalities and indisputable abstractions, and sometimes those drawn from Supreme Court Justices and those of the author tend to merge into one another. The chapter titles are forced into an awkward parellelism of "rights"—*Sanctity of the Person, Privacy of the Person, Expression of the Person, Equality of the Person, Belief of the Person,* and *Dignity of the Person*—and these capitalized titles are then used in the text as if they were established terms of constitutional law. The style also suffers from alternating the editorial "we" with abuse of the passive voice ("It is felt," "it has been pointed out"), which sometimes leaves the source in doubt. The most irritating quirk, however, is the author's undeviating misuse of "such" for "this" or "the," paragraph after unrelenting paragraph, until one is distracted from the substance to search for even one "this." Such kind of editing ought to be one modest service a publisher extends to an author and his readers.

Despite its shortcomings, the completed work adds up to an im-

pressive accomplishment. It is a detailed inventory of American constitutional rights as they exist two thirds of the way through the twentieth century. The picture it presents is that of a mature legal system, hedging the application of power to the individual by procedures evolved over centuries of English and American history and by a few substantive axioms with which men of good will seek to umpire the many collisions between the claims of government and of individuals in a complex modern society.

Such an inventory largely submerges the original excitement of clashing principles in a judicious review of working compromises. But the reasonable judgments of judicious men—as lawmakers, judges, or academic commentators—do not exhaust the function of these principles. The protections against authority that law promises the individual are always unfinished business. Their classic statement in the Constitution permits the perennial questions always to be reopened: whether this Constitution does not pledge the society it governs to be even more free, committed to tolerating even hostile heresy and offense to good taste, committed to trusting in its survival even without elaborate structures of secrecy and surveillance to protect it. In the nature of things, such questions will long be pressed only as minority views, in dissent on and off the Supreme Court. They are not then "constitutional law." We knew, when we studied the Constitution in the post-war years, that it did not forbid racial segregation, or prosecutions based on illegally obtained evidence, or the malapportionment of legislatures. Today there are other claims that are not constitutional law. But even if some minority views never become "constitutional law," it is nonetheless important that those who assert them are appealing *to* the Constitution of the United States—not *against* it.

Although Professor Schwartz stays close to prevailing doctrine both in his presentation of "the law" and in his own preferences he knows that his commentary necessarily speaks from its own time, and he indicates where some of the known constitutional frontiers in our time are. Whatever may lie beyond those, his work will have lasting value in telling the future where the Rights of the Person stood in the United States of 1968.

Hans A. Linde,
Professor of Law,
University of Oregon

SECURITIES REGULATION: CASES AND MATERIALS (2d ed.). By *Richard W. Jennings* and *Harold Marsh, Jr.* Mineola, N.Y.: Foundation Press. 1968. Pp. xxxv, 1261. $15.

Thirty-six years after the passage of the Securities Act of 1933, the first of the federal statutes, it is almost unbelievable how rapidly the subject of securities regulation is still changing in some areas and how slowly in other areas. The elapsed time is important because it means that the 1933 Act is more than half as old as the onset of modern times, which can be dated for this purpose from the beginning of mass production of the automobile and other consumer goods at the turn of the century. This statute was one of the achievements of the first hundred days of Franklin D. Roosevelt's first term, a period that marked the assumption of an active role for the federal government in stimulating the economy, controlling financial affairs, and promoting public welfare. Today, securities regulation has become a substantial portion of the content of corporation law.

Just as Professor Loss' treatise[1] is the almost indispensable book for the study of securities regulation in the law office, the Jennings and Marsh casebook is the almost indispensable volume for the study of this topic in the classroom.[2] Thus, we may welcome the appearance of an improved and updated second edition.[3]

The editors have provided compilation of really necessary working data for a "cases-and-materials" student book. The text includes many of the important SEC interpretative releases. On occasion they could have chosen different cases—for example, I would have preferred the leading "first *Hughes* case"[4] and the "second *Hughes* case"[5] both of which announce doctrines, rather than some of the later follow-up decisions, in which the basic doctrine is never clearly stated. But these are matters of judgment, and on the whole the selection is clearly right and provides the indispensable cases.

