Technology and Privacy

APPENDIX 5
TO

The Report of
The Privacy Protection Study Commission

July 1977

The Report of the
Privacy Protection Study Commission

Personal Privacy in an Information Society
(Stock No. 052-003-00395-3)

Appendix 1:
Privacy Law in the States
(Stock No. 052-003-00421-6)

Appendix 2:
The Citizen as Taxpayer
(Stock No. 052-003-00422-4)

Appendix 3:
Employment Records
(Stock No. 052-003-00423-2)

Appendix 4:
The Privacy Act of 1974: An Assessment
(Stock No. 052-003-00424-1)

Appendix 5:
Technology and Privacy
(Stock No. 052-003-00425-9)

Copies of each of these volumes may be ordered from the:
Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402

PRIVACY PROTECTION STUDY COMMISSION

Chairman

David F. Linowes
Certified Public Accountant, New York City, and
Boeschenstein Professor of Political Economy
and Public Policy, University of Illinois

Vice Chairman

Dr. Willis H. Ware
The Rand Corporation
Santa Monica, California

William O. Bailey, President
Aetna Life & Casualty Company
Hartford, Connecticut

William B. Dickinson
Retired Executive Editor,
Philadelphia Evening Bulletin
Philadelphia, Pennsylvania

Congressman Barry M. Goldwater, Jr. of California
Washington, D. C.

Congressman Edward I. Koch of New York
Washington, D. C.

State Senator Robert J. Tennessen, Attorney
Grose, Von Holtum, Von Holtum, Sieben & Schmidt
Minneapolis, Minnesota

PRIVACY PROTECTION STUDY COMMISSION — STAFF

Carole W. Parsons
Executive Director

Ronald L. Plesser
General Counsel

Louis D. Higgs
Deputy Executive Director and Director of Research

Office of the Executive Director

Susan J. Bennett, *Special Assistant*
Arthur A. Bushkin, *Staff Technical Advisor*
Commander Walter E. Conner,[1] *Administrative Officer*
Pamela S. Ellsworth, *Administrative Assistant*
Mark F. Ferber, *Special Consultant to the Executive Director*
Christopher E. Heller, *Senior Research Associate*
Justine V. R. Milliken, *Assistant to the Chairman*
James F. Sasser,[2] *Administrative Officer* (September 1975 to February 1977)
Alan F. Westin, *Special Consultant to the Commission*

Office of the General Counsel

Christopher J. Vizas, II, *Special Staff Counsel*
John A. Turner, Jr., *Assistant General Counsel*
Stephen C. Nichols, *Assistant to the General Counsel*
Shirley A. Lewi, *Administrative Assistant*

Office of Public Information

Mark F. Ferber, *Director*
John F. Barker, *Director* (September 1975 to April 1977)
Eleanor B. High, *Assistant*

Project Management

Lois Alexander,[3] *Research and Statistics*
Susan J. Bennett, *Public Assistance, IRS, Social Security Number*
Arthur A. Bushkin, *Privacy Act Assessment, Technology Assessment*
William H. Foskett, *Education*
Christopher E. Heller, *Credit, Credit-Reporting, and Depository Institutions*
Joan Holloway,[4] *Medical Records*
David M. Klaus, *Investigative Agencies*
Christopher J. Vizas, II, *Government Access*
Jane H. Yurow, *Employment and Personnel*

---

[1] On detail from the Department of Defense.
[2] On detail from the Department of Health, Education, and Welfare (DHEW).
[3] On detail from the Social Security Administration, DHEW.
[4] On detail from the Division of Hospitals and Clinics, U.S. Public Health Service.

Professional Staff and Consultants

Arthur J. Altenberg
Donald Bartlett
Joan Berry
Timothy B. Braithwaite[5]
Joe S. Cecil
Nancy H. Chasen
Claire Dalton
Warren O. Davis[6]
Priscilla DeGasparis
Major William R. Elliott, Jr.[5]
David Galbraith
Timothy Gay
Charles Grezlak
Charles Gustafson
Claudia R. Higgins
Florence B. Isbell
Mary Kay Kane
William R. Klamon
Charles R. Knerr
John Langton, III
Donald Letourneau
Abe Levin
Michael Liethan
Daniel H. Lufkin
Kenneth E. Mannella
Ruth Matthews
Justine V. R. Milliken
Hubert A. Mitchell
William B. McMahon
Margaret A. Neel
David Nierenberg
G. Russell Pipe
Bruce Ransome
Ira Reed
James B. Rule
Francis M. Rush, Jr.[5]
Cynthia E. Schaffhausen
Arden Schell
Harold D. Skipper
Joyce R. Starr
J. Michael Taylor[7]
Patricia Tucker
Rein Turn
Philip Vargas
Alease M. Vaughn
Fred W. Weingarten[8]

Administrative Staff

Phyllis R. Anderson
A. Kristen Austin
Zemphria Raymond Baskin
Mary K. Chin
Alice Cumberland
Louise Goldstein
Debbie J. Graham
Emily Hanis
Lori J. Haselhorst
Jeanne L. Holmberg
Fran Hoyle
Susan Kaslow
Alan C. Luckett
Nancy Mathes
Nina A. Mohay
Joanne Robinson
Mary Scott

Research Assistants

Phyllis R. Anderson
Zemphria Raymond Baskin
Laura Bonn
Vernease Herron
Brenda Reddix
Catherine J. Rodgers
Adrienne Taylor
Roger S. Tilton
Helene Toiv
Michael S. Turchin

[5] On detail from the Department of Defense.
[6] On detail from the Bureau of the Census.
[7] On detail from the Department of Labor.
[8] On detail from the National Science Foundation.

Portions of this volume were prepared
for the Office of Naval Research pursuant
to Government Order N00014-77-F-0030.

Table of Contents

Preface

This volume is about the personal privacy implications of society's increasing dependence on computer-based record-keeping systems. Because it is primarily an analysis of trends, it contains no recommendations. Rather, it presents a picture of a rapidly changing world in which insufficient attention is being paid—by policy makers, system designers, or system users—to the privacy protection implications of these trends.

In a consumer-oriented society such as the United States, there are many forces that directly or indirectly result in the proliferation of computer-based record-keeping systems. In the private sector, pressures for automation arise from growth in the number and complexity of services offered to individuals, businesses, and institutions. In the public sector, new or expanded social programs, as well as increasing regulation of the private sector, encourage new record-keeping applications of computer and telecommunications technologies at all levels of government. The technologies themselves play a forceful role by making it possible for organizations to perform services that would be prohibitively costly, and even inconceivable, without them.

Technological developments, and their application to personal-data record keeping, tend to occur on a much shorter time scale than is generally perceived. Furthermore, record keeping tends to be an invisible, background activity whose consequences are not readily appreciated by the formulator of a new service or program. As the material in this volume will show, undesirable consequences are highly likely to occur if the proliferation of computer-based record keeping is left unattended. This is so, not because of any sinister act or intent, but rather because of the incremental effects of independent decisions by well-intentioned administrators.

Even in areas already subject to privacy protection legislation there is the danger that personal privacy will be further eroded due to applications of new technology. Policy makers must not be complacent about this potential. The economic and social costs of incorporating privacy protection safeguards into a record-keeping system are always greater when it is done retroactively than when it is done at the system's inception.

The Commission was fortunate to have an unusually industrious and diverse project staff; additionally, our Vice Chairman, Willis H. Ware, actively participated in the project's development and execution. Arthur A. Bushkin served as Project Manager. Working with him as staff and consultants at various times throughout the life of the project were: Donald

Bartlett, Timothy B. Braithwaite, Rein Turn (who also provided the material for the Appendix to this volume), Fred Weingarten, and Christopher J. Vizas, II.

In addition to its dedicated staff, the Commission was privileged in having the help of numerous individuals, both in and out of government, at various stages of this project. Among those who provided advice, administrative assistance, or reviews of draft material were: Paul Armer, Paul Baran, John Berg, Richard L. Bisbey, II, Edward Boback, Dennis Branstad, Ralph Busch, John Couleur, John J. Geraghty, Dennis Hollingworth, Jeffrey Meldman, Richard G. Mills, Philip S. Nyborg, Samuel I. Schaen, and Terril J. Steichen. Their efforts were extremely helpful in our work—final responsibility for the entire volume, of course, rests with the Commission.

To all of those who were involved in the preparation of this volume, I extend the Commission's sincere appreciation.

David F. Linowes
Chairman

Chapter 1

Introduction

In the course of its two-year inquiry, the Privacy Protection Study Commission reached important conclusions with respect to the technology of personal-data record-keeping in American society:

> First, advances in computer and telecommunications technologies are dramatically and rapidly altering the way records about individuals are created, maintained, and used;
>
> Second, while computer and telecommunications technologies serve the interests of organizations and can be best appreciated as extensions of those interests, their broad availability and low cost provide both the *impetus* and the *means* to perform new record-keeping functions;
>
> Third, technology, like the law, has by and large failed to provide the tools an individual needs to protect himself from the undesirable consequences that recorded information can create for him today; and
>
> Fourth, growth in society's record-keeping capability threatens to upset existing power balances between individuals and organizations, and between government and the rest of society, thereby creating the danger that delay in addressing important privacy protection issues will irrevocably narrow the range of options open to public-policy makers.

Simply stated, the record-keeping world is changing, and the rapidity with which the change is occurring must not be allowed to outstrip our ability to deal with it. As Americans, we live inescapably in an "information society." Our consumer-oriented economy has prompted the creation of wholly new types of record-keeping systems, like the ones the airlines use to make and keep track of flight reservations and the ones that now allow banks to dispense cash and accept deposits 24 hours a day. The first computer-based personal-data systems were essentially mirror images of their manual antecedents, with some enhanced features resulting from the ease of restructuring machine-readable information. In a few short years, after the early commercial applications of computers came into vogue, however, this new technology was coupled with existing telephone networks in order to allow information to be transmitted and retrieved to and from

points all over the country, and eventually all over the world. Further enhancements in information processing coupled with the demands of a service-oriented society caused record-keeping systems to be restructured to the point that many of today's applications bear no resemblance to earlier manual systems, but rather represent completely new approaches which could not be replicated in a manual environment.

Government agencies, among the largest suppliers of services to individuals, have also begun to exploit the new record-keeping technologies in innovative ways. Moreover, government, unlike the private sector, has investigative and enforcement responsibilities which make the search and tracking capabilities that stem from applying computers and telecommunications to personal-data record keeping an attractive instrument, be it the government's own or a private-sector one to which government, under current law, can have easy access.

The magnitude of our growing dependence on the new record-keeping technologies was aptly captured by a recent *Time* magazine article on the Soviet Union where computers are still used principally for advanced scientific, industrial, and military purposes. Attributing the U.S.S.R.'s lag in computer development to "its decision not to foster the kind of consumer society that has nurtured the rapid growth of the industry in the West," the article went on to point out that of the 300,000 computers installed in the U.S. (compared with 22,000 in the Soviet Union)

> . . . fully three-quarters of them are engaged in commercial operations—everything from billing credit-card accounts and writing paychecks to sending flowers by wire and keeping baseball statistics up to date. . . . A Western cybernetics expert in Moscow estimates that while an American has dealings linked with a computer at least ten times a day, the average Soviet citizen comes in contact with a computer perhaps once every six months, if then. Though the Soviet State Bank is the world's largest banking operation, it does not possess a modern computerized check-processing and accounting system. Stores do not use computers for charge accounts, since Soviet citizens are not permitted this capitalist excess, and they have not computerized other parts of their operations, like inventory control. Aeroflot, the Soviet national airline, in 1975 bought two Univac 1106 computers, worth about $5 million apiece, from the U.S.'s Sperry Univac to automate reservations on international flights; but the world's largest airline has not yet computerized its domestic reservation system.[1]

The image of the world's largest airline trying to handle its domestic reservation system without the aid of the computer cannot help but underscore for an American what a great boon the technology has been. The benefits, however, must not be allowed to obscure the real dangers that can lurk behind them. Giving large organizations the ability to reach out to individuals directly, anywhere and at any time, has its costs as well as its

[1] *Time*, August 1, 1977, p. 45.

benefits, and one of the greatest long-run costs could be a marked diminution of personal privacy.

This volume explores the impact of computer and telecommunications technologies on personal-data record keeping in American society during the last two decades and ventures a projection of the pace and direction of developments in information technology into the 1980's. While it is no doubt true that many aspects of the Commission's inquiry have been concerned with record-keeping practices that are independent of computers, the increasing influence of automation has, nonetheless, been in the forefront of all the Commission's investigations, deliberations, and recommendations. Not only did the Commission believe it important to understand the various dimensions of the technologies' impact; it also wanted to make sure that its recommendations would not be rendered obsolete by technological advances.

Because the technologies are changing so rapidly, the Commission did not attempt a forecast in the sense of a prediction of new technologies not yet in the research prototype stage. Rather, the Commission asked the more simple question: "What will be the effect of more widespread availability of what we know to be possible right now?" The answers to this question are presented in the chapters that follow.

Chapter 2 presents an overview of information technology. The basic elements of a computer system are described, and some of the more common terminology is introduced. The rapid pace of computer development is summarized and the difficulty of forecasting future developments is briefly discussed.

Chapter 3 addresses the impact of information technology on record-keeping practices and privacy protection. It illustrates, through examples, why policy makers should be concerned with current trends in information technology and automated record keeping.

Chapter 4 highlights a number of important technical considerations that must be taken into account in formulating privacy protection policy. Again, the list is illustrative, not exhaustive.

Chapter 5 closes the loop by discussing the effects that trends in privacy protection safeguards will have on the design and development of automated information systems. While the necessarily general discussion is aimed at the technical reader, the topics will be meaningful to the general reader as well.

The Appendix to this volume presents a detailed projection of advances in information technology through the mid-1980's. It treats the issues raised in Chapter 2 at a greater level of technological refinement; all readers, however, may wish to skim it in order to get a greater sense of the pace of technological development.

Chapter 2

Information Technology: An Overview

Record-keeping technology has existed since the dawn of civilization. Some 14,000 years ago, primitive men carved notches on an eagle's wing bone to keep track of the number of days between two consecutive full moons.[1] Later, knotted cords, clay tablets, papyrus scrolls, and parchment were used to record the wealth of kings and princes, and the obligations of their subjects. As the forms of human social organization grew and became more complex, the content of records also changed from information about astronomical and natural events to information about people (e.g., records of property ownership, tax records, population registers, and rosters of organizations).

Record-keeping technology reached the age of mechanization in the 1880's[2] when Herman Hollerith invented punched cards and electromechanical equipment to "read" and process them. This new mode of record keeping was first used in the U.S. Census of 1890, and provided a dramatic, eight-fold decrease, relative to manual methods, in the time necessary to tabulate census data on over 63 million people. Over the next 65-70 years, punched-card processing and tabulating equipment was refined and manufactured on a large scale by corporations such as IBM and Remington-Rand. Numerous installations were made in government, business, and industry. The maximum data storage density of punched cards is small—only 350 characters per cubic inch—and the processing speed is relatively slow; thus, large record-keeping facilities required many file cabinets to store their data bases, and large numbers of key punches, verifiers, sorters, collators, duplicators, and tabulators, as well as large numbers of people to operate them.

The development of electronic digital computers in the 1940's, and their application to business data processing and record keeping in the 1950's, set the stage for new advances in record-keeping technology. Data processing was no longer limited to simple counting and tabulating, but included virtually any desired processing operation. Magnetic tape technology improved the achievable storage density more than 50 times over punched cards. The processing rate jumped over a thousand-fold—from

[1]DHEW Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens,* (Washington, D.C.: U.S. Government Printing Office, 1973).

[2]Huskey, Harry D. and Velma R., "Chronology of Computing Devices," *IEEE Transactions on Computers*, December, 1976, Volume C-25, Number 12, pp. 1190-1199.

approximately 130 characters per second (for punched-card readers) to over 15,000 characters per second. The simple operation of mounting a magnetic tape replaced the time-consuming and error prone loading of card decks into readers. A more detailed discussion of recent and projected advances in information technology can be found in the Appendix to this volume.

What is a Computer System?

Most of the discussion in this volume is concerned with what a computer can and does do. Hence, it will be useful to have a general appreciation of both computer and telecommunications technology.