---

1. L. LOSS, SECURITIES REGULATION (2d ed. 1961) (3 vols.).

2. The only rival casebook seems to be H. BLOOMENTHAL, SECURITIES LAW (1966). This book has undeniable merits, but one may comment that it is heavily weighted toward matters which reflect its author's Western and enforcement experience, and that it is one of the most discouraging layout jobs ever produced by a printer.

Professor Loss also has a one volume edition designated "Temporary Student Edition," but this is in no sense an abbreviated form of the monumental treatise. While whole chapters of the treatise are left out, the chapters which are included appear without abbreviation or even repaging; therefore, by reason of its tremendous detail this edition is just as difficult for student use as his three-volume treatise.

3. R. JENNINGS & H. MARSH, SECURITIES REGULATION: CASES AND MATERIALS (2d ed. 1968).

4. Charles Hughes & Co. v. SEC, 139 F.2d 434 (2d Cir. 1943), *cert. denied*, 321 U.S. 786 (1944) (the first judicial recognition of the "shingle theory").

5. Hughes v. SEC, 174 F.2d 969 (D.C. Cir. 1949) (the first judicial formulation of the fiduciary theory).

The editors were lucky enough to catch the *BarChris* case;[6] unlucky enough to close the book too early for the Second Circuit's opinion in *Texas Gulf Sulphur*[7] and the district court decision in *Globus v. Law Research Service;*[8] and, in my opinion, unlucky enough to catch *North American Research*[9] without the time necessary to edit it down to a size digestible by a student.

The treatment of the Securities Act exemptions is basically unchanged. While the materials are there, I have great difficulty teaching the section 4 exemptions under the editors' divisions of the material: chapter 6, *Offerings by an Issuer or Underwriter;* chapter 7, *Secondary Distributions;* and chapter 8, *Private Offerings.* My students and I get lost along the way. I find the same material much easier to teach if organized by problems: (1) the mechanism of the statutory hold on a controlling person; (2) the single-level private offering to a limited group; and (3) the double-level offering that turns out to be public when the limited group lacks investment intent. The latter leads naturally into a preliminary discussion of the section 3(a)(9) exemption and then of convertible securities, which I pull from the end of chapter 9 and teach with the foregoing.

The second edition runs 1251 pages compared to 984 in the first edition. Yet, to keep the book within bounds after this expansion, Professors Jennings and Marsh have had to omit not only the *Jones* case,[10] which some of us old-timers remember with nostalgic resentment, but also the *Columbia General* case,[11] which appeared in the first edition. They have omitted such old stalwarts as the *Tucker* case,[12] the Statement on Pegging, Fixing and Stabilizing,[13] *In re NASD,*[14] and the *Halsey Stuart* case[15]—all to make room for the expansions discussed below.

Part of the new bulk of the book comes from the inclusion of materials on the developing frontiers of securities law: the antitrust laws; the rate structure and exclusionary practices of the New York Stock Exchange; the third market; the impact of mutual fund and other institutional trading on the foregoing; variable annuities and bank efforts to enter the mutual fund field; and some other current principal problems of mutual funds. There is no time in a three-hour SEC course designed to follow a single corpora-

6. Escott v. BarChris Constr. Co., 283 F. Supp. 643 (S.D.N.Y. 1968).

7. SEC v. Texas Gulf Sulphur Co., 401 F.2d 833 (2d Cir. 1968), *cert. denied sub. nom.* Coates v. SEC, 37 U.S.L.W. 3399 (U.S. April 21, 1969).

8. Globus v. Law Research Serv., Inc., 287 F. Supp. 188 (S.D.N.Y. 1968).

9. SEC v. North American Research & Dev. Corp., 280 F. Supp. 106 (S.D.N.Y. 1968).

10. Jones v. SEC, 298 U.S. 1 (1936).

11. Columbia Gen. Inv. Corp. v. SEC, 265 F.2d 559 (5th Cir. 1959).

12. *In re* Tucker Corp., 26 S.E.C. 249 (1947).

13. Statement of Policy on the Pegging, Fixing and Stabilizing of Securities Prices, SEC Securities Exchange Act Rel. No. 2,446 (1940).

14. *In re* National Assn. of Securities Dealers, Inc., 19 S.E.C. 424 (1945).

15. *In re* Halsey, Stuart & Co., Inc., 30 S.E.C. 106 (1949).

tion law course to take up such advanced materials, but the book provides much of the necessary fodder for a seminar in these and other advanced securities problems.

While the book has been expanded, it is still regrettable that some of the editors' footnotes are as short and condensed as they are. Those on fiduciary obligation have been rewritten and are reasonably lengthy and helpful, but my students seem to get very little out of the ones in the exemption chapters of the book, which have not been expanded from the first edition and which I believe suffer from undue compression. This is, however, a small matter. No one could learn securities law solely from this book or the Loss treatise or both in combination; students must have a teacher or an older lawyer experienced in the field with whom to interact. Every teacher must bring to the text his own practical background, and when he does, the general excellence of this book will outweigh its very minor deficiencies.[16]

I will conclude this Review by presenting some thoughts on teaching securities regulation in relation to the corporation law segment of the curriculum. Such reflection is made timely by the almost simultaneous appearance of this second edition of the securities regulation casebook and a new edition of a casebook on corporations[17] with Professor Richard W. Jennings of the University of California at Berkeley appearing as a co-author of both. It is particularly interesting to note the correlation between the two books and to compare this correlation with the earlier editions of the SEC casebook[18] and the corporations casebook.[19] Together the two pairs of books illustrate the difficulty of determining a clear position as to the allocation of SEC materials between the two courses. First, the earlier edition of the corporations book has nothing on distribution of securities, while the 1968 edition has about sixty-five pages. Of course, both editions of the securities regulation casebook deal with this topic at length. Second, the earlier edition of the corporations book has only eleven pages of non-SEC material, and no SEC material, on the use of inside information, but the 1968 edition has about twenty-five pages of rule 10b-5 material. The securities regulation book contains much more extensive treatments of rule 10b-5 in both editions, and the 1968 edition is heavily reorganized and on

16. The book is nearly but not quite impeccable in readability and mechanical care. One strike should be called on the publisher's staff for having obliterated in the Table of Cases to the first edition the distinction between Securities Act Releases and Securities Exchange Act Releases, and two more strikes must be called on them for having perpetuated the error in the present edition.

17. N. LATTIN, R. JENNINGS & R. BUXBAUM, CORPORATIONS, CASES AND MATERIALS (4th ed. 1968).

18. R. JENNINGS & H. MARSH, SECURITIES REGULATION, CASES AND MATERIALS (1st ed. 1963).

19. N. LATTIN & R. JENNINGS, CASES AND MATERIALS ON CORPORATIONS (3d ed. 1959).

the whole more useful for instruction than was the first edition.[20] Third, in the earlier edition of the corporations book, the SEC proxy rules were inadequately treated, and the first edition of the SEC book failed to deal with them. This latter omission was a mistake that I felt I had to rectify with mimeographed materials. The treatment in the 1968 edition of the corporations casebook is somewhat expanded. Some material has also been introduced into the SEC casebook, but its focus is more upon the problem of liability, tying into rule 10b-5, than upon a broad view of the functions of the proxy machinery; this matter is presumably left to the corporations course. Fourth, section 16(b) of the Securities Exchange Act of 1934 is treated inadequately in the earlier edition of the corporations casebook and not at all in the first edition of the SEC casebook. Again, I felt that, to teach the SEC course, I had to supplement the casebook with mimeographed materials. In the new 1968 editions, the corporation casebook contains about the same coverage, but the SEC volume has a new and reasonably adequate treatment of the subject.

It is clear that many of these topics fell unsatisfactorily beween the two stools in the older editions, but Professor Jennings and his co-editors have now found a generally acceptable solution to the problem of how to teach securities regulation—that is, a warning dose of "the federal law of corporations" in the corporations course and an integrated treatment in a separate securities regulation course. But this approach is by no means universal. The former Chairman of the SEC, Professor Cary of Columbia Law School, takes a somewhat perplexing position on this question of teaching securities regulation. His 1959 tome on corporations, written in collaboration with the late Professor Ralph J. Baker of Harvard,[21] contains a smattering of SEC material, leaving a need for a separate securities regulation course. This, of course, fits naturally into the program at Harvard, the fief of the redoubtable Professor Loss. But the Columbia Law School catalogue shows only a seminar—not a basic course—in securities regulation. Moreover, the matter gets more puzzling upon consideration of Professor Cary's 1968 supplement to the corporations book.[22] It contains a great deal of SEC material, but there is neither the comprehensiveness that is necessary to obviate the need for a full SEC course nor the compactness needed for an introduction to

20. By saying "more useful," I do not mean to say that rule 10b-5 has become more understandable. Professor Marsh's article, *What Lies Ahead Under Rule 10b-5?*, 24 Bus. Law. 69 (1968), predicting that the future of Rule 10b-5 is "more chaos," was written before the court of appeals decision in *Texas Gulf Sulphur*, but one would guess that he would not be disposed to withdraw the characterization.