It is convenient to think of a "computer" as equipment (called the "computer hardware") that stores information[3] and manipulates it according to a set of rules, or instructions (called a "computer program"), that has been prepared by a "computer programmer." If the stored data are the financial affairs of a company and the rules are those of bookkeeping, the computer is for all practical purposes doing corporate accounting. If the data are about people, and the rules are those of maintaining, updating, and consulting records, then the computer is running a record-keeping system about people.

Computer hardware consists of a number of physical devices which collectively are called a "computer system." (Regrettably, the terminology here is not precise, and the term "computer system" is sometimes used to refer to the entire ensemble of hardware, programs, people, and procedures that together constitute an automated record-keeping operation.) The important components of the hardware system are:

- the "central processing unit" (CPU), which is the device that actually executes the computer instructions and, in so doing, manipulates data;
- the high-speed or fast operating "storage" or "memory" (sometimes called "main memory"), which serves as the repository for programs or data when they are being actively used;
- the low-speed or slower secondary storage or memory, which serves as the long-term repository for programs or data—such storage may be "on-line, random access" in that it is always directly accessible by the CPU in any order (e.g., magnetic discs, which are similar to phonograph records) or it may be "sequential" (e.g., magnetic tape); and
- "input/output" (I/O) devices, such as card readers, card punches, printers, typewriter terminals, and cathode ray tube (CRT) displays.

In addition, there are various control units to ensure that the devices work together properly.

As would be expected, the central processing unit can perform the four basic arithmetic operations (i.e., addition, subtraction, multiplication, and

[3]The terms "information" and "data" will be used interchangeably through this discussion.

division), but it also can perform certain other operations that often are collectively called "logical" operations. Examples include:

- storing an item of data and then retrieving it from memory;
- combining data fragments into a single item;
- separating data into fragments;
- rearranging the format of a data item;
- choosing between different sequences of operations depending upon the value or form of a particular data item;
- moving data among storage devices; and
- moving data to and from an input/output device.

By combining arithmetic and logical operations into a proper sequence of steps, the programmer arranges for the data to be manipulated in a desired way.

A computer, it must be emphasized, will perform only the sequence of operations contained in a program; it has no inherent judgment or self-knowledge that can permit it to compensate for:

- errors in the program;
- omissions from the program; or
- situations not covered by the program.

Thus, conversion of a manual record-keeping system into an automated one does not consist of simply replicating, in a sequence of computer instructions, the activities of file clerks. Rather, it also includes identifying those actions that file clerks take because they are people with judgment, especially with respect to recognizing and accommodating error situations or to handling special cases. Hence, a typical computer program is very complex; it must account for *all* possible cases of a problem; there can be no loose ends or anomalies. The program must have the capacity to recognize and handle errors; what should the program do, for example, if a user misspells a word while typing at his terminal?

Large computer programs are among the most complex intellectual tasks man has ever attempted. All programs must be elaborately and carefully tested, but it is usually impossible to test all possible sets of conditions in a large program, so it is usually also impossible to guarantee that there are no errors in a large program.

The process of programming:

- is largely an intellectual task;
- is labor intensive;
- is complicated;
- demands that the programmer understand the task or problem in minute detail;
- is the conversion of an intellectually understood task into an unambiguous sequence of steps;
- does not rest on a theoretical foundation and, thus, is largely an art;
- is heavily experimental; and

- is an exercise in dealing with the finest of details completely and without error.

Given such a characterization of computer programming, it is easy to understand why a computerized record-keeping system sometimes goes astray and behaves peculiarly—it may have encountered a situation that the program was not designed to handle or it may have come upon an error that caused it to behave in unforseen ways. Similarly, changes to a program are neither simple nor straightforward, especially since a change can have repercussions throughout the whole program. Sometimes, a change will require a complete redesign of the program. Naturally, the changed program requires thorough retesting.

Some computer programs are now so subtle and comprehensive that they frequently amaze programmers themselves. Computers can be programmed to play games exceedingly well (e.g., chess, bridge, and checkers), to imitate thought processes, and to appear surprisingly humanoid. With respect to record keeping, however, there is an effect of computer programming that is quite remarkable, even though it is commonly taken for granted. It is the ability, through sophisticated programming techniques, to create for a user the illusion of a situation that does not really exist.

For example, assume that there is a set of records[4] whose first three items are name, address, and employee number; the next 10 items are payroll information; and the last 16 items are medical information. It is possible, through sophisticated programming techniques, to make user A (the payroll clerk) think that his data base[5] consists of the first 13 items; to make user B (the corporate physician) think that his data base consists of 19 items (i.e., the first 3 plus the last 16); and to allow user C (the boss) to see all 29 items. Moreover, it is possible to design the system so that each user will not know of the existence of the other users or of that portion of the total data base—called an "integrated data base"—that he cannot see. It is also possible that the 29 items do not even exist together in one computer, but rather that they are parts of a "distributed data base," parts of which exist at physically different, but electrically interconnected, locations. The detailed

[4]The terms "record" and "file" have several meanings in a computer context, all of which differ from their general meaning in privacy protection literature. The term "record" will be used herein to refer to any collection or grouping of information about an individual. The term "file" will be used to refer to a collection or grouping of records. Thus, one file should be understood to contain records on many individuals, rather than as a file, in the colloquial sense, maintained on an individual. The term "file" therefore substitutes for the terms "system of records" and "system" as they have generally been used in the Privacy Act of 1974 and in the Commission's final report. This substitution is necessary because the term "system" also has several special meanings in a computer context, and will be used in that context in this volume.

[5]We are using the term "data base" here to refer only to the raw data as they are stored in the computer system; the terms "information system" or "record system" generally refer to the "data base" plus the appropriate software used to maintain it. The terms "data base" and "file" are often used interchangeably. To the extent that a distinction is meaningful, the term "file" is generally used more loosely to refer to any collection of records, regardless of format, whereas the term "data base" usually refers to a collection of records which is formatted for use by a particular software system, such as a data-base management system. Note, the popular term "data bank" has no technical meaning.

infrastructure of the physical location of data and the way in which it is organized into computer records can be made completely invisible to a user.

The technique for achieving this effect is so common that the result is described by the special term "virtual data base." Indeed, programming systems that achieve the effect are now so sophisticated that it is even possible to create the illusion that a programmer is using a computer with different hardware characteristics than the one to which he is "really" connected.[6]

The "virtual" technique also has an important impact on record-keeping centralization. Most people think of centralization as physical centralization; that is, the records are stored in one computer, at one location, and under the control of one authority. However, computer networking—the interconnection of computers via telecommunications—and advanced programming techniques now make possible physical decentralization, but functional centralization, of records. For example, a bank may have its records physically located at a number of branches, but computer networking and advanced programming techniques can make this transparent to the customer when he makes a transaction at other than his normal branch. In effect, the system appears and behaves as though there were only one physically centralized data base.

To summarize some of the more common terminology, computers can communicate in many ways: by *reading* cards or tape; by *punching* cards; by *writing* magnetic tape; by *responding* to key strokes from a terminal; by *displaying* data; or by *printing* paper. Moreover, there is virtually no limit to the types of *input/output* devices that can be used in conjunction with a computer. Computers can be programmed to read sensors (e.g., thermometers, flowmeters, voltmeters, or switch positions); detect images (e.g., pictures or characters on a printed page); or recognize spoken words. Computers can also be programmed to operate devices (e.g., move valves, open or close doors, or start or stop motors); display or draw pictures; generate speech; and communicate with other computers.

A computer system can *store* and *retrieve* data, and it can perform *arithmetic* and *logical* operations on those data. A computer system can also *communicate*, or *interact*, with (some portion of the rest of) the world. As seen from the computer's point of view, this communication consists of *input* from the outside world or *output* to the outside world. Data stored in a computer system can be numerical, alphabetic, special punctuation, mathematical symbols, foreign alphabets, arbitrary symbols, or any combination thereof. Each unit of data is called a *character*, or, more precisely, an *alphanumeric character*. Within the computer, data are represented by binary digits, or *bits*, and eight bits are typically used to represent one character. A computer can be instructed—or constructed—to recognize particular "bit patterns" and treat them as characters.

[6]The terms "virtual" and "real" are frequently used to describe and contrast such effects, although occasionally the terms "logical" and "physical" are also used for the same purpose. Additionally, the term "functional" is sometimes substituted for the term "logical," as in the sentence: "The physically decentralized airline reservation system operates as the *functional equivalent* (i.e., *logical equivalent*) of a single, centralized system."

The sequence of steps or instructions which the computer follows is called a *program*. The generic term for programs is *software*, and the process of creating software is called *programming*. Every computer has its own native "language" to which it responds. Called *machine language*, it consists of all the individual instructions to which the computer can respond. To facilitate the programming task, *programming languages*, or *higher order languages*, have been developed. Before a computer can respond to a program written in a higher order language, however, the latter must be *translated*, or *compiled*, into machine language. Finding and correcting errors in a program is called *debugging*.

The Pace of Computer Development

In its short life of some 25 years, there have been dramatic and continuous advances in computer technology. Every five years, a new generation of computer components and equipment has appeared, increasing computational speed and reliability but reducing physical size and relative cost. Vacuum tubes were followed by the "solid-state" era. Initially, solid-state technology was characterized by the use of individual transistors, but later it witnessed the development of the monolithic chip of silicon on which complete circuits and subsequently entire subsystems, such as arithmetic units or storage units, were packaged. The improvement of manufacturing techniques now makes it possible to put an entire central processing unit, complete with its control and input/output buffer memories, on a single chip.[7]

As new generations of electronic components have been introduced, and as new hardware architectures have been developed,[8] computing speed has increased from a few tens of thousands of instructions per second in the late 1950's to one million instructions per second, or one MIPS, in 1963, to 12-15 MIPS in 1967, to nearly 100 MIPS in the fastest processors in 1972. At the same time, storage capacity of the high-speed main memory has increased from 150,000 characters accessible in tens or hundreds of microseconds in the early 1960's, to millions of characters accessible in a fraction of a microsecond.[9] Such fast storage is backed by almost unlimited amounts of slower storage capacity on magnetic discs, tapes, and mass memory units. For example, the main fast memory of the STAR-100 machine from Control Data Corporation has a capacity of four million characters which can be accessed at the rate of 160 million characters per second. One available mass memory is the IBM 3850 Mass Storage System, whose capacity is over 470 billion characters—equivalent to over 2,000 sets of the 23-volume Encyclopedia Britannica; the time to find any portion of the stored data averages 15 seconds, but it then flows sequentially at a rate of millions of characters per second.

While computing speed and storage size have been advancing,

[7]This progression of events is usually referred to as: discrete components, integrated circuits (IC), medium-scale integration (MSI), and large-scale integration (LSI).

[8]For example, multiprocessor configurations, vector processors, and array processors.

[9]One microsecond equals one millionth of a second.

dramatic reductions have been taking place in the electronic parts of computers. On a single monolithic chip of silicon a quarter-inch square were first deposited integrated circuits of tens, then hundreds, then thousands, and now tens or even hundreds of thousands of individual circuits or memory elements. Such an improvement has led to an unprecedented number of innovative applications—witness the proliferation of pocket calculators, digital watches, and electronic games. Today, there are semiconductor silicon chips with over 2,000 characters of memory—a density of 320,000 characters per cubic inch as compared with the 350 characters per cubic inch of punched cards.

To acquire data, there are now optical character readers that recognize a variety of printing fonts and convert printed text into computer-readable form at a rate of over 400 characters per second. Output from a computer can also be printed at phenomenal rates of speed. The IBM 3800 Page Printer, for example, is reported to be able to print one hundred sixty-seven 8-1/2 by 11 inch pages a minute at a maximum speed of 10,020 lines per minute (assuming the standard 6 lines to the inch).

In recent years, there has been a marked change in the cost picture. While the unit cost of computing has declined steadily over time, at any one calendar point an increase in computing power implied a corresponding increase in cost, because the greater capability required a larger computer. In the early 1970's, however, the situation changed abruptly. The development of the minicomputer and its use of integrated circuits, and more recently the growth of microelectronic technology, has led to dramatic reductions in both the size and the cost of computer systems. Moreover, because the cost of a microelectronic element is relatively independent of its complexity, dramatic increases in computing capability can be obtained with inconsequential increases in cost.

In addition, microelectronic components pour forth from automated production lines, making some of the smaller computers almost of a mass production variety. Witness, for example, the pocket calculator which is actually a small, special-purpose computer that in some cases is actually programmable. Hobbyists now buy and build computers the way people used to buy and build model trains. Electronic bill paying from one's home is already a reality, and home computers that anybody can use are on the horizon. Video-display games that connect to one's television are a form of computer, and the future will bring increased use of cable television facilities for information processing. An individual's television set, or a modified version thereof, will become his home computer terminal, and automated libraries and electronic mail will become practical realities—as will record-keeping systems for the home and every small business.[10]

Improvements in computer hardware have been accompanied by advances that make their use easier, and their utilization more efficient.

[10]A recent report in *Time* magazine put the number of home computers already sold at approximately 50,000, with industry analysts predicting sales of three times that many in the next year alone. Some 500 retail outlets have opened in the past couple of years to sell and service such computers, and at least 150 computer clubs and a dozen home-computer magazines have been launched. Prices for such computers typically range from $400 (if one's

Programming in machine language has been supplanted by the successive development of, first, program assemblers and, later, compilers which translate programming statements expressed in a higher order language into machine-acceptable form. Specialized languages for scientific calculations, business applications, or text processing have been developed to give the human user more convenience and to relieve him of great burdens of intricate detail.

Special programs—the computer "operating system"—have been developed to maximize the use of computer resources and to relieve the user of having to manage the availability and utilization of all parts of the system configuration (e.g., having to schedule transfers to and from tape units or to allocate storage space to different portions of his program). "Multiprogramming" and "time-sharing" modes have evolved to permit many programs to be processed simultaneously, and thus to give many users at remote terminals the ability to interact with the system simultaneously, and without realizing that the system is at the same time providing service to other users. New concepts (such as virtual memory and virtual machines) have evolved to further relieve the programmer of the burden of managing memory space, and to better isolate and insulate users from each other. Special languages and programs for managing data bases—called "data-base management systems"—have been developed to implement conceptual advances in data organization. The net effect of all such advances is to:

- enable the user to concentrate his attention on the details of performing the task at hand;
- relieve the user of tedious burdensome details of managing system resources;
- cause the system to "take care" of the user in a wide variety of ways automatically; and
- enable a user to interact with the system in a style and at a rate matched with his own intellectual processes.

Table 1 summarizes the more important concepts introduced by successive computer generations.

The Difficulty of Forecasting

No one could have foreseen in the late 1870's that the development of a commercially successful electric motor would culminate in less than a hundred years with one powered by a tiny battery and operating in a lady's wristwatch; neither could the Wright brothers visualize the jumbo jet. In a similar way, Professor Douglas Hartree, the developer of the first analog computer (called a differential analyzer) and an expert in computing, predicted in 1951 that not only could all the computations ever needed in England be performed by the three computers then under construction, but also that no one else would ever need a computer of his own or be able to

---

own television set is used as the viewing screen) to $2,500 for more sophisticated models. *Time*, September 5, 1977, p. 39.

Table 1

GENERATIONS OF U.S. COMPUTER TECHNOLOGY

Generation	Time of Introduction	Hardware Technology	Software and Architecture
1	1951-52	Vacuum tubes; modularity* on individual circuit component level.	Machine language programming, symbolic assemblers, subroutines, program libraries. Special-purpose architectures.
2	1958-60	Transistors; modularity on individual component level.	Higher-level language (FORTRAN, COBOL, ALGOL), monitors, macroassemblers, executive programs. General-purpose computer architectures; families of systems.
3	1963-65	Integrated semiconductor logic circuits; modularity on multiple logic circuit level.	Operating systems, many programming and simulation languages, modular programs. Centralized, multiprocessor architectures; families of systems.
4	1970-72	Medium- and large-scale integration; modularity on subsystem function level.	Extendible language, metacompilers, subprograms in hardware, conversational systems. Networks of computer systems. Vitual memory systems.

*Basic units of construction

afford one. Subsequent predictions about the growth of the computing industry were similarly understated, because computers were initially seen as devices for engineering and scientific calculations, not as devices to manipulate data for business and government information requirements. For example, IBM estimated in 1955 that there would be four thousand computers in operation in the United States by 1965, whereas there were actually 20 thousand.