21. R. Baker & W. Cary, Cases and Materials on Corporations (3d rev. ed. unabr. 1959).

22. R. Baker & W. Cary, Cases and Materials on Corporations (3d ed. Supp. 1968).

federal securities regulation in the first corporations course. In a recent conversation, Professor Cary indicated, I believe, that he is swinging toward the view that a full securities regulation course will be necessary.

There remain, however, other teachers whom I respect who use still another approach. They tell me that their schools simply do not offer an SEC course, but that they teach the necessary materials on fiduciary obligation as part of the corporations course, and the exemptions and other materials as part of courses on corporation finance or the like.[23] I cannot believe that this approach is satisfactory. I strongly doubt that one could give enough attention to fiduciary obligation in a corporations course of ordinary length. Certainly rule 10b-5 looks very different if one leads up to it through common-law liability and the express statutory liability than it does when taught standing in isolation in a corporations course. One cannot teach section 16(b) adequately in a corporations course with a hasty treatment that emphasizes only its function as a prophylactic against breach of fiduciary obligation, instead of providing enough detailed analysis to expose its remaining fearful traps.[24] Moreover, I feel that to a student who has learned only a smattering of the Securities Act exemption system, a little knowledge can be a dangerous thing. The subject is so bogged down with elusive interpretative "theology"[25] that one who has not been immersed in it deeply enough to be ordained had better not think he can grant dispensation from the registration requirement.

Finally, after thirty-five years during which securities regulation theology has been ramifying in complexity and lack of predictability, we face both the urgent need for a house-cleaning effort and the certainty that programs for reform will be an important concern during the next five years. The result of the Disclosure Policy Study

23. For a book constructed on this theory, *see* D. HERWITZ, BUSINESS PLANNING (1966).

24. Notably, (1) corporate reorganizations, *see* Lang & Katz, *Liability for "Short Swing" Trading in Corporate Reorganizations*, 20 SW. L.J. 472 (1966); Marsh, *What Lies Ahead Under Rule 10b-5?*, 24 BUS. LAW. 69, 72 (1968); (2) the possibility that trading in an option or warrant might cross trading in the stock, *see* Chemical Fund, Inc. v. Xerox Corp., CCH FED. SEC. L. REP. [Transfer Binder 1964-1966] ¶ 91,653 (S.D.N.Y. 1966), *rev'd on other grounds*, 377 F.2d 107 (2d Cir. 1967); Cook & Feldman, *Insider Trading Under the Securities Exchange Act*, 66 HARV. L. REV. 612, 617-24 (1953); SEC Securities Exchange Act Rel. No. 8,325 (1968), *amending* rule 16a-2; SEC Securities Exchange Act Rel. No. 8,229 (1968), adopting rule 16b-11 and expressly reserving this question.

25. The word "theology" is in such common use among practitioners that I cannot recall where it first appeared. It appears in Schneider, *Acquisitions Under the Federal Securities Acts—A Program for Reform*, 116 U. PA. L. REV. 1323, 1340 (1968). Former Chairman Demmler referred to the "priesthood" of practitioners in the *Conference on Codification of the Federal Securities Laws*, 22 BUS. LAW. 793, 832 at 833 (1967).

Former Chairman Cohen's approach is more decorative than religious. He refers to "the many decorative curlicues and imaginative interpretations with which it has been embellished over the years." Cohen, *The Lawyer's Role in Securities Regulation*, 24 BUS. LAW. 305 (1968).

by an internal SEC committee headed by Commissioner Wheat has just been published.[26] In addition, the Council of the American Law Institute has voted to work on a study and revision of the securities laws, subject to obtaining financing of the cost.[27] Given this focus on reform, students can receive proper preparation in the topic of securities regulation only in a separate, carefully integrated survey course.

Homer Kripke,
Professor of Law,
New York University

26. REPORT AND RECOMMENDATIONS TO THE SEC FROM THE DISCLOSURE POLICY STUDY, DISCLOSURE TO INVESTORS: A REAPPRAISAL OF ADMINISTRATIVE POLICIES UNDER THE '33 AND '34 ACTS (March 1969).

27. For the leading discussions chronologically, *see* Knauss, *A Reappraisal in the Role of Disclosure*, 62 MICH. L. REV. 607 (1964); Cohen, *"Truth in Securities" Revisited*, 79 HARV. L. REV. 1340 (1966); *Conference on Codification of the Federal Securities Laws*, 22 BUS. LAW. 793 (1967); Schneider, *Reform of the Federal Securities Laws*, 115 U. PA. L. REV. 1023 (1967); Schneider, *An Administrative Program for Reforming the Federal Securities Laws*, 23 BUS. LAW. 737 (1968) (with colloquy); Wheat, *The Disclosure Policy Study of the SEC*, 24 BUS. LAW. 33 (1968); Knauss, *Disclosure Requirements—Changing Concepts of Liability*, 24 BUS. LAW. 43 (1968).

Books Received

ADMIRALTY

Admiralty Law of the Supreme Court (2d ed.). By *Herbert R. Baer*, Professor of Law, University of North Carolina. Charlottesville, Va.: The Michie Company. 1969. Pp. xiv, 653.

COMPARATIVE LAW

Processo e Ideologie. By *Mauro Cappelletti*. Bologna, Italy: Il Mulino, Via Santo Stefano 6, Casella Postale N. 119. 1969. Pp. xi, 569. Paper. L. 6,000.

EUROPEAN COMMUNITIES

Droit des Communautés Européennes. Edited by *W. J. Ganshof van der Meersch*. Brussels, Belgium: Maison Ferdinand Larcier, 39, Rue des Minimes. 1969. Pp. cxiii, 1193. 3,200 F.B.

INCOME TAX

Collapsible Corporations—General Coverage. By *Frederic A. Nicholson*. Washington, D.C.: Tax Management, Inc. 1969. 9 chs. Paper.

Farm and Ranch Expenses and Credits. By *Martin B. Dickinson, Jr.*, Assistant Professor of Law, University of Kansas. Washington, D.C.: Tax Management, Inc. 1969. 4 chs. Paper.

H.R. 10 Plans—Taxation of Distributions. By *David G. Lilly*. Washington, D.C.: Tax Management, Inc. 1969. 9 chs. Paper.

INTERNATIONAL LAW

International Legal Process: Materials for an Introductory Course. (2 vols.). By *Abram Chayes*, Professor of Law, Harvard University; *Thomas Ehrlich*, Professor of Law, Stanford University; and *Andreas F. Lowenfeld*, Professor of Law, New York University. Boston: Little, Brown. 1968. Pp. xxiii, 704; vi, 697.

LEGAL HISTORY

Conservative Crisis and the Rule of Law: Attitudes of Bar and Bench, 1887-1895. By *Arnold M. Paul*. New York: Harper & Row. 1969. Pp. xviii, 259. Paper, $1.95.

Scottsboro—A Tragedy of the American South. By *Dan T. Carter*, Professor of History, University of Maryland. Baton Rouge: Louisiana State University Press. 1969. Pp. xiii, 431. $10.

OBSCENITY

Obscenity and Public Morality. By *Harry M. Clor*, Associate Professor of Political Science, Kenyon College. Chicago: University of Chicago Press. 1969. Pp. xii, 315. $9.50.

POLICE

Varieties of Police Behavior. By *James Q. Wilson*, Professor of Government, Harvard University. Cambridge, Mass.: Harvard University Press. 1969. Pp. xi, 309. $6.50.

SALES

Problems and Materials on Sales and Secured Transactions. By *Robert J. Nordstrom*, Professor of Law, Ohio State University; and *Norman D. Lattin*, Professor of Law, University of California. St. Paul, Minn.: West. 1968. Pp. xxv, 809.

SATELLITE COMMUNICATIONS

Les Télécommunications par Satellites. *Centre National de la Recherche Scientifique*. Paris, France: Éditions Cujas, 19, rue Cujas, Paris 5e. 1968. Pp. xi, 456. Paper.