Such underestimations of the demand for technology are, of course, not unusual,[11] but forecasting the demand for computer technology has been particularly difficult because of the speed at which the technology has advanced—faster than any other technology ever has. In slightly more than 25 years,[12] we have witnessed the following:

- maximum processing speed has increased over *50 thousand-fold*;
- high-speed memory capacity has increased over *10 thousand-fold*;
- reliability has been increased over *a thousand-fold*;
- physical volume has been reduced over *100 thousand-fold*; and
- cost per operation—price-performance—has been reduced over *100 thousand-fold.*

Computers that required hundreds of cubic feet 25 years ago have been supplanted by ones that take only a few cubic inches—and go a hundred-fold faster.

To say that computing power and computer-accessible memory have become plentiful and cheap and small only begins to convey the true awareness and reality of what has happened. As new applications have become technically or economically feasible, they, in turn, have spurred the computer industry to further advances which give one or another vendor a competitive edge in the marketplace. While it is hard to believe that computer technology can continue its steady rate of progress—because mankind has never experienced such a thing before—the positively reinforcing cycle of technological advance and its applications shows no signs of abating. It has already produced pocket calculators selling for under $10 a piece. It will produce new applications and new innovations yet unperceived. Indeed, reasonable estimates anticipate that further growth of at least one hundred-fold and perhaps one thousand-fold can be obtained from technology now known and understood.[13]

The interested reader will find a much more detailed discussion of

[11]Other dramatic underestimations of the technological advances are discussed in detail in: Martino, J.P., *Technological Forecasting and Decisionmaking,* (American Elsevier, New York) 1972.

[12]UNIVAC I was designed in 1949. Its maximum processing speed was approximately 2,000 additions per second, the high-speed memory capacity was 12,000 digits, its volume and weight were 940 cu.ft. and 16,300 lbs., respectively, and the power consumption was 81 KW; CPU cost was $750,000. For detailed description, see Weik, M. H., *A Second Survey of Domestic Digital Computing Systems,* Report No. 1010, Ballistic Research Laboratories, U.S. Army Aberdeen Proving Grounds, Md., June 1957.

[13]"The Ultimate Computer," *IEEE Spectrum,* March 1972, The Rand Corporation, P-4825.

advances in information technology in the Appendix to this volume. The major elements of a computer system are discussed, showing past evolution and projected developments through the mid-1980's.

Chapter 3

Technology and Privacy

Personal Privacy in an Information Society, the Privacy Protection Study Commission's final report to the President and the Congress,[1] looks toward a national policy to guide the way public and private organizations treat the records they keep about individuals. Its findings reflect the fact that in American society today records mediate relationships between individuals and organizations and thus affect an individual more easily, more broadly, and often more unfairly than was possible in the past. This is true in spite of almost a decade of effort to frame the objectives of a national policy to protect personal privacy in an information-dependent society. It will remain true unless steps are taken soon to strike a proper balance between the individual's personal privacy interests and society's information needs.

The Commission concluded that if personal privacy is to be protected, national policy must focus on five systemic features of personal-data record keeping in America today.

> *First*, while an organization makes and keeps records about individuals to facilitate relationships with them, it also makes and keeps records about individuals for other purposes, such as documenting its own actions and making it possible for other organizations—government agencies, for example—to monitor the actions of individuals;
>
> *Second*, there is an accelerating trend, most obvious in the credit and financial areas, toward the accumulation in records of more and more personal details about an individual;
>
> *Third*, more and more records about an individual are collected, maintained, and disclosed by organizations with which the individual has no direct relationship but whose records help to shape his life;
>
> *Fourth*, most record-keeping organizations consult the records of other organizations to verify the information they obtain from an individual and thus pay as much or more attention to what other

[1] *Personal Privacy in an Information Society*, The Report of the Privacy Protection Study Commission (Washington, D.C: U.S. Government Printing Office, 1977) (hereinafter, *Personal Privacy in an Information Society*).

organizations report about him than they pay to what he reports about himself; and

Fifth, neither law nor technology now gives an individual the tools he needs to protect his legitimate interests in the records organizations keep about him.[2]

This chapter focuses on the role that technology plays in shaping these five features of personal-data record keeping and explores the ways in which the application of computer and telecommunications technologies affect the growing tension between an individual's privacy interests and society's information needs. The chapter examines the effect of technology on the collection and storage of information, the processing and retrieval of information, and the generation of "new" record systems, and then explores the implications of those effects for personal privacy, particularly in relation to access to public records, the disclosure of information to third parties, and the development of individual "profiles" whose use can markedly enhance the reach and effectiveness of organizational authority.

Impact of Technology on Record Keeping

Collection and Storage of Information

Historically, most of the information that organizations have recorded about individuals has been collected and filed away on forms: application forms for employment, credit, and insurance; reporting forms for taxes, accidents, and medical expenses; and transaction forms for purchases and deliveries. Often, some of the information on these forms was assigned a special code to simplify the record-keeping process. With the advent of automated record keeping, however, the process of collecting and storing information about individuals was broken up into several steps: collection (which still, by and large, involved writing the information out on a form); coding; and, finally, transcription onto a machine-readable medium, such as a punched card, or direct entry into the machine itself. While this three-step process is still the usual one in many automated record-keeping operations, a number of developments have served to modify and simplify it. In an airline reservation system, for example, data collection, coding, and entry (into the computer) are all accomplished in one step. In the credit-card business, each card holder is assigned a unique number that is embossed on his card and substitutes for his name and address when information about the use of his account is transcribed into machine-readable form.

The elimination of the necessity to transcribe information manually is also an increasingly common phenomenon. One of the earliest simplifications was the use of machine-readable account numbers on checks and other banking documents. This was made possible initially by the use of magnetic ink, but today there is equipment available that can read the impressions made by an ordinary typewriter or by an individual printing in clear longhand. Bar codes to facilitate the identification and pricing of merchan-

[2] *Ibid.*, p. 8.

dise sold by supermarkets and department stores and the magnetic stripes on the backs of some credit cards are still other simplifying devices. With magnetic stripes, it is no longer necessary to transcribe the embossed account number manually, since the stripe already contains that information in machine-readable form, and machines have been developed to "read" such cards.

It is difficult to say exactly where these improvements in data collection techniques will lead, but a few trends seem clear. One is growth in the number of individuals who use the services that automated collection techniques facilitate. In the banking industry, for example, the initial impact of magnetic ink character readers was simply to make the data collection process associated with automated check processing more efficient. That increased efficiency, however, made it possible for banks to pursue the personal checking-account market more aggressively and that, in turn, led to a dramatic increase in the number of checks being written. Without magnetic ink character readers, there is no question that today there would not be enough clerks to process all the checks that circulate daily.[3]

In other areas also, the exploitation of automated data collection techniques has prompted an expansion, and often a lowering of the cost, of the services being offered, and thus a corresponding increase in the number of individuals using them. The telephone company's ability to make a machine-readable record of every long-distance telephone call, automatically, has greatly reduced the time necessary to make a long-distance call, and thus has permitted a rapid increase in the number of calls that people make and in the number of people who make them. Some transactions, such as car rentals and airline ticket purchases, have also become much easier for a consumer to execute if he uses a credit card rather than a check or cash. This trend, which has been abetted by the need for some form of positive identification in certain types of consumer transactions, as well as by concern about the risks that having large amounts of cash on hand may pose in today's society, can only grow as point-of-sale (POS) electronic funds transfer services become commonplace. With POS services, a consumer will not only pay for his travel and entertainment without using cash, but also his more mundane transactions like supermarket and drugstore purchases.[4]

A second major trend associated with these advances in information collection techniques is a great increase in the variety of transactions that generate records about individuals—or, more precisely, readily accessible (because they are automated) records about individuals—and thus the amount of detail about an individual's personal life that will build up in the files of record-keeping organizations. For some years now, the availability of inexpensive microfilm equipment has made it possible for a bank to

[3]In 1970, an estimated 21.5 billion checks were written on demand deposit accounts in commercial banks in the United States. Approximately one billion additional checks were written by the Federal government. It has been estimated that the total cost to society of the check-payment system is $10 billion annually. See Arthur D. Little, *The Consequences of Electronic Funds Transfer: A Technology Assessment of Movement Toward a Less Cash/Less Check Society*, (June 1975), Chapter 4.

[4]For a more detailed discussion of credit and debit cards and electronic funds transfer (EFT), see *Personal Privacy in an Information Society*, particularly pp. 113-124.

maintain a retrievable copy of each check an individual writes, but in the future the amount of detail in today's check-processing systems will seem miniscule in comparison to the amount acquired or "captured" in the course of everyday consumer transactions in which paper checks may play no role whatsoever.

"Transaction" or "event-related" data, as they are called, are a new phenomenon inasmuch as the individual actions that generate them have not traditionally generated any kind of permanent record. Moreover, the individual is often unaware that he is generating these machine-readable trails that provide an increasingly more detailed profile of his life.

Finally, there is another fairly recent development in data collection which may be even more far-reaching in scope. As already noted, many record-keeping systems require that information be coded for ease of data entry and for the purpose of ensuring unique identification. There are some indications that this may become a superfluous task in some settings. For example, it is now possible to scan textual information to generate codes or establish a unique identification. This capability simplifies the data collection process, since it eliminates a very tedious step in many existing record-keeping systems, and opens up new vistas for the emergence of new types of record-keeping systems based on textual information.

Processing and Retrieval of Information

The most significant implication of transaction data captured in machine-readable form stems from the fact that they can be readily utilized for multiple purposes, some of which may be unrelated to the transactions or events that generated them. The transactional records the telephone company generates, for example, can, in principle, be retrieved by the telephone number of either the calling or receiving party, and thus be an invaluable resource for investigators of various kinds. Likewise, credit-card and automated credit-bureau records can be used to develop mailing lists and statistical profiles for use in marketing campaigns. In an electronic funds transfer environment, of which point-of-sale systems would be an important part, it may even be possible to track an individual's movements by, for example, monitoring the time and place of his purchases. Monitoring of long-distance telephone calls could provide similar information.

The ability to perform these types of selection and tracking operations is a direct result of the impact computer and telecommunications technologies have had on the way records about individuals are physically distributed and organized. In the manual record-keeping era, the record keeper had to choose whether to keep all records at one central point, which could slow service to a client at all local offices, or whether to decentralize the record-keeping function and thereby make it easy to service a client at the local office where its records on him were maintained, but not elsewhere. Similarly, a decision had to be made as to how the records should be physically organized. Should they be filed alphabetically by client name, numerically by client number, or by some type or mix of client services being provided? Often the requirements of the various users of the records

led to the creation of duplicate files or several files on the same client population, each physically organized in a different way. This, of course, was costly and called for complicated updating routines, so that in many cases user needs for information simply were not fulfilled.

Today, however, most of these problems are easily solved. Records can be stored in computer-accessible form and made available in a number of ways not previously possible. First, the records may be made available to remote locations different from the physical location of the records themselves. Computer terminals connected via telecommunications facilities—often a standard telephone line—can provide "on-line" access to a data base.

Second, and more significantly, the physical organization of the records in the data base, as well as the physical organization of the items of data within the record, are ceasing to be limiting factors on the way data or records are stored or retrieved. In manual systems, or in early automated systems which mirrored manual ones, the manner in which data were physically stored markedly limited what could be done with them. Consider, for example, the difficulty of finding all individuals in the telephone book the second digit of whose telephone number is a "4"; or, as a harder task, find your next door neighbor's telephone number without using his name as the search key (i.e., find the entry in the telephone book whose street address is closest to your own).

While computers can easily be programmed to sort or reorganize data on the basis of any particular index, attribute, or characteristic, such physical reorganization can be costly and inefficient. Newer data-base management systems employ data storage structures that permit subsequent update and retrieval of the data according to various search indices or criteria. While the human user may visualize the result as several physically reorganized data bases, this is again an illusion. The same physical data are being dynamically searched to produce the desired result, with the result being: (1) the user need no longer be concerned about the manner in which the data are physically stored; and (2) in some cases, new information has effectively been "created" in the sense that the information could simply not be realistically obtained in a manual environment (e.g., all telephone numbers whose second digit is "4"), even though it was theoretically "always there."

In practice, the centralization of records combined with the decentralization of service functions and the ability to retrieve records in a variety of ways has been perceived as the solution to numerous problems. Not long ago the only way to deposit or withdraw money from a savings account was to present a passbook at the branch where the account was physically located. Today, however, a withdrawal can be made at any branch that has access to the bank's computer-based customer records. Airline reservations can be made and cancelled at any branch office or ticket counter throughout the world, and a credit-card transaction can be authorized at any subscribing merchant location at any hour of the day.

In addition, a large number of record search operations that used to be carried out by having file clerks manually review the contents of thousands

of records can now be carried out with little or no personal intervention and on a scale that would have been impossible when the task had to be performed manually. Before State Motor Vehicle Departments automated their vehicle registration files, for example, it could take days or even weeks to identify all of the automobiles matching a particular description as to make, model, year, and color. Yet, today, such a search can be carried out in minutes, and the technique can be used by many organizations for many purposes. Late bill payers, accident-prone drivers, outstanding employees, purchasers of large appliances, or taxpayers taking unusually large deductions can all be identified in minutes, provided the organization's computer-based record-keeping system contains the items of information that are to be used to select their records from all the others.

The Commission learned of many search operations of this sort during its hearings on personal-data record keeping in both the private sector and government. Automated credit bureaus, for example, take mailing lists provided by credit grantors and retailers and produce a "targeted" list of individuals on the original list who possess certain specified characteristics, such as income level and prompt payment of their bills. This technique, called "pre-screening," enables the credit grantor or retailer to employ the resulting list for more effective marketing because certain basic attributes of the individuals on it are revealed by the selection process. In the Federal government, such techniques have been employed to determine whether government employees were receiving welfare benefits (properly or not). The IRS has developed techniques whereby tax returns, after they have been computerized, are automatically reviewed for possible audit if they do not conform to certain standards. Indeed, the ability to search through hundreds of thousands, or even millions, of records to identify individuals with particular characteristics of interest is at once the most important gain, and the most important source of potential harm, stemming from the automation of large-scale personal-data record-keeping systems, and it is likely to grow in importance as "textual search" techniques are refined.

Besides making it possible to select records on the basis of individual characteristics or attributes represented as individual data elements, advances in information-processing technology have also made it possible to search running text for information concerning a given individual. This contrasts with the usual approach to automated storage and retrieval in which every item of information is arranged in a particular format (e.g., a specific number of characters in a fixed location within a record), and it opens the way to much broader information-processing capabilities. The record-keeping operations of the Senate Select Committee on Presidential Campaign Activities (often called the Senate Watergate Committee) illustrate the advantages that textual search techniques can offer.

The Committee's early investigations generated thousands of documents (records) which were initially organized and cross-indexed by topic. Very quickly, however, this manual system became difficult to use because of the volume of material under each of the subject headings. Somehow the material had to be made more readily amenable to analysis, and transcribing it into machine-readable form proved to be the most attractive solution.

Doing so, however, dramatically altered the whole record-keeping process. First, it become less important to pre-classify the material by subject matter, since the computer could be programmed to examine the content of the documents and sort them. Second, the system was no longer limited by the original set of topics, since the computer could be programmed to search along other lines as well. And third, it became possible to retrieve textual information on the basis of its association with a particular event, individual, date, place, or time. This capability, needless to say, significantly facilitated the investigation.

Textual search techniques are being used today by a number of Federal agencies. Both the Department of the Interior and the Federal Trade Commission (FTC) currently transcribe much of their incoming correspondence and then use computers to control internal agency routing and monitoring of the replies. The Department of the Interior hopes to use its system to discover when the same letter has been sent to several people (e.g., to a Representative, two Senators, one Cabinet Officer, and the President), so that all the replies to it will be consistent. If the subject matter is within the Department's purview, all the recipients of such a letter would ultimately forward it to the Department for appropriate action or reply, but unless the letters are all routed to the same office, and many times in the past they have not been, there is the risk that the writer will get back some contradictory responses. The FTC is also using its system to respond to consumer complaints alleging unfair trade practices, but, in addition, it is using its system to analyze the letters it receives for evidence of repetitive patterns of consumer abuse.

Finally, the ability to correlate information provided by the new technologies allows organizations to develop profiles of large classes of individuals much more easily and less expensively than was possible in the past. And the knowledge thereby gained can be used to modify the way decisions are made about individuals. For example, many credit grantors are experimenting with a technique called "point scoring." This technique determines an applicant's credit worthiness on the basis of a small cluster of personal characteristics which statistics show to be a reliable measure of ability and willingness to pay. A credit grantor using this system rates its applicants as credit risks according to the total number of points they score on the characteristics it considers predictive. The characteristics in a particular point-scoring cluster and the numerical value assigned to each may vary from credit grantor to credit grantor and from one geographic area to another, and a credit grantor may revise its formula from time to time to take account of its experience with customers and of changing economic conditions.