TAXATION: STATE AND LOCAL

State and Local Taxation—Cases and Materials. By *Jerome R. Hellerstein*, Professor of Law, New York University. St. Paul, Minn.: West. 1969. Pp. xl, 741. $14.

WAGES

Guideposts for Wages and Prices: Criteria and Consistency. By *Edward F. Denison*. Ann Arbor: Institute of Public Policy Studies and Department of Economics, University of Michigan. 1968. Pp. 32. Paper. $1.75.

PERIODICAL INDEX

This index includes *articles, comments* and some of the longer *notes* and *recent developments* which have appeared in leading law reviews since the publication of the last issue of this *Review*. (a) indicates a leading article.

EMINENT DOMAIN

Allocating the costs of determining "just compensation." (a) Douglas Ayer. 21 Stan. L. Rev. 693-726 (April).

EQUAL PROTECTION

See also *Elections, Zoning.*

Developments in the law—equal protection. 82 Harv. L. Rev. 1065-192 (March).

EVIDENCE

See *Attorneys.*

FAMILY LAW

The response of some relevant community resources to intra-family violence. (a) Raymond I. Parnas. 44 Ind. L.J. 159-81 (Winter).

FEDERAL RULES OF CIVIL PROCEDURE

See *Discovery.*

FEDERAL TORT CLAIMS ACT

Claims settlement for air force noncombat plane crashes. (a) Cornelius P. Cotter. 47 Texas L. Rev. 593-614 (March).

FOREIGN INVESTMENTS

American private direct investment in eastern Europe: intersection of business interests and foreign policy. 21 Stan. L. Rev. 877-937 (April).

The foreign direct investment program: an analysis and critique. 55 Va. L. Rev. 139-76 (Feb.).

The foreign direct investment regulations: a look at ad hoc rulemaking. (a) William W. Lancaster, Jr. 55 Va. L. Rev. 83-137 (Feb.).

Governmental regulation of foreign investment. 47 Texas L. Rev. 421-47 (Feb.).

FOREIGN RELATIONS

Alien inheritance statutes and the foreign relations power. 1969 Duke L.J. 153-71 (Feb.).

FREEDOM OF SPEECH

Less drastic means and the first amendment. 78 Yale L.J. 464-74 (Jan.).

GAMBLING

Federal regulation of gambling: betting on a long shot. 57 Geo. L.J. 573-98 (Feb.).

GERMANY, FEDERAL REPUBLIC OF

The federal constitutional court in Germany: scope of its jurisdiction and procedure. (a) Hans G. Rupp. 44 Notre Dame Law. 548-59 (April).

HOUSING

See also *Landlord & Tenant.*

Overcoming barriers to scattered-site low-cost housing. 2 Prospectus. 327-46 (April).

Private enforcement of municipal housing regulations. 54 Iowa L. Rev. 580-96 (Feb.).

HUSBAND AND WIFE

Denial of loss of consortium to wife as violation of fourteenth amendment right of equal protection. 44 Ind. L.J. 293-307 (Winter).

ILLINOIS SUPREME COURT

Illinois supreme court review. 63 Nw. U. L. Rev. 614-98 (Nov.-Dec.).

INCOME TAX

See also *Poverty Law.*

The cost of lifting minerals dedicated to outstanding production payments in ABC transactions: an expense? 47 Texas L. Rev. 624-32 (March).

Principle and prepaid interest. (a) Michael Asimow. 16 UCLA L. Rev. 36-85 (Nov.).

The private annuity and the foreign situs trust. (a) Arnold Kassoy. 16 UCLA L. Rev. 86-119 (Nov.).

The real estate investment trust: receptacle for foreclosed property and nonconforming loans. (a) Robert J. Jensen. 42 S. Cal. L. Rev. 70-91 (Fall).

The tax bargain in executive compensation. 47 Texas L. Rev. 405-20 (Feb.).

The tax consequences of redemption of convertible bonds. 49 B.U. L. Rev. 96-113 (Winter).

Tax consequences of withdrawal from a two man partnership: sale or liquidation. 54 Cornell L. Rev. 438-47 (Feb.).

Tax-exempt organizations: the attack on unreasonable accumulations of income. (a) Stuart Duhl. 57 Geo. L.J. 483-507 (Feb.).