An advantage of point scoring is that it may eliminate the need for a credit report. However, it also may effectively eliminate the individual's opportunity to challenge the basis of an adverse credit decision. The Equal Credit Opportunity Act, which now permits a rejected applicant to request the reasons for an adverse credit decision, relies on the theory that an adverse decision can be explained in terms of one or more particular characteristics in an overall score. Yet, with point scoring, all the

characteristics included in a formula contribute to the score, so that a decision is the result of a *combination* of factors weighted in a particular way. A change in the credit grantor's weighting of any one of the factors could alter the decision, and thus make existing legal protections impossible to apply.

Generation of "New" Record Systems

As noted, the ability to assemble information selectively, or the ability to correlate existing information, can at times be functionally equivalent to the ability to create new information. For example, before the advent of computers it was possible for a State Motor Vehicle registry to find out if someone owned two or more cars, but it was only practical to do so for a very small number of owners. Today, however, it is easy for a State to assemble the information in its files on multiple ownership, and then to correlate that information with its records on licensed drivers. The ease with which this can be done depends on the availability of identifiers common to both systems—the vehicle registry and the driver registry—but such correlation is increasingly possible at a reasonable cost. Examples from the Commission's hearing record include a bank that is developing a computerized customer information system which will permit it to correlate a customer's use of different services throughout its 137-branch system. In the bank's words:

> This system will contain a synopsis of deposit and loan account information obtained from the customer and credit bureaus and other creditors, if applicable, together with commentary prepared by bank personnel about the bank's relationship with that customer.
>
> The system will be used to record additional information about the customer, such as change of address or use of additional bank services.
>
> In addition, the system will be used by the banks to identify certain classes of customers to which new services might be marketed. We think it only reasonable for the customer to assume that a banking institution will be interested in offering its full range of services to customers and will take steps to identify customers who might be interested in using those services.
>
> For example, a customer maintaining a high account balance may be a good prospect for trust services as well.
>
> Additional records pertaining to loan customers are generated whenever a borrower fails to meet the terms of his obligation, and, again, we believe the customer in default knows that the lendor will maintain a record of that default. Charged-off loans are reported to credit bureaus after the customer has been advised that failure to meet his obligation will have an adverse affect on his credit rating.

> In summary, records from which a particular customer is identifiable contain information provided through the customer himself, through his own past relationships with the bank, or through outside sources which he can fairly assume will supply information relevant to credit transactions.[5]

When an organization offers a multiplicity of services to a single population of clients, it is only logical for it to want to maximize its use of the information in its client records, and, in many cases, doing so can be a convenience to clients. Indeed, many of today's integrated record-keeping systems have client convenience as one of their principal objectives. Many, however, are also aimed at protecting the record-keeping organization from undesirable client behavior.

The National Driver Register maintained by the U.S. Department of Transportation, for example, is a system whose objective is to apprise a participating State driver licensing authority of the fact that an individual has previously been denied a license in another State or has had his license suspended or revoked. An independent credit-card authorization service exists to inform a subscribing organization, such as an airline or a car-rental agency, that a credit card presented to it is invalid. The account monitoring services offered by some credit bureaus are designed to inform a credit grantor when an individual's charges against accounts he has with other credit grantors indicate that he may be exceeding his capacity to pay his bills.

One does not usually think of systems of this sort as "integrated" systems, since most do not contain a record on every client of every organization that uses them. Logically, however, they function as integrated systems, because they consist of records made up of information flowing into them from a variety of separate record-keeping operations, and, by virtue of that fact, provide a context (i.e., new information) that a subscriber can use to interpret and evaluate the information on an individual in its own files. Most, moreover, exist to facilitate preemptive actions against individuals by their subscribers. A State licensing agency queries the National Driver Register in order to avoid issuing a license to someone whose license is currently suspended or revoked due to a serious driving violation in another State. An independent authorization service exists to enable a merchant to avoid accepting an invalid credit card, and an account monitoring service aims to give a credit grantor the option of lowering an individual's authorized credit limit. Their objective, in other words, is to allow an organization to alter its behavior in relation to a client in a way that the organization could not confidently do if it were forced to rely exclusively on the information in its own records.

A further refinement in the direction of *de facto* integration of record-keeping systems is the use of computer communications to allow one organization to query the files of another one on any individual named in its

[5]Testimony of the Bank of Virginia Company, *Depository and Lending Institutions*, Hearings before the Privacy Protection Study Commission, April 21, 1976, pp. 326-328, 365-367 (hereinafter, "Depository and Lending Institutions Hearings").

records; not just someone who is of interest because of some type of delinquency. For example, in geographic areas in which they are not in direct competition, two major automated credit bureaus have established a computer-communications line which allows each to search the other's files automatically when it receives a subscriber's inquiry about an individual on whom it has no information in its own files.[6] Government agencies have also begun to develop such automated record linkage systems. The proposed message-switching capability of the National Crime Information Center, for instance, would provide Federal and State law enforcement agencies with direct access to each other's fugitive, stolen property, and related criminal record files.

The Personal Privacy Implications of Automated Record Keeping

A major problem created by the widespread application of computer and telecommunications technology to personal-data record keeping is the inability to anticipate and control future uses of information. Systems evolve on the basis of immediate need, often with little or no explicit consideration of their long-term consequences for individuals, or for society as a whole. Nonetheless, it is clear that there are inherent dangers, and while it may sometimes be difficult to visualize them in their full array, it is essential to understand the kinds of choices they may present and, broadly, the kinds of public-policy initiatives that will tend to keep them from being realized.

The following discussion will focus on three particular areas in which the automation of record-keeping practices and systems raises important public-policy issues. These are: (1) access to public records; (2) third party inter-organizational transfers of information; and (3) growth in institutional capacity to affect people's lives. This list is not intended to be exhaustive, but it is instructive. It demonstrates the broad range of issues and questions which the use of information technology can raise.

Access to Public Records

Access to public records is one area in which citizens and policy makers alike are beginning to acknowledge some unexpected and perplexing consequences of automating records about individuals. State and local governments maintain extensive records on individuals and by law or by custom a large number of them are open to public inspection. Among the records that may be available for the asking are ones that give details on the ownership, financing, and taxation of real property, voting registration, motor vehicle ownership, drivers' licenses, marriages, births, deaths, arrests, and convictions, and numerous licenses—for hunting, fishing, barbers, plumbers, and so on.

The record-keeping practices of the government agencies responsible for the maintenance of these records vary considerably. Real property records, for example, are filed by the geographic location of the property,

[6] *Personal Privacy in an Information Society*, p. 58.

and it does not follow that a second set of records is kept in alphabetical order by the name of the parties, or that it is easy to search real property records by attributes other than location or the date of a real estate transaction. Moreover, the physical dispersal of public records among a variety of State and local government agencies has meant that they are seldom requested out of idle curiosity or even vague expectations as to their possible usefulness. The user generally has some practical reason for wanting access to them and is interested in particular records, not entire files. Thus, while agencies of State and local government have extensive detailed public-record information about the property we own, the taxes we pay, our political affiliations, the composition of our households, the number of cars we own, and our driving histories, the physical manner in which these records have been distributed and organized has served to minimize their utility as vehicles for intruding into our private lives. As long as the user of the public records has had to search them manually, a fair amount of effort has been needed to construct a personal profile of any one individual.

Recently, however, many large public-record systems have been automated to allow agency uses of the records that would have been impractical when they existed only in manual form. Although the capabilities of these new systems range from the mundane to the highly complex, there are now some jurisdictions in which it is possible to acquire all of the public records maintained on a given individual by simply providing his name. The result, of course, is that more complete information on an individual is at least potentially available to the public, much of it in machine-readable form, and the question that public-policy makers must now resolve is whether the old policy of access to manual (usually paper) records by the public on demand should extend to the automated records as well.

With respect to some types of public records, the answer is clearly "yes." Voter registration files, for example, have become increasingly accessible to the public as a consequence of successive applications of increasingly sophisticated information-processing technology, and there are sound reasons why they should not become any less so. Should the same policy, however, apply to any automated public record? Should a citizen be able to walk into a real property records office and obtain a copy of all records in its automated system on his neighbor John Smith? Should he be told "Here are folios and folios of files; look through them to your heart's content."? Or should the records office share its automated retrieval capability with him? Should the answer the real property records office gives be the same as the answer the office that maintains the municipality's integrated information system gives to a request for a copy of all its records on John Smith?

Obviously, the new technologies raise interesting, and so far unresolved, public-policy issues with respect to the dissemination of heretofore public-record information. They are issues that will be difficult to resolve, and it is likely that many different types of solutions will be necessary. The Privacy Protection Study Commission addressed two such problem areas in

its final report and reached different conclusions with respect to each. On one hand, it recommended that Congress enact a statute which includes a prohibition on the disclosure of individually identifiable information about public assistance and social services clients to members of the public, a provision that would restrict disclosure of certain information which is currently a matter of public record in some States.[7] On the other hand, in considering the use of public records to compile mailing lists, the Commission did not suggest any restriction on the disclosure of public records, but rather recommended that each State agency which maintains records that are used for direct-mail marketing and solicitation purposes

> devise a procedure whereby an individual can inform the agency that he does not want a record pertaining to himself to be used for such purposes and have that fact noted in the record in a manner that will assure that the individual's preference will be communicated to any user of the record for direct-mail marketing or solicitation.[8]

The Commission reached these two distinct conclusions on the basis of its judgment that when public availability of information was not compatible with the purpose for which it was collected, the information should not be made public, but where information is properly a matter of public record, First Amendment concerns and the potential for misuse through particular disclosures must be balanced against the privacy interests of the individuals to whom the information pertains. With regard to records about public assistance and social service clients, the Commission agreed with the legislative policy adopted by the Congress that such information should not ordinarily be publicly disclosed because such disclosure would be incompatible with the purposes for which the records were compiled. Conversely, the recommendation on mailing lists took the form it did after considering the several different ways of informing a mailing list compiler that an individual does not want his name used for direct-mail marketing or solicitation. One was to have the list compiler send a notice to each individual named in its records, but that would be inordinately costly. Another was to have each State and local government agency offer a negative check-off option to each individual whose name appears in its public records; that is, offer each individual an opportunity to indicate to the agency that he does not want information about himself disclosed in individually identifiable form. This, however, would run afoul of one of the main objectives of public-record statutes, since it would require an agency to distinguish between an individual acting as a mailing list compiler's representative and the same individual asking for information in his capacity as a private citizen. Moreover, to have the negative check-off apply to all public requests for access to a record, so as to avoid having to distinguish between different types of requestors, would even further undermine the purpose of public-record statutes.

Fortunately, the Commission found an alternative which took account

[7] *Ibid.*, p. 476.
[8] *Ibid.*, p. 153.

of the mailing list user's (i.e., the compiler's and client's) desire for selectivity. The Commission concluded that if it is possible to rely on the mailing list user's much stressed desire not to send messages to individuals who do not want to receive them, it should be enough to note next to an individual's name on a public record that he does not want his name used for marketing or solicitation. The list compiler would still be able to copy the record, just as any other member of the public can, but it would be on notice that the individual had objected to having his name on a mailing list, and presumably, for economic reasons, would not include that name on any such list it develops for one of its clients. This resolution allowed the Commission to avoid wrestling with the difficult, and perhaps insurmountable, problem of distinguishing between citizens and organizations that should have access to public records and those that should not.

Disclosures to Third Parties

The access issues which the automation of public records poses are but one facet of a larger set of policy questions raised by the disclosure of records about individuals maintained by any organization. While third-party access issues are basic ones in any modern society that values personal privacy, they are exacerbated and, indeed, multiplied, by the application of computer and telecommunications technologies to personal-data record keeping.

In speaking of dangers to personal privacy caused by the disclosure of recorded information to third parties, certain value choices and assumptions are ordinarily made. Usually, protecting personal privacy is thought of as restricting disclosure by the record keeper, except to persons with a legitimate right to know. The focus of public-policy concern is not necessarily on *prohibiting* disclosure, but rather on ensuring that information is disclosed only to those with a legitimate right to receive it. In the past, a few legal barriers to the disclosure of records about individuals to particular parties (such as government agents) have developed but, because of the constraints upon disclosure created by limitations of time, money, and effort, most restrictions have been informal. As the Commission indicated in various sections of its final report, however, patterns of contemporary record keeping have undermined the usefulness of existing legal barriers and the deployment of information technology tends to nullify the informal restrictions.[9]

Currently, information about an individual maintained by all sorts of record-keeping organizations can legally be disclosed to a third party largely at the organizations' discretion. Historically, because of the costs of disclosure, both to the record keeper and to the third party, such information was released only when the third party had a specific need for it. The cost of retrieving information made it worthwhile for the record keeper to refuse some requests and to limit its response to others, and thus, in many cases, there was a satisfying coincidence of high-minded principle and economic interest. For example, the banker who was not inclined to use

[9] *Ibid.*, Chapters 2, 3, and 9.

his resources to assist some official in a broad search of his customers' records could easily refuse to disclose the records on the grounds that their disclosure would violate the customers' trust.[10] Today, however, it may be much more difficult to say "no," because the cost of saying "yes" is much lower than it used to be. When the banker's records are no longer ledger entries and boxed receipts, but electronic and microfilm files that can be retrieved almost instantly at remote terminals, the cost of retrieval becomes minimal and, thus, the pressure to accede to requests, particularly official ones, becomes greater. When it costs the banker little or nothing to disclose detailed record information, when there are no legal barriers to such disclosure, and when the goodwill of those on whom the banker must rely for cooperation or services, such as law enforcement officers, can be increased, the pressures to disclose become enormous and often insurmountable.[11]

In addition, the realities of the manual record-keeping world helped to assure that those third-party disclosures that were made were legitimate. A request would have to be processed by a number of people, any of whom might question its legitimacy and all of whom might remember it if any subsequent inquiry about it were made. That too, however, is changing as a direct consequence of automation. Fewer and fewer people are now involved in making many disclosures. Indeed, direct linkage of computerized records through telecommunications can result in the human element being totally withdrawn from a particular disclosure or disclosure decision, and that has consequences not simply for the legitimacy of the disclosure, but also for the accuracy and relevance of the information disclosed. Moreover, even where people remain part of the disclosure process (as is likely in most instances in the foreseeable future), the reduction of those involved to a few persons, or even a single individual, will reduce the potential oversight which previously existed in the process.

The dangers of improper disclosure of recorded personal information, however, do not lie exclusively in improper disclosures from a private record keeper to government. Disclosures from a private record keeper to another private person or organization could be equally improper and damaging,[12] as could disclosures from one governmental jurisdiction, or one government agency, to another. The changes in record keeping wrought by information technologies alter an individual's relationship with all of society, not just government, although alteration of the relationship between the individual and government may be the most visible, and potentially the most perilous, as it relates to the protection of personal privacy and other individual liberties.

---

[10]See, e.g., *Brex v. Smith*, 104 N.J.Eq. 386, 146 A. 34 (1929); *United States v. First Nat'l Bank of Mobile*, 295 F. 142 (S.D. Ala. 1924), *aff'd, per curiam*, 267 U. S. 576 (1925).

[11]See, *Personal Privacy in an Information Society*, pp. 347-350, 357-358; testimony of Internal Revenue Service, Depository and Lending Institutions Hearings, April 22, 1976, pp. 777-830.

[12]See, e.g., *Peterson v. Idaho First National Bank*, 83 Ida. 578, 367 P.2d 284 (1961), involving gratuitous disclosure by bank of a customer's financial condition to his employer; *Hammonds v. Aetna Casualty and Surety Co.*, 243 F. Supp. 793 (D.C. Ohio 1965), wrongful disclosure by health-care provider to insurance company.

Increases in Organizations' Capacity to Affect People's Lives

To understand the full extent of the change which is occurring and will continue to occur in the record-based relationships between individuals and organizations, one must appreciate an additional development (besides the decreased costs, and increased ease, of accessing information) resulting from the use of computer and communications technologies—the creation of *more* and *new kinds* of recorded information. Point-of-sale electronic funds transfer (EFT) systems, for example, will produce a central detailed record on an individual's purchasing habits that could be of considerable value to private enterprises in designing marketing campaigns. Although one can argue that the information a point-of-sale system will generate is not inherently private (because an individual willingly enters into a market relationship when he makes a purchase), the multiplicity of transactions recorded by such a system will generate a highly detailed profile of an individual's consumption habits and propensities and thus raise questions about the commercial uses to which it may legitimately be put.

The record of personal activity generated in a point-of-sale system would also provide an invaluable resource for law enforcement and other government agencies who wanted to trace an individual's past actions and activities. These EFT records will combine many small pieces of personal information, each of which is public knowledge in the sense that somebody other than the person to whom it pertains knows about it, but which, when combined and analyzed, provide a mosaic of an individual's life. As point-of-sale EFT networks are deployed, it will be possible for anyone who gains access to the record of transactions generated in the network to determine what an individual has been doing, what he has been reading, where he has been, when he was there, and from these items of information to form a fairly accurate picture of his political, economic, and social activities, associations, and interests—all for relatively little cost in dollars, time, or effort. For this information to be disclosed to government, one would assume that a legitimate interest in and right to receive the information would have to be established. Neither existing law nor practice, however, ordinarily require that government establish the legitimacy of such an inquiry. As explored more fully in the Commission's final report, government access to such records in their currently scattered and less detailed form is already an issue of concern and controversy.[13]

The disclosure of such records provides organizations with an *ex post facto* surveillance capability, already commonly used in the law enforcement arena. Existing record-keeping practices, however, still make such *ex post facto* surveillance an expensive and time-consuming proposition, and therefore limit its use to those situations in which government is willing to expend substantial resources. Further, because access to these records ordinarily involves disclosure of and participation in the investigation by numerous private parties, some scrutiny of their legitimacy continues.

[13]See generally, *Personal Privacy in an Information Society*, and particularly Chapter 9, "Government Access to Personal Records and Private Papers."

Overall, however, the delicate balance between the power of government to acquire such information and the ability of the individual to protect it is already seriously disrupted,[14] and the continuing deployment of information technologies, without basic policy changes, will only exacerbate that imbalance.

Consider, for example, a shift from *ex post facto* to *real-time* surveillance capability. As more and more record-keeping systems are converted to on-line, real-time ones—real time in the sense that the transactional data they contain are available at the approximate time the transactions occur—the possibilities for *real-time* surveillance will grow commensurately.

Moreover, an organization's ability to conduct surveillance of any form is, to a certain extent, limited by the size of the data base to which it has access, and the size of the data base is, in turn, related to the actual size (i.e., in terms of storage capacity and processing ability) of the computer system being employed. This is especially true in the case of on-line, random access systems. Yet, the rapid evolution of distributed system technology will change this situation in a fundamental way.

By combining inexpensive and fast techniques for routing electronic messages over private or public communications systems, such as 'packet switching,' with sophisticated arrangements which allow computers to call each other and access each other's data bases, the finite size limitation on computer complexes is about to disappear. Although processor speeds and data storage have improved dramatically, it had seemed that there would always be some finite limit on the size of the total computer system that could be created. As long as this finite size was well below that required to keep track of *every* individual, the possibility of large-scale or widespread surveillance seemed acceptably remote. When this limit disappears, however, it will become practical for large organizations or for the government itself to consider monitoring the day-to-day activities of large groups of citizens.

The dangers posed by profiling an individual's activities, interests, and beliefs can also result from more clearly benign and limited developments in information policy and practice. The new techniques for handling correspondence, discussed earlier, employed by the FTC and the Department of the Interior can be seen as simply representing more efficient ways of dealing with the age-old problem of citizens' petitions for redress of grievances. Congressmen routinely refer grievances and questions to the executive agency or office best able to solve the problem—typically, in the context of a complaint, the agency complained about. The FTC may refer a consumer complaint which involves matters outside its jurisdiction to an appropriate State official. Neither practice on the surface seems obnoxious. But the theoretical "chilling effect" of such referral practices on the willingness of individuals to petition for redress of grievances could easily become a reality in an automated environment.

The Department of the Interior is also establishing a centralized text-

[14] *Ibid.*, particularly pp. 19-21, 346-350, 359-364.

processing system utilizing a large, central computer. This will allow internal agency policy memoranda to be prepared, distributed, and retrieved via the computer system. This could easily have a chilling effect on an employee's willingness to express his opinions and concerns frankly, knowing, as he will, that a variety of unknown persons at some later date will be able to retrieve, easily, internal memoranda advocating policy positions or recommendations contrary to their own.

The use of records to monitor the activities of individuals is obviously an area with profound public-policy implications, regardless of the number of persons in the group being monitored. As an issue, it goes to the heart of our basic constitutional liberties, and cannot be ignored until the "crisis" stage is reached. While information technology will provide important new tools to be used in the detection, deterrence, and prosecution of crime, for instance, the possibility of a marked erosion of civil liberties must also be seriously considered.

Chapter 4

Technical Considerations in Policy Formulation

The inquiry conducted by the Privacy Protection Study Commission was an effort to assist the Executive and Legislative branches of the Federal government in formulating public policy concerned with the collection, maintenance, use, and disclosure of recorded information about individuals. In this emerging area, technological considerations can sometimes make a significant difference in the choice of policy alternatives, and a few are so fundamental as to pervade the entire public-policy debate. This chapter is focused on those fundamental considerations as they have arisen in the Federal legislative forum, but the issues and problems discussed clearly have their counterparts elsewhere. Some of the topics considered are: (1) oversight; (2) who and what is covered by policy; and (3) establishing acceptable levels of performance. These topics have been selected as illustrations and do not constitute an exhaustive array of those that need to be taken into account by policy makers.

Oversight[1]

On Thursday, July 28, 1966, Mr. Paul Baran, then a computer expert with the Rand Corporation, testified before the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations. The Subcommittee, concerned about the possible dangerous consequences of centralized data banks, was considering a proposal to establish a National Data Center. The burden of Baran's testimony, however, was that the Subcommittee's focus on the centralization issue could be misleading; that we might "already be part way down the road toward building a system with all the obvious dangers of a single Federal data system, but without its clear visibility." Threats to personal privacy, Baran said,

> . . . will exist whether or not the central data bank is created by the government. Individual data systems, both public and private, now

[1]The term "oversight" is being used broadly herein to include any formal scrutiny or review process at any stage in the proposal, design, development, implementation, or operation of a record-keeping practice or system.

> being developed, can be tied together eventually into a network that will present essentially the same problems.[2]

Baran compared the then evolving system with the growth of early rail and telegraph networks and suggested that in information handling, as in communications and transportation, there is a tendancy toward "natural monopolies." That is, it is more economical to connect independent systems than to incur the expense of building separate but duplicative networks.

> Today we can see the independent, private automated information systems being interconnected to form larger growing systems . . . . Today we are already building the bits and pieces of separate automated information systems in both the private and government sectors that so closely follow the pattern to the present integrated communications structure that a de facto version of the system you are now pondering [the national data center] is already into the construction phase. It is in many ways more dangerous than the single data bank now being considered.[3]

Baran's warning, more than a decade ago, is even more relevant today. As described in this volume and in its final report to the President and the Congress, the Privacy Protection Study Commission found a number of examples in which separate data bases have been automated, for clearly benign and beneficial purposes, and then at some later date consolidated or integrated—increasingly, but not necessarily, through the direct electrical interconnection of their respective computer systems. There is no doubt, in other words, that concern about the protection of personal privacy is improperly focused if its exclusive preoccupation is with the development of physically centralized information systems.

In its 1966 hearings, the Subcommittee on the Invasion of Privacy was exercising a legislative oversight function. Similar efforts have continued in both the House and the Senate throughout the intervening decade. As a society, however, we are still far from knowing how to assess and deal with the potential societal implications of new information-processing technologies.

Two principal questions that need to be addressed are:

(1) What should "trigger" the policy process so that policy makers can avoid being in the proverbial position of attempting to lock the barn door after the horse is gone; and
(2) What evaluation criteria should be applied in order to make meaningful determinations, not only with respect to a particular innovation as it is proposed, but also with respect to the subsequent evolution of such an innovation?

While these questions have general applicability to issues involving new

[2]Statement of Paul Baran, reprinted in *The Computer and Invasion of Privacy*, Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives (U.S. Government Printing Office, Washington, D.C.), July 26, 27, and 28, 1966, p. 120.

[3]*Ibid.*, p. 122.

technology, the following discussion focuses exclusively on privacy-related matters.

Trigger Mechanisms and Threshold Conditions

In the simplest case, the oversight process can either be reactive or anticipatory. That is, it can begin *after* a particular record-keeping system or practice has been implemented, or it can begin *before* implementation. One common approach which combines both possibilities is oversight that occurs after a system or practice is proposed but before it is implemented. This was the case with the National Data Center proposal, and it is the model inherent in the Privacy Act's new system reporting requirement.[4] In all of these cases, however, there must be some mechanism for getting the attention of those charged with the oversight function.

In government, the two simplest "attention getters" are political ramifications and cost. Political ramifications, however, do not themselves constitute a reliable trigger mechanism, because they depend on a proposal having enough visibility to generate an overt political response, and potential problems seldom have that type of visibility. As the energy crisis debate illustrates, moreover, even high visibility does not guarantee a convergence of opinion as to whether a problem exists, and whether it demands a public-policy response of a particular type.

Where record-keeping practices or systems are concerned, the budget-making mechanism has traditionally been one reliable means of triggering oversight, particularly when large telecommunications systems have been involved. Yet, cost *per se* is increasingly becoming an ineffective trigger. The cost of information technology, in relation to what can be done with the acquired processing, communications, and storage capabilities, is dropping dramatically. The systems that caused concern five to ten years ago are no longer costly enough to make them stand out in a budget request. Indeed, all but a few very large systems now go unnoticed—or, at least, unscrutinized—on budgetary grounds, and this is even more true of improvements of capabilities already in place. The incremental costs of merging existing systems, increasing access to personal information, transmitting data to other agencies, and so forth, can be so small as to escape scrutiny completely.

Interestingly, the Privacy Act takes an innovative and important, if not totally successful, step toward creating a new triggering mechanism. Section 3(o) of the Act requires that:

> each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the

[4] 5 U.S.C. 552a(o).

preservation of the constitutional principles of federalism and separation of powers. *[5 U.S.C. 552a(o)]*

In this way, the burden is on the agency desiring to install a new system, or to modify an existing system, to bring the matter to the attention of the overseers—in this case, the Congress and the Office of Management and Budget (OMB). In order to make this self-triggering process work, however, it is necessary for agencies to have criteria for deciding when they must provide new system reports. Obviously, every small change to an existing system should not have to be reported.

OMB has established the following threshold conditions:

(a) A Report on New Systems must be submitted when:

(1) *A new system of personal records subject to the Privacy Act is proposed.* A new system of records subject to the new system reporting requirement is one for which no public notice consistent with the provisions of subsection (e)(4) is currently published in the *Federal Register.*

If a public notice for any specific system of records is withdrawn, suspended, cancelled, or terminated and subsequently reinstated, the subject system of records shall be considered a new system and subject to the new system reporting requirement at such time that it is reinstated.

(2) *A change to a system of personal records subject to the Privacy Act is proposed.* A new system report is required for any change to an existing system which meets any of the following criteria.

(a) *Increase or change the number or types of individuals on whom records are maintained.* Changes involving the number (rather than the types) of individuals about whom records are kept need only be reported when that change significantly alters the character and purpose of the system of records, e.g., normal increases in historical files or other increases in the number of records in a file which can be attributed to normal growth patterns need not be reported. A change resulting from a change in the scope of the population covered; e.g., a system which only covered a portion of the work force is expanded to cover all, is required to be reported.

(b) *Expand the type or categories of information maintained.* For example, if an employee payroll file is expanded to include data on education and training, this would be considered an expansion of the "type or categories of information" maintained, and would have to be reported.

(c) *Alter the manner in which the records are organized*

or the manner in which the records are indexed or retrieved so as to change the nature or scope of those records. For example, the combining of two or more existing systems or splitting an existing system into two or more different systems such as might occur in a centralization or decentralization of organizational responsibilities would require a report.

(d) *Alter the purposes for which the information is used.* For example, a proposal that files currently used as historical military service records are to be used for making determinations on eligibility for disability benefits would require a report. A proposal to establish or change the "routine uses" of the system will not require the submission of a Report on New Systems if such use is compatible with the purposes for which the system is maintained; i.e., does not, in effect, create a new purpose. Any new or changed "routine use" would, however, be subject to the requirements to give 30 days prior notice of such change in the *Federal Register (5 U.S.C. 552a(e)(11)).*

(e) *Change the equipment configuration (i.e., hardware and/or software) on which the system is operated so as to create the potential for either greater or easier access.* For example, the addition of a telecommunications capability which could increase the risk of unauthorized access would require a report. *[40 F.R. 45877 (October 3, 1975)]*

The questions yet to be answered center around whether these are adequate threshold conditions (e.g., do they allow some important systems and practices to escape scrutiny?), as well as whether the agencies are applying them effectively.

As one illustration, consider the impact on personal-data record-keeping systems and practices of the recent reorganization of the Department of Health, Education, and Welfare (DHEW). The DHEW reorganization, announced on March 8, 1977, provided for the administration of all DHEW cash-assistance programs to be transferred to the Social Security Administration (SSA), including administration of the controversial Parent Locator Service (PLS), which theretofore had been the responsibility of another DHEW component, the Social and Rehabilitation Service (SRS).

While SRS ran the Parent Locator Service there was extensive debate over whether SSA should provide the PLS with information on the whereabouts of absent parents. SSA argued that its records were never intended to be used for that purpose and should not be. Although the matter was finally resolved in favor of SRS, the Congress having passed a statute in effect compelling SSA to open its files to the Locator Service, it should be noted that the issue was in fact debated at the highest levels of the

Department. Today, however, the situation is, organizationally at least, quite different.

What SSA once contended was an "external" disclosure of questionable legality under existing statutes and regulations, is today an "internal" use potentially subject to markedly different considerations. On one hand, SSA now has much greater control than before over any information it allows the Parent Locator Service to use, but, on the other hand, it also has much broader responsibilities. It can no longer concern itself exclusively with the administration of the Old-Age, Survivors, and Disability Income (OASDI), Supplemental Security Income (SSI), and Medicare programs, including the confidentiality of information pertaining to program participants, but must also be concerned for the effective administration of the Aid to Families with Dependent Children (AFDC) and Child Support Enforcement programs. This can put SSA in a difficult situation whenever new proposed uses of its various record systems create conflicts between its desire to fulfill its administrative responsibilities and its desire to remain faithful to the confidentiality expectations and confidentiality pledges previously made to program participants. Moreover, unless some oversight mechanism is able to function effectively at the departmental level, there may be little protection against the initiation of undesirable internal uses other than the integrity and good faith of SSA management.

In summary, the administrative consolidation of programs can have the potential effect of changing the manner in which decisions affecting the disclosure of information are reviewed within a department or its component agencies. Hence, in considering reorganization proposals and plans, the interest in administrative efficiency must be balanced against the privacy interests and expectations of the individuals whose records are being moved under another roof, and some way must be found to assure that those respective interests are properly identified and weighed.

Evaluation Criteria

Once a record-keeping system or practice has been brought to the attention of the bodies with oversight authority, there must be criteria for evaluating it. The threshold conditions implicitly contain some evaluation criteria, since they define when evaluation should occur. However, effective evaluation of a proposed new or altered record-keeping system, raises public-policy issues in its own right, a point that can be well illustrated by an example from the Privacy Act experience.

OMB has directed that the content of the Privacy Act new system report be as follows:

> b. *Content of the Report.* The agency report on proposed new systems, or proposal to modify existing systems shall consist of a brief narrative description, supporting documentation and an update of the inventory of Federal personal data system as outlined below:
>
> (1) Narrative Statement—A brief statement, normally not to exceed four pages in length, which:

- Describes the purposes of the system of records.
- Identifies the authority under which the system of records is to be maintained.
- Provides the agency's evaluation of "the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals and its effect on the preservation on the constitutional principle of federalism and separation of power," and
- Provides a brief description of steps taken by the agency to minimize the risk of unauthorized access to the system of records including a discussion of higher or lower risk alternatives which were considered for meeting the requirements of the system. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established shall be available on request.
- The narrative statement should make reference, as appropriate, to information in the supporting documentation rather than restate such information.
- Where changes to computer installations, communications networks, or any other general changes in information collection, handling, storage or dissemination are made which affect multiple systems of records; a single consolidated new system report may be submitted. In such cases, the narrative statement should address the overall privacy implications of the proposed change, identify all systems of records affected by the change and briefly describe any unique impacts on any specific system of records. Supporting documentation, as defined in the subsequent paragraphs, shall be provided for each system of records.