INDIANS

Indians: better dead than red? 42 S. Cal. L. Rev. 101-25 (Fall).

INHERITANCE AND SUCCESSION

See *Community Property, Foreign Relations.*

INTEGRATION

The Sweatt case and the development of legal education for Negroes in Texas. 47 Texas L. Rev. 677-93 (March).

MOTOR VEHICLES

Automobile manufacturers—a new liability for design defects. 49 B.U. L. Rev. 167-80 (Winter).

MUNICIPAL CORPORATIONS

The municipal revenue crisis: California problems and possibilities. (a) Donatas Januta. 56 Calif. L. Rev. 1525-58 (Nov.).

NEWSPAPERS

The duty of newspapers to accept political advertising—an attack on tradition. 44 Ind. L.J. 222-41 (Winter).

Press releases and defamatory pleadings. 63 Nw. U. L. Rev. 699-722 (Nov.-Dec.).

OIL AND GAS

The lease allowable system: new method of regulating oil production in Texas. 47 Texas L. Rev. 658-76 (March).

PAROLE

See *Constitutional Law.*

PARTNERSHIPS

See *Income Tax.*

PENOLOGY

Short-term rehabilitation and crime prevention. 2 Prospectus. 451-64 (April).

POVERTY LAW

See also *Public Utilities, Social Welfare, Zoning.*

Administration of a negative income tax. (a) William D. Popkin. 78 Yale L.J. 388-431 (Jan.).

PRIVILEGED COMMUNICATIONS

See *Corporations.*

PRODUCTS LIABILITY

See also *Motor Vehicles.*

The remote purchaser of made-to-order goods: third-party beneficiary in products liability law. 54 Cornell L. Rev. 473-81 (Feb.).

PUBLIC DEFENDERS

Client service in a defender organization: the Philadelphia experience. 117 U. Pa. L. Rev. 448-69 (Jan.).

PUBLIC EMPLOYEE UNIONISM

See also *Labor Law.*

Labor relations in the public sector: a symposium. Articles by Russell A. Smith, Charles M. Rehmus, Theodore H. Kheel, Arvid Anderson, H. W. Arthurs, Eli Rock, Donald H. Wollett, Ida Kaus, and Ralph S. Brown, Jr. 67 Mich. L. Rev. 891-1082 (March).

State and local public employee collective bargaining in the absence of explicit legislative authorization. (a) Richard F. Dole, Jr. 54 Iowa L. Rev. 539-59 (Feb.).

PUBLIC UTILITIES

Public utilities and the poor: the requirement of cash deposits from domestic consumers. 78 Yale L.J. 448-63 (Jan.).

RES JUDICATA

Res judicata and the bifurcated negligence trial. 16 UCLA L. Rev. 203-15 (Nov.).

RIGHT OF PRIVACY

Credit investigations and the right to privacy: quest for a remedy. 57 Geo. L.J. 509-32 (Feb.).

SCHOOLS AND SCHOOL DISTRICTS

Equality of educational opportunity: are "compensatory programs" constitutionally required? 42 S. Cal. L. Rev. 146-68 (Fall).

Public secondary education: judicial protection of student individuality. 42 S. Cal. L. Rev. 126-45 (Fall).

The scope and sources of school board authority to regulate student conduct and status: a nonconstitutional analysis. (a) Stephen R. Goldstein. 117 U. Pa. L. Rev. 373-430 (Jan.).

SCIENCE

See *Legal History.*

SEARCH AND SEIZURE

Scope limitations for searches incident to arrest. 78 Yale L.J. 433-47 (Jan.).

Stop and frisk. 63 Nw. U. L. Rev. 837-61 (Jan.-Feb.).

SECURITIES REGULATION

Civil liabilities under the federal securities acts: the BarChris case—part I —section 11 of the securities act of 1933. (a) Ernest L. Folk, III. 55 Va. L. Rev. 1-82 (Feb.).

Escott v. BarChris Construction Corp.: "due diligence" defenses under section 11 of the securities act of 1933. 16 UCLA L. Rev. 177-202 (Nov.).

Securities regulation and the foreign issuer exemption: a study in the process of accommodating foreign interests. (a) Richard M. Buxbaum. 54 Cornell L. Rev. 358-78 (Feb.).