(2) Supporting Documentation—The following shall be appended to all new system reports:

(a) An advance copy of the new or revised system notice (consistent with the provisions of 5 U.S.C. 552a(e)(4)) which the agency proposes to publish for the new or altered system(s). For proposed alterations of existing systems the documentation should be provided in the same form as the agency proposes to publish the public notice of such changes. If the agency proposes to publish changes in the form of a revision to the public notice, a

copy of the proposed notices of revision should be provided. If the agency plans to supersede the entire existing notice, changes from the currently published notice shall be highlighted by underlining all new or revised portions.

(b) An advance copy of any new rules or changes to published rules (consistent with the provisions of 5 U.S.C. 552a(e)(11)(f)) which the agency proposes to isse for the new or altered system. If no change to existing rules are required for the proposed new or altered system, the report shall so state. Proposed changes to existing rules shall be provided in a manner similar to that described for the system notices.

(c) An advance copy of any proposed rules setting forth the reasons why the system is to be exempted from any specific provision (consistent with the provisions of 5 U.S.C. 552a (j) or (k)) if the agency head plans to invoke any exemptions for the new or altered systems. *[40 F.R. 45877-8 (October 3, 1975)]*

Obviously, the criteria upon which to base an evaluation will not come directly from the report itself, except perhaps in a most superficial way. Faced with this problem, the Executive and Legislative oversight bodies must necessarily develop their own evaluation criteria. In the case of the Tax Administration System (TAS) proposed by the IRS, the Congress formally sought the assistance of the Office of Technology Assessment (OTA) in doing so.

The TAS proposal would establish a computer system that would make Federal income tax returns of the past three to five years immediately available within each of the 10 IRS regions via on-line computer terminals in IRS offices. Currently, only about 10 percent of the 132 million tax returns submitted to the IRS are immediately available using the present IRS computer systems. The remainder are held on magnetic tape and can be obtained only after a wait of several days.[5] OTA's response to this proposal, after over half a year of study, was to indicate that it was unable to answer all of the questions it believed needed to be answered, and to recommend that hearings be conducted before the Subcommittee on Oversight of the House Ways and Means Committee "in order to acquire the background information needed for defining issues."[6]

The observation to be made here does not concern the particular system or OTA's particular response, but rather what the entire episode reflects about the government's ability to assess and evaluate the impact of a

[5]Witt, Evans, "Lack of Privacy Feared with IRS Computer Plan," *The Washington Post,* March 4, 1977, p. D11.

[6]Office of Technology Assessment, *Investigation of a Request to Assess the IRS Tax Administration System,* February 1977, p. 12.

major automated information system. The TAS proposal received a disproportionate amount of attention when one considers that it is only one of many proposals for new or materially revised information systems sent to the Congress. There were over 100 new system proposals in the first year of the Privacy Act's operation. Obviously, the others received less congressional scrutiny, and the more common occurrence of changes to an existing system which are not of sufficient magnitude to constitute "new systems" under the Privacy Act received no scrutiny at all.

As the OTA report observes both explicitly and implicitly, extensive knowledge, often of a highly technical nature, is needed to perform an effective assessment and evaluation of the impact of a proposed information system. Knowledge of the law, knowledge of computer and telecommunications technology, and knowledge of the particular agency and program functions are needed. Rarely does such knowledge exist in one place, especially when one considers all of the possible programs involved. As far as the Congress is concerned, moreover, the committees most concerned with privacy matters in the Federal government (i.e., the Senate Committees on Governmental Affairs and the Judiciary and the House Committees on Government Operations and the Judiciary) often do not have the necessary jurisdiction to do detailed program evaluation; and conversely, the committees concerned with programs are generally not concerned with reviewing privacy implications in depth.

The Role of the Individual

No discussion of oversight would be complete without a consideration of the role of the individual in the process, and the Privacy Act is again a good example, for it is typical of most so-called fair information practice legislation, State as well as Federal. The Privacy Act gives the individual a set of rights, the exercise of which is intended to serve as a check on governmental record-keeping activities. The assumption is that the individual's exercise of his rights will create incentives for the agencies to comply vigorously with the requirements levied on them by the Act, the effect being an overall upgrading of the information management policies and practices of the Federal government. Yet, as the Commission's assessment of the Privacy Act[7] clearly shows, these assumptions are subject to some powerful constraints.

First, many of the record-keeping activities within the Executive branch are mandated by the Legislature or the result of Judicial interpretations. In such instances, the Executive agencies often have limited, if any, discretion over the amount of information to be collected or the manner of its use. And even when the Executive agency does have discretion, there is still no mechanism for determining whether a particular record-keeping practice or system should exist at all. In these cases, the value of the rights granted by the Privacy Act is diluted. Second, taxpayer demands for better services, more efficient operations, and stricter accountability for public

[7]See Chapter 13 of *Personal Privacy in an Information Society* and Appendix Volume 4, *The Privacy Act of 1974: An Assessment.*

expenditures often supersede concerns about privacy in public-policy decisions. Third, the adoption of new record-keeping practices has created the capability to make much more exhaustive use of existing information. The full extent of developments in this area is not completely understood, even by its more advanced practitioners, but it is becoming increasingly difficult to state definitively the manner in which information collected today can, or will, be used in the future.

Unintended Effects

A final, but unavoidable, observation to be made about oversight is that public-policy responses to technological developments can have their own unintended, and equally undesirable, effects. While the debate about centralized record systems has been extensive—and, in some cases, improperly focused—emerging privacy protection requirements, like the Privacy Act, may actually encourage centralization.

Consider, for example, a problem currently faced by the Department of the Interior. Each of the 300 national parks maintains its own system of records. When an individual asks the Park Service for access to his record(s), the Service asks him to recall which parks he has visited. Then, of those parks, the Service asks him to try to recall the ones in which he might have had an encounter which would have generated an individually identifiable record. Finally, the Service suggests that he write those particular parks directly. For the time being, this arrangement seems adequate. If the number of requests increases, however, or if future litigation results in the requirement that the Park Service itself contact each field location instead of placing the burden on the individual, the Service might well be inclined to centralize its records.

Nor is access to records the only feature of the Privacy Act that could tend to promote further centralization. In a centralized system, there is less need to propagate corrections, particularly if there are no derivative files; and there is centralized control and protection. Furthermore, the notice requirements of the Privacy Act have shed light on similar systems in the same agency, and there are signs that this too may foster a trend toward the sharing, and ultimate integration, of systems among components of the same agency. The issue here, of course, is not whether such centralization is good or bad, but rather that it is probably not what the drafters of the Privacy Act had in mind.

Who and What is Covered?

A particularly perplexing problem which strikes at the basis of policy formulation is the one of deciding who and what is to be covered by the policy. While intuitively this may seem quite simple, poorly drawn definitional boundaries can render obsolete or circumventable the policy aspects of any law. Even well drafted definitions—or well established "boundary conditions," as a computer scientist would say—can be

susceptible to circumvention by unforeseen developments in, or applications of, technology.

The most well known example of this problem in the information policy area centers around the Privacy Act's "record" and "system of records" definitions. The Privacy Act applies to a "record" that is "retrieved" from a "system of records" by the name of an individual "or by some identifying number, symbol, or other identifying particular" assigned to him. Indeed, where the Act fails to meet its objectives, the failure can often be traced in part to the record and system-of-records definitions.

As defined in subsection 3(a)(4) of the Privacy Act, the term "record" means:

> . . . any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. *[5 U.S.C. 552a(a)(4)]*

It seems clear that this definition includes every record that *contains* any kind of information associated with an individual. Subsection 3(a)(5), however, defines a "systems of records" as:

> . . . a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. *[5 U.S.C. 552a(a)(5)]*

Thus, unless an agency, in fact, retrieves recorded information by reference to a "name . . . identifying symbol, or other identifying particular . . .," the system in which the information is maintained is not covered by the Act.

Whereas the record definition refers to information about an individual which *contains* his name or identifier, the system-of-records definition refers to information about an individual that is *retrieved* by name, identifier, or identifying particular. The crucial difference between the two definitions is obvious, and the effect has been to exclude from the Act's requirements many records about individuals that are not accessed by name, identifier, or assigned particular.

The congressional intent behind it is, however, quite justified. Some limit needed to be placed on the range of the search that an agency would be obligated to conduct in response to a request for access to a record. The problem, of course, is that any well defined sorting procedure can rearrange information so that it is or is not retrieved by individual identifier, depending upon the agency's preference.[8]

The significant flaw in the system-of-records definition is that it

[8]Two examples will illustrate the extremes of agency implementation of the Privacy Act's "system of records" provision. A small component of one agency rearranged its personnel records by Civil Service grade, instead of individual identifier, in order to avoid the Act's requirements. The Department of the Navy, on the other hand, elected to bring a file of

springs from a manual rather than a computer-based model of information processing. In a manual record-keeping system, records are apt to be stored and retrieved by reference to a unique identifier. This, however, is not necessary in a modern computer-based system that permits *attribute searches* (e.g., "list all blonde, female Executive Directors of Federal Commissions"). An attribute search, in contrast to the conventional "name search," or "index search," starts with a collection of data about many individuals and seeks to identify those particular individuals in the system who meet the prescribed conditions or who have the prescribed attributes or combination of attributes. For example, officials of the Veterans Administration (VA) testified in the Commission's hearings on medical records that the VA has produced lists of names for another agency by using psychiatric diagnosis, age, and several other personal attributes as the search keys,[9] and this type of search capability is possible in most modern data-base management systems.

The system-of-records definition also creates legitimate uncertainty as to which records are or should be subject to the Act. For example, questions have been raised about the status of the State Department's cable system, which Federal agencies use to transmit information overseas. Because this computerized communications system has retrieval algorithms that make it possible to retrieve information in the cables on the basis of personal identifiers, the State Department might be considered to maintain an extensive system of records derived from other agencies' cable traffic. So far, however, there has been no clear determination as to whether the cable system should be considered a State Department system of records or simply a facility for communicating information in records maintained by the user agencies.

A growing number of computer systems today are also capable of retrieving information by a "textual search" process. The search program is keyed to "hit" on certain arrangements of characters or items of data as it scans material that has previously been collected and stored into the system as raw text, such as reports, letters, or memoranda. It would appear, however, that such a system would not be subject to the Privacy Act because, by the Act's operating definitions, it does not constitute a system of records. The fact is, though, that retrieval of individually identifiable information by scanning (or searching) large volumes of computer records is not only possible but an ever-increasing agency practice. The Federal Trade Commission, for example, is transcribing all written material in its litigation files for computer retrieval, thereby making it possible to search for all occurrences of a particular name, or any other character pattern for that matter.

The Privacy Protection Study Commission's suggested revisions to the

interview records under the Act even though they were filed (and hence retrieved) by the date of the interview.

[9]Testimony of the U.S. Veterans Administration, *Medical Records*, Hearings before the Privacy Protection Study Commission, July 21, 1976, pp. 444, 445.

Privacy Act may be considered instructive, for they embody a new approach that balances technical considerations with other interests.[10] The definition of the term "record" is expanded to include attributes and other personal characteristics assigned to an individual, and a new term, "accessible record," is defined to delineate those individually identifiable records that ought to be available to an individual in response to an access request. Accessible records would include those which, while not retrieved by an individual identifier, could be retrieved by an agency without unreasonably burdening it, either through its regular retrieval procedures or because the subject is able to help the agency find the record. If an individual knew he was mentioned in a particular record, for example, he would be entitled to access to it whether or not agency practice is to access the record by reference to him. Finally, the Act's term "system of records" is abandoned in favor of a new term, "system," which is defined as a collection (or grouping) of records which is systematically filed or stored according to some established retrieval scheme or indexing structure (this would include a textual search) and and which is in practice referenced by such retrieval scheme or indexing structure. The effect, then, is to preserve the philosophy of the current system-of-records definition, although the new term "system" is only used in the suggested revision of the Act to delineate the entities for which an annual notice must be published in the *Federal Register*.

The Commission drafted an illustrative revision of the Privacy Act in order to show how its suggestions for revision of the law might appear as legislative requirements.[11] The terms "record," "accessible record," and "system" are defined in subsections (a)(3), (a)(6), and (a)(7) as follows:

> (3) the term "record" means any item, collection, or grouping of information about an individual including, but not limited to:
>
> (A) normal directory information, such as the individual's name, address, telephone number, business address, or similar information,
>
> (B) other numbers, symbols, fingerprints, voiceprints, photographs, or identifying particulars assigned to, or associated with, the individual,
>
> (C) information relating to the individual's background, education, finances, health, criminal history, or employment history, or
>
> (D) any other attributes, affiliations, or characteristics associated with, or assigned to, the individual;
>
> (6) the term "accessible record" means an individually identifiable record, except a research and statistical record, which is:
>
> (A) systematically filed, stored, or otherwise maintained according to some established retrieval scheme or indexing structure and which is, in practice, accessed by use of, or reference to, such retrieval scheme or indexing structure for the principal purpose of retrieving the

[10]See Chapter 4 of Appendix Volume 4, *The Privacy Act of 1974: An Assessment*.

[11]See Appendix B of Appendix Volume 4, *The Privacy Act of 1974: An Assessment*.

record, or any portion thereof, on the basis of the identity of, or so as to identify, an individual, or

(B) otherwise readily accessible because:

(i) the agency is able to access the record without an unreasonable expenditure of time, money, effort, or other resources, or

(ii) the individual to whom the record pertains is able to provide sufficiently specific locating information so as to render the record accessible by the agency without an unreasonable expenditure of time, money, effort, or other resources;

(7) the term "system," or the term "subsystem," means any collection or grouping of individually identifiable records which is systematically filed, stored, or otherwise maintained according to some established retrieval scheme or indexing structure and which is, in practice, accessed by use of, or reference to, such retrieval scheme or indexing structure for the principal purpose of retrieving the record, or any portion thereof, on the basis of the identity of, or so as to identify, an individual or individuals;

The significant point to be made here is that a "reasonable burden" test in subsection (a)(6)(B) is substituted for the current law's fixed test of "is retrieved by." This avoids the problems with the current law without substituting the more undesirable alternative of a "retrievable" test, which would cover all theoretically retrievable information. While the difficulties inherent in trying to comply with such a provision will be discussed below, it is important to note that the Commission found no other acceptable alternative, and concluded that the Act should have a flexible, as opposed to a fixed, test for what is covered.

This flexible coverage approach appears increasingly more appropriate as one examines the difficulties of drawing definitional lines in area so diverse and undergoing such rapid change. While this places an increased burden of judgment on those who must comply with the law, as well as on the courts that must ultimately interpret it, in the long run the policy objectives of the Privacy Act will be better achieved.

Establishing Acceptable Levels of Performance

Once legislative policy is established, there is another important problem that must be addressed, either directly or indirectly. Legislation is inherently a broad statement of social or public policy goals. Generally, a statute sets forth the policy objectives to be achieved, but the details of how to achieve them are left for others to work out. In the Federal government, the agencies exercise their rule-making authority using the processes called for in the Administrative Procedures Act *[5 U.S.C. 551 et seq.]* to develop and describe the details and implementation alternatives which are allowed. These define what is frequently called an "acceptable level of performance" with respect to the given policy objectives in a law. Thus, compliance with

the law entails meeting the criteria for an acceptable level of performance set forth in the agency rules and regulations.

There are cases in which the Congress itself has specified acceptable levels of performance (the emissions standards in the Clean Air Act are one example), but this rarely occurs in legislating information policy. Indeed, in its suggested revisions of the Privacy Act of 1974, the Commission specifically chose to allow Federal agencies even broader latitude and flexibility than they now have in implementing the law's policy objectives. While the Commission took steps to clarify the interpretational variances in the Privacy Act, it did not believe that it should narrow, and in fact thought it should somewhat expand, the implementation alternatives available.

In many instances, the difficulty with the Privacy Act does not appear to arise from the flexibility of implementation it allows, but rather from the fact that some agencies have taken advantage of that flexibility to contravene its spirit. Yet, making the law less flexible is not a desirable solution. Implementation costs would rise dramatically, and new developments in information technology could invite uncontrollable circumvention of rigidities in the statute. The Commission's approach represents an attempt to allow for changing information technology and diversity of agency information needs and uses, as well as to foster the constructive creativity that can arise in the absence of overly restrictive requirements.

Setting forth broad public-policy objectives while allowing for various implementation alternatives and strategies does, however, create a need for reasonably definitive guidance to operating personnel on what constitutes acceptable levels of performance in certain areas. Today, operating personnel who must implement the policy objectives embodied in a fair information practice statute frequently have little or no guidance on how to proceed. This is particularly true in the case of automated information systems, because technologists are necessarily trained to work with and from detailed specifications arising from precise statements of the task to be performed and well-defined steps leading to its attainment or solution. To tell a technologist that he should implement "reasonable" safeguards does little to guide him in determining what an acceptable level of performance will be for that particular requirement.

This is not to say, however, that "reasonableness" standards are not workable, but rather to observe that a "reasonableness" standard is a test for use in establishing noncompliance with a particular requirement. Over and over again, at both the State and Federal level, the Commission staff encountered agency operating personnel who had numerous questions regarding the specifics of an acceptable level of performance for a particular statute. How specific should system notices be? What particular methods of storage and retrieval were acceptable for maintaining an accounting of disclosures? What particular security techniques and features would be considered "adequate"? And so on. While in the case of the Privacy Act some guidance has been forthcoming, it has largely been concerned with manual procedures and requirements of the law. The problem yet to be addressed in any broad and effective way, at either the State or the Federal level, is how to translate the broad social goals of privacy and fair

information practice legislation into precise steps which computer scientists and managers of automated systems may follow in order to achieve acceptable levels of performance.

It should be noted that this is a continuing rather than a one-time task. The acceptable performance levels will not only vary depending upon the environment and the particular hardware and software configuration, but it will change as technology changes. Indeed, changing record-keeping environments and changing technology are the strongest rebuttal to the critics of privacy/fair information practice legislation who maintain that Congress should be more precise and more specific in the legislative drafting process. While it is fair to say that the Congress should be attentive to the specifics of information technology to the extent that it strives to draft statutes which will not be quickly rendered obsolete by technical developments, it would, nonetheless, be a poor legislative strategy to embody in a law any precise specifications of information technology for the simple reason that these would be potentially inappropriate in many current environments and, most certainly, in future environments.

In the short run, there will probably have to be different standards and criteria for new systems, as compared to old ones, since there are enormous investments in existing automated record systems that do not necessarily lend themselves to even minor modifications without major redesign. One of the ironies of the rapid development of computer technology has been the tendency to utilize the newer and faster equipment and software to operate old systems at a faster speed, without taking advantage of improved capabilities for file organization, data communications, retrieval algorithms, and general design flexibility.

As new systems evolve to perform new applications or to replace older systems, it becomes appropriate to expect much higher standards of performance with respect to the protection of personal privacy. These might include extensive data-base management facilities, protection against unauthorized access, recording of modifications and disclosures, and so on. Given the current difficulties in monitoring compliance in environments utilizing highly automated record-keeping systems, it is also likely that newer designs will begin to incorporate sophisticated procedures for automated compliance monitoring.

Chapter 5

Technical Implications of Privacy

As the trend toward automation of record-keeping functions and practices increased in the past two decades, it naturally became increasingly clear that the privacy protection implications of technological developments had to be considered. What has yet to emerge clearly, however, is the other side of the problem: namely, the impact on information system design and development of trends in the formulation of privacy protection requirements. This chapter will discuss the general technical implications of emerging privacy protection requirements and proposals, including some of the those made in the Commission's own final report. While the chapter is mainly directed at information system designers, developers, managers, and users, the principal points should be clear to a broader readership.

The Security Implications of Privacy

The phrase "technical implications of privacy" has been overworked in the computer community, in large measure because the notions of "privacy" and "security" are often used interchangeably—and wrongly so—by many computer professionals. The perception that privacy and security can be equated, however, emerges naturally from from the logical historical development of information management policy and practice as seen by the technologist, and to appreciate some of the subtleties of the security implications of privacy protection it is important to understand that historical perspective.

By the middle 1960's, computer scientists were increasingly aware that the use of computer systems could have undesirable consequences or unpredicted, or even unpredictable, results. While the problems relating to personal information were generally in the "erroneous bill" and "computer error" category, and not perceived as privacy protection problems, there was an increasing realization that a serious problem existed in the potential misuse of the computer systems which were a part of our national defense posture.

The Defense Science Board Task Force on Computer Security was established in 1967 as one of the first formal efforts to study the security problem. The DSB Task Force, and other efforts like it that followed, had a simple goal: the deterrence, prevention, and detection of a covert attempt to misuse a computer system by a technologically sophisticated penetrator. It was assumed, in other words, that the "penetrator"—as the perpetrator of

the misuse came to be called—was as technically sophisticated as the computer scientists studying the problem and that he had access to the (publicly available) documentation of the particular system in question.

This portion of the computer security field is obviously important, and continues to flourish. Moreover, it has resulted in a better understanding of how to build reliable computer systems in general, for the easiest method of penetrating a computer system is to exploit a flaw, inconsistency, or incompleteness in the system's design. It developed, however, that the early assumptions of the computer security field were too narrow to encompass all of the potential problems surrounding the use of computer systems. In particular, the initial view that safeguards to protect the security and integrity of national defense information would also be appropriate for personal information neglected to consider other, more probable, threats to personal privacy.

By the early 1970's, it had become clear that technically unsophisticated, and even well intentioned, users of a computer system could be the source of problems. First, stories began to emerge of clerks, managers, accountants, tellers, and the like, misusing, for their own personal gain, the computer systems to which they had access. In this case, the threat came from the technically unsophisticated, but dishonest, user; such an individual usually had some form of authorized access to the system, which he then abused to his advantage. This has become known as the area of "computer abuse."

Second, and perhaps more important from a societal point of view, it became increasingly clear by the 1970's that even honest people, doing their jobs with the best of intentions, could use computer systems in such a way as to affect other people adversely. In the simplest case, people make errors and omissions (while, contrary to popular belief, computer systems do not). Errors and omissions in system design or development, in data collection, entry, or reporting, or in data correction or updating can cause people financial loss, employment dislocations or difficulties, embarrassment or stigmatization, or simply inconvenience. In the more complex case of the problem, the use of a particular system may have unintended effects; it may have an impact on people, institutions, or society in ways that were not foreseen. While in some cases these could be called omissions during the system design phase, it is probably fairer to say that the practitioners are still learning which questions to ask in this regard.

With this perspective in mind, it is now easier to discuss the security implications of privacy protection, and a natural illustration to use is the Privacy Act of 1974. Section 3(e)(10) of the Act, usually called the *safeguarding provision*, requires an agency to:

> establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment,

> inconvenience or unfairness to any individual on whom information is maintained.[1]

As reported in Chapter 13 of the Commission's final report, as well as in the separately published Appendix 4 assessing agency experience under the Act,[2] the Federal agency response to the safeguarding provision has ranged from no response at all to what may only be termed "technological overkill." To the extent that a pattern emerged in conversations with agency personnel, however, two distinct dimensions of agency behavior were apparent: (1) technically trained agency personnel tended to be more concerned with protecting against threats by the more technologically sophisticated penetrators; and, (2) while there was some tendency at all levels to protect against abuse by dishonest employees, or mistakes by honest ones, there was a general presumption by management and technical personnel that "our people are all right." This pattern was found repeatedly and also appears to be consistent with prevailing views in the private sector.

The tendency of technically trained personnel to focus on the highly technical threats to computer systems is consistent with their background and with the development of the computer security field. Indeed, most of the literature still concentrates on that aspect of the problem. Furthermore, the natural tendency to have confidence in one's colleagues or employees mitigates against efforts that start from the presumption that they too are threats against which protection is required.

The framers of the Privacy Act specifically intended that the safeguarding provision not be directed towards the highly technical and exotic forms of attack against a computer system.[3] Instead, the legislators allowed "for a certain amount of 'risk management' whereby administrators would weigh the importance and likelihood of threats against the availability of security measures and the considerations of cost."[4] In other words, the probability of a mishap or abuse occurring, as well as its impact, should weigh heavily in the agencies' actions. Indeed, the Senate Committee report on the Privacy Act states that

> the Committee . . . intend[ed] that the term "appropriate safeguards" should incorporate a standard of reasonableness and "refer to those safeguards which represent current state-of-the-art procedures at any given time, despite any weaknesses that may exist in the technology at that time."[5]

Furthermore, the safeguarding provision plays another, even more important, role that has virtually been ignored by technologists. Simply

---

[1] 5 U.S.C. 552a(e)(10).

[2] Report of the Privacy Protection Study Commission, Appendix Volume 4, *The Privacy Act of 1974: An Assessment.*

[3] For a further discussion of this topic, see: Bushkin, Arthur A. and Schaen, Samuel I., *The Privacy Act of 1974: A Reference Manual for Compliance* (System Development Corporation, May 3, 1976) pp. 111-117.

[4] Report of the Senate Committee on Government Operations to Accompany S. 3418 (Senate Report No. 93-1183), September 26, 1974, p. 55.

[5] *Ibid.*, p. 54.

stated, one need only consider how the Privacy Act would be differently implemented if there were no safeguarding provision. Because the safeguarding provision does not impose any specific record-keeping practices on an agency, no specific record-keeping requirements would be dropped from the Act. Agencies would still be limited in the disclosures that they could make of personal information,[6] and they would still be required to maintain accurate, timely, relevant, and complete data.[7] Indeed, all of the Act's other requirements would still apply. However, without the safeguarding provision, which establishes a level of acceptable performance regarding the maintenance of records that an agency must reach in order to avoid potential liability, the separate "cause of action"[8] in the Act for an agency's failure to adequately protect data in its possession would be vitiated. Thus, the impact of the safeguarding provision is primarily in the legal domain; its only "record-keeping" requirement being the implicit one that an agency must assure that its practices meet the performance level specified in the safeguarding provision.

The Commission's approach to the safeguarding provision in the Privacy Act illustrates this point. To correct the drafting deficiencies in the current safeguarding provision, as well as to make the obligations it imposes more realistic, the Commission believes that an agency should be required to establish *reasonable* administrative, technical, and physical safeguards to assure the integrity, confidentiality, and security of its individually identifiable records so as to *minimize* the risk of substantial harm, embarrassment, inconvenience, or unfairness to the individual to whom the information pertains. Such a change would be consistent with the Act's legislative history and should protect against the overreaction occasioned in some agencies by the current language of the Act which requires agencies to establish *appropriate* safeguards against *any anticipated threats or hazards.*

In the case of the private sector, on the other hand, the Commission has not recommended application of the safeguarding provision, or any analogue for it, even when it has recommended legislation relating to the collection, maintenance, use, and dissemination of private-sector records. This does not mean that no safeguards or security measures would be required of private-sector organizations, but rather that the Commission expects private-sector organizations subject to statutes and regulations emanating from its recommendations to behave as though a safeguarding provision similar to the one recommended for the Privacy Act also applied to them. Unlike government agencies, organizations in the private sector have a strong incentive to develop performance standards of the sort called for in the safeguarding provision by virtue of the fact that they are ordinarily liable to an individual for any injury to him resulting from their failure to

[6]In the Privacy Act, sections 3(b)(1)-3(b)(11) would still apply. In particular, section 3(b)(1) would still limit disclosures to only those agency personnel with a need to know the data.

[7]5 U.S.C. 552a(e)(5).

[8]A "cause of action" is the legal term for the basis upon which a suit is brought. In the case of laws applying to the government (e.g., the Privacy Act), the government must also waive "sovereign immunity" by giving an individual standing to sue the government.

comply with the kinds of requirements the Commission's private-sector recommendations would impose.

In summary, the technical community has traditionally viewed the misuse of computers as a technical computer security problem—and, indeed, this view is not so much wrong as narrow. If one takes the larger view that security is the condition in which "right things occur and wrong things do not occur," then the totality of a piece of privacy protection legislation must be viewed as defining what the "right things" are. An explicit safeguarding provision in the law recognizes the impossibility of achieving perfect implementation of the rest of the law, and therefore establishes an acceptable level of performance which can serve as the basis for a separate cause of action for alleged failures to achieve that level of performance or compliance.

"Finer Granularity" of System Functions

Fundamental to the security of a computer system is the ability to control access to the data in the system. Authorized users of a computer system—particularly the large on-line systems with directly accessible secondary storage—are generally assigned special identifiers, passwords, account numbers, and the like. Presentation of these "keys" to the system is necessary before the user will be permitted to perform his tasks.

Larger systems with large heterogeneous user communities not only discriminate between the data different users may see, but they also can discriminate between the uses that different users may make of the same data. The simplest breakdown is that some users (e.g., clerks) may only be authorized to access (i.e., read) particular data, whereas other users (e.g., administrators) may be authorized to change or modify those data as well; and the computer system will enforce this discrimination.

What most computer systems do not generally do, however, is enforce such discrimination at the data item level. Access to data, update of data, transfers or disclosures of data, generation of audit trails or accounting logs, access to those audit trails or accounting logs, all usually occur at the "record" or the "file" level.[9] Yet, *a major technical implication of privacy protection is the requirement to restrict system functions*[10] *so that they operate either on subsets of a file—that is, particular records or records with particular characteristics or attributes—or on subsets of a record—that is, particular data items or data items with particular characteristics or attributes.*

A general theme pervading the Commission's recommendations and most existing privacy protection legislation is that system functions must be performed at a level below the file level, and often below the record level. The latter is particularly true as more and more information is consolidated into a single record. For example, payroll personnel must not be permitted access to an employee's medical data. Likewise, when payroll data are

[9]See Chapter 2, note 4.

[10]As used here, the term "system function" refers to any function of the operating system, of a generalized or a specialized subsystem, or of a particular application program.

transferred to the Internal Revenue Service, only the appropriate payroll data should be disclosed from the larger record.

This finer granularity in system functions is not a particularly new or startling concept. Indeed, the principal reason that most systems do not employ such facilities now is that there has always been a certain cost involved, and the need has not been that great.

Implementing this capability will generally require software modifications, along with appropriate descriptor data items embedded in the data base[11] upon which the software will operate.[12] In some cases, the modifications will be simple; in others, a major rewrite of the relevant software will be required. Certainly, as new systems for handling personal information are designed and developed, they should be planned with this finer granularity of system function in mind.

Descriptor Data

For various system functions to discriminate between different elements of a record, it is necessary for those functions (i.e., the software) to be able to distinguish between the various data items of a record. For example, in a consolidated personnel record containing payroll and medical data, the access control software must be able to distinguish between the payroll data items and those which are medical information. Then, assuming there exists a means for distinguishing between different types of users, the access control software can ensure that only the payroll user has access to the payroll data and the medical user has access to the medical data.

One method of implementing such discrimination would be to rely on implicit information in the record itself. For example, if the software "knew" that the first 10 data items of a record contained directory information (e.g., name, address, identifiers, etc.), the next 13 data items contained payroll information (e.g., salary, number of deductions, hours worked, State tax, etc.), and the last 17 items were medical-record information, then the access control software could be written so as to treat the particular data items according to their relative location in the record. As any programmer knows, however, systems are always subject to change and reliance upon such implicit information is not always the best programming strategy.

More generalized data-base management systems, and even some specialized application programs, usually rely upon directory definitions to identify the particular types of data items, as well as the particular types of records, in a data base. Alternatively, the record itself may be expanded to include additional data that are not a substantive part of the record but rather describe the data items in the record. In the previous example, such descriptor data would indicate that the first 10 items were directory

[11]See Chapter 2, note 5.

[12]Information relating to the points made in this and the next two sections can be found in: Fong, Elizabeth, *A Data Base Management Approach to Privacy Act Compliance*, U.S. Department of Commerce, National Bureau of Standards, Special Publication 500-10, June 1977.

information and the next 13 were payroll and the last 17 were medical. Whether these descriptor data exist explicitly in the record or whether they exist in some data-base directory or dictionary associated with that collection of records, the software must specifically recognize them and then act accordingly.

The concept of "descriptor data"—that is, data describing the structure or attributes of data—is not particularly new and data definition procedures are familiar to most programmers. What does appear new, however, is that the requirement for finer granularity of system functions implied by current and pending privacy protection legislation seems to be mandating a more sophisticated approach to the definition and treatment of descriptor data. The decision as to how much of this functional discrimination can be done in software alone and how much will have to be dependent upon some form of descriptor data imbedded in, or associated with, the data base is generally a function of the particular system and data base at hand. More advanced data-base management systems with sophisticated data definition capabilities may not need extensive additions of descriptor data to the data bases themselves and may be able to satisfy future requirements with only changes to the system's software. More conventional data-base management systems and applications programs, on the other hand, may require additional descriptor data in the data base, as well as some software modifications.

The concept of descriptor data is fairly straightforward when one thinks of it in programming terms as merely the creation of data items to describe other data items. It is more elusive, however, when one examines all of the situations in which the concept of descriptor data is implied by the Commission's recommendations or by emerging trends in privacy protection legislation. For example, the Commission has made a distinction between information relating to an individual's health which is generated by a medical professional or by the individual himself, and information about his health which is generated by anyone else (for example, by a neighbor).[13] Thus, the same information, depending upon its source, would have to be described by two different descriptor data items.

This example illustrates one of the inherent difficulties with descriptor data—difficulties which are both practical and conceptual. The practical difficulties of keeping descriptor data accurate, timely, and complete with respect to the data items being described are well known to any programmer. The conceptual difficulties arise as one considers all of the situations in which it is becoming necessary to distinguish between the different types, functions, or other attributes of the same data being described. The legal situation, for example, may be different in different circumstances. Information about an individual's medical condition that is generated and maintained by a doctor may be subject to different legal requirements than it would be if it were in the possession of an insurance company or an employer. Similar differences arise as one spans the gamut of record keeping, from social service to employment, from credit to criminal justice,

[13]See Chapter 7 of *Personal Privacy in an Information Society*, especially note 7 on p. 278.

from insurance to health, and so on. One finds the same data being used over and over again in different legal environments, and as these data become increasingly concentrated, and as flows between environments become more and more the norm, the ability to discriminate between functions becomes something more than simple access control to keep one class of user from seeing another class of user's data. Individuals may have different correction, amendment, and appeal rights with respect to different kinds of data; record keepers may have different audit, accounting, and updating rights with respect to different data; and political jurisdictions may impose different requirements on the record keeper, such as different reporting requirements.

All of these trends taken together tend to imply an increased reliance on descriptor data to the extent that software systems will have to have a greater "knowledge" about the types of data items upon which they are operating. Once again, the actual decision whether to imbed this knowledge in the software itself, in a data-base dictionary or definition module, or as explicit descriptor data items in the record itself will be a function of the particular system in question. What seems clear is that the emerging trend will require a heightened "awareness" on the part of the system regarding the types of information being processed.

Uses of descriptor data actually span a broad cross section of programming situations, many of which are already familiar to most programmers. Common examples include the use of "status indicators," or "flags," in records (as opposed to their use in programs). As an example, the Fair Credit Billing Act[14] provides that, when an individual disputes a particular line item on a charge account bill, he should not be charged any interest or carrying charges until the dispute is resolved. Thus, if an individual defers payment on a charge account bill that has one line item under dispute, interest charges may only be computed on the undisputed portion of the bill. This implies that the software that computes the interest charge must not simply compute a percentage (typically 1.5 percent per month) of the total bill but instead must be able to recognize disputed line items. One method of handling this is to associate a code with each line item indicating whether or not it is in dispute. Such codes are another form of descriptor data.

Routing Data

Closely related to descriptor data is another class of "data about data" called "routing data," or sometimes "traffic data." Simply stated, routing data consist of data regarding the recipients of the (substantive) data in a record. Different systems and situations will dictate that varying amounts of routing data be maintained, and that various methods be used. In some cases, routing data will be maintained with their associated record or file; in other cases, they will be maintained separately. In some cases, routing data will be implicit in that no actual data will be maintained (as, for example, in the case in which it is known that a payroll tape is always transferred to the

[14] 15 U.S.C. 1601 *et seq.*

accounting department on Tuesday); and, in some cases, combinations of these will be used.

It is useful to differentiate routing data from descriptor data for a number of reasons. First, the requirements that dictate the maintenance of routing data are usually different. Second, routing data are usually maintained differently—that is, routing data are generally not maintained as an integral part of the substantive data record. Third, the things done with routing data are also usually quite different. And, finally, the routing data are themselves generally larger (i.e., whole fields instead of bits or other codes) and more voluminous—a list of recipients of a record can be longer than the record itself.

The issue of granularity mentioned earlier also affects routing data. In the above example of the transfer of the payroll tape to the accounting department, it is still necessary to determine whether a particular individual was on the payroll that week in order to establish whether his payroll record was on the tape. This is a case in which the (implicit) routing data item (i.e., "transferred to accounting department on Tuesday") refers to a collection or grouping of substantive records. Obviously, knowing which records are in the group so described can itself become a difficult and complex task, and this implies the necessity for "finer granularity" of routing data.[15]

The requirement to maintain routing data generally follows from one of three objectives:

(1) to provide the subject of the record with an accounting of the uses and disclosures of his record;
(2) to facilitate the propagation of corrections of erroneous information to the sources and the prior recipients of the information; or
(3) to facilitate internal monitoring or auditing by the record-keeping organization.

The emphasis of the accounting of disclosures requirement in the Privacy Act,[16] for example, is currently on the first objective. The Commission concluded, however, that the Act was not effectively meeting this objective and, more importantly, that the primary emphasis of the Act's accounting of disclosures requirement should be on its utility in propagating corrections.[17]

The actual wording of any requirement that mandates the maintenance of routing data is very important, since the amount of data required to be maintained could be inordinate. In the case of the Privacy Act, the Commission basically agreed with the prevailing view that this is the statute's single most burdensome provision. The Commission was sensitive to the necessity of establishing "reasonableness" tests for determining the

[15]For a further discussion of this topic, see: Bushkin, Arthur A. and Schaen, Samuel I., *op. cit.*, pp. 92-96.

[16]5 U.S.C. 552a(c).

[17]*Personal Privacy in an Information Society*, p. 525.

period of time for which an accounting must be kept, as well as for the amount of detail about each disclosure that must be kept.[18]

The change of emphasis in the Privacy Act's accounting requirement from providing the individual with information to facilitating the propagation of corrections is a theme that not only is found in the Commission's recommendations but which can probably be expected to become increasingly popular. As more and more records are created and disseminated, record-keeping organizations (both public and private) will increasingly bear the burden of propagating corrections. The alternatives are either inaccurate information or requiring the individual to be an "errand runner" in the process. While individual involvement is clearly desirable from a public-policy point of view, it can be impractical, or insufficient, or both, and especially when the correction is initiated by the record-keeping organization itself. In this case, the individual will probably not even know about the correction. The technical implication of the emerging policy response to this problem, however, will be the need for more routing data.

[18]See: *Personal Privacy in an Information Society*, pp. 524-26, and Appendix Volume 4, *The Privacy Act of 1974: An Assessment.*

Appendix

Advances in Information Technology

The computer industry in the United States has consistently outperformed the predictions of its technological prophets. The ultimate potential of the computer and the fullest scope of its applications frequently elude technologists, who often have difficulty hypothesizing technological breakthroughs of which there is yet no hint, even though they are bound to occur in a myriad of different ways. As Martino [1] puts it, technological progress is a continuous process of breakthrough; assuming that none will occur in the future is a highly unlikely course of events. All of the projections discussed in his report have proved to be overly conservative. Like a more recent forecast [9], they are based on the assumption that the future will be characterized by an evolutionary improvement from currently known component technologies and computer architectures. While this may or may not be true, past history leads us to the nearly inescapable conclusion that computer technology will continue to create unforeseen capabilities which will exert irresistible pressures for their adoption also in record-keeping systems.

The discussion in this appendix will present a summary of advances in computer technology that are likely to have an impact on record keeping, personal privacy, and individual liberties. Unlike the body of this volume, it is intended for the technologically sophisticated reader, although the nontechnical reader should be able to get a sense of the types and trends of technological developments. A list of references is also provided, some of which will be cited in the text (with square brackets).

Computer Systems

At the present time, it is customary to classify computers as conventional computers, minicomputers, and microcomputers. The *conventional* small, medium, and large computers are characterized by a physical size of many cubic feet, a required floor space of many square feet, and purchase costs starting at tens of thousands of dollars. Nominal processing speeds[1] range from hundreds of KIPS (thousands of instructions per second) to approximately a hundred MIPS (millions of instructions per second). Until recently, computers in the conventional category tend to be

[1]There is no standard measure for processing speeds. Frequently, it is the rate at which the ADD instruction can be performed, although it is also often the rate at which some mix of instructions can be performed.

older designs and, thus, make limited use of the most recent microelectronic circuitry and large scale integration (LSI) manufacturing technology.

Minicomputers evolved in the late 1960's as physically small, portable units characterized by a short word length, a limited instruction set, and a processing speed of a few tens of KIPS; more importantly, the typical purchase price then approximated ten thousand dollars. Subsequently, low-cost bulk memory and input/output equipment were developed, and programming languages and operating systems suitable for small processors were designed. Performance improved steadily into the hundreds of KIPS and, at the present time, there is no longer a significant difference between small conventional systems and minicomputer systems. Minicomputers have dramatically extended the application of computers into areas where the cost and physical size of conventional ones would have been unacceptable. Now, there is a pronounced trend in the United States toward distributed minicomputer systems for some applications instead of using conventional computer systems.

Microcomputers are much smaller in physical size and cost than minicomputers. Hand calculators are a well known example of such technology. Microcomputers, much more powerful than any calculators—without, of course, bulk memory and input/output devices—can be placed on a single circuit board; for example, the LSI-11, the microcomputer version of the Digital Equipment Corporation's PDP 11/35 minicomputer, can perform all the processing tasks of the latter but is mounted on a single circuit card and, in large quantities, sells for 1/10th of the price. Microprocessor products are evolving very rapidly; speed and capability is improving steadily. Already, there are microprocessors with limited memory that occupy a single circuit package of less than two square inches in area; they require very little power, operate at high speeds, and sell for under ten dollars in large quantities. When such a basic processor package is combined with additional memory, power supply, and interface circuits for bulk memory and input/output, the cost is still under a thousand dollars and the volume is about one cubic foot. The microprocessor state-of-the-art is now rapidly approaching and overtaking the capability of some minicomputers. Except for shorter word lengths and relatively simple instruction sets, the most advanced microcomputers are competitive with minicomputers and sometimes even with smaller or medium size conventional computers.

The traditional computer vendors—the ones that have developed conventional machines—gradually moved from vacuum tube technology of the early 1950's into solid state technology of the 1960's, but because of financial considerations like plant investment, organizational resistance to change, and equipment installed with customers, they did not always embrace the latest advances in microcircuit technology as quickly as some of the newer, smaller companies. Thus, the initial minicomputers were largely introduced by a completely new group of vendors, although the traditional industry did add its own models in time. Similarly, microcomputers have involved new vendors as well—ones that tend to be closely connected to the microcircuit industry.

Each of the three, conventional, mini, and micro, is following roughly

a similar path in evolution—from simple architectures with modest memory and small instruction sets to complex architectures with huge memory and comprehensive instruction sets. The microcomputer is less than five years behind the mini in evolutionary sophistication, and the mini, in turn, is somewhat over five years behind the conventional machine on the evolutionary trail. Each, of course, progresses more rapidly than its ancestor, and in time, the three aspects of the present situation will blend into a continuum of computing capability—from smallest to largest, from simplest to most complex—which in all cases will be inexpensive, not always on an absolute basis but in terms of the unit of capability represented.

Similarly, programming languages are following the same progression. Microprocessors of the mid-1970's are using assembly language and programming techniques that were first conceived by the traditional industry in the mid-1950's. The mini's of the mid-1970's support the popular higher order languages and largely have sophisticated executive and operating systems—advances that the traditional industry achieved initially in 1955-65 period. In a very real way, the contemporary computing industry has been launched in successive decades—the conventional machine in the 1950's, the mini in the 1960's, and the micro in the 1970's.

Advances in the Computer Industry

In 1950, there were a few conventional digital computers in operation in the United States. In 1960, there were only a few minicomputers, and in 1970 a few microcomputers could be found in manufacturers' research laboratories. Today, in 1977, as illustrated in Figure 1, there are in operation tens of thousands of computers of each type [10,11]. It is estimated that in the time period from 1955 to 1975 the data-processing industry has grown from annual expenditures of approximately $500 million to $41 billion, a factor of 80. By 1980, the expenditures are expected to double, and then to double again by 1985. Annual industry-wide expenditures in data-processing research and development were approximately $1 billion in 1970, and $1.27 billion in 1975. They are expected to reach $1.5 billion in 1980, and $2 billion in 1985. Growth by such factors eloquently testifies to the universality of information and, equally, to the inevitable need to store and manipulate it.

The present data-processing industry is in the midst of change to an *information* processing industry, with consequent new applications. Many innovative aspects of business communications, in the broadest sense of the word, are being introduced—word processing, message systems, point-of-sale, and electronic funds transfer systems, among others. Some businesses and industries have been installing new computer-based systems seemingly without pause. Others, in order to remain competitive, are installing systems or automating information-handling operations for the first time [12]. Implications for personal information record-keeping systems are clear: many systems that are now manual will be automated; very many new systems will be created to support new services and meeting new demands; decisions that are now made by people will be turned over to automated

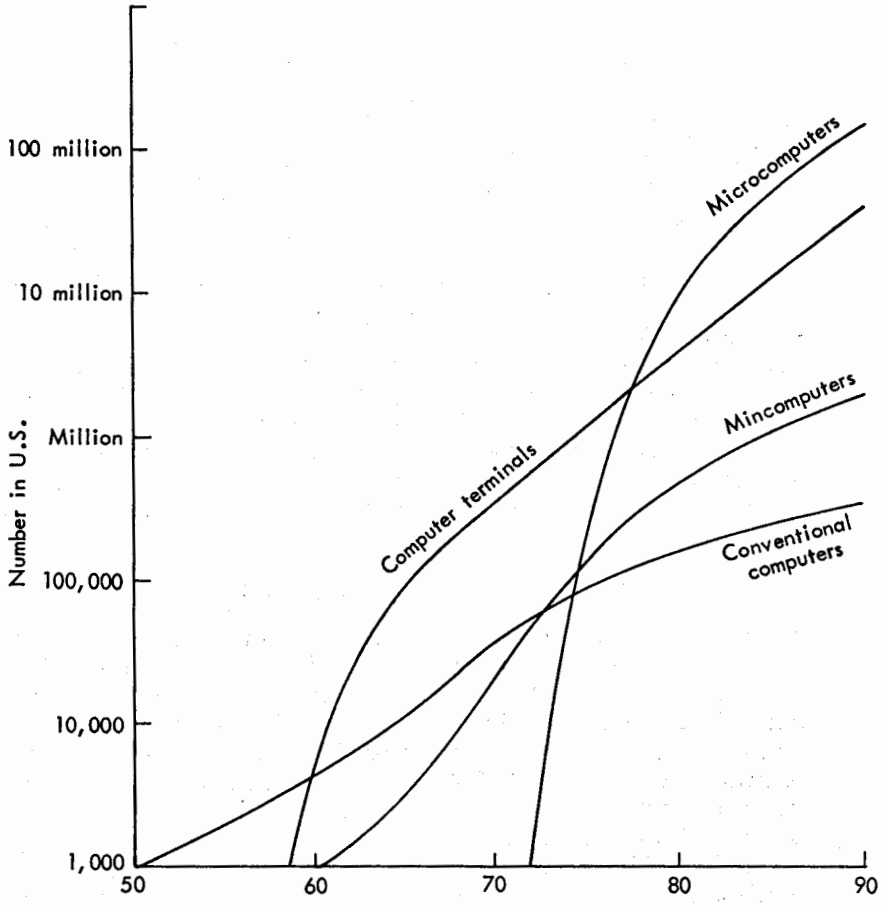

Fig. 1 — Projected growth in installed computers and computer terminals

processes; and systems will regularly communicate with one another through totally automated interfaces. And there will be more than enough computing power available, usually at attractive prices, to support anything that an organization finds economically attractive.

Microelectronics and LSI

Using photolithographic, electron-beam, or x-ray techniques, arrays of complex patterns of tens of thousands of line segments are projected onto tiny areas on a wafer of silicon, and then subjected in a high vacuum to chemical treatments and depositions of ultra-thin layers of various semiconducting, insulating, and metallic materials. The end-product of this activity is the large-scale-integrated (LSI) microelectronic circuit on a monolithic silicon chip typically one quarter inch square. On a single such chip, there might be a 16-bit microcomputer complete with thousands of bits of memory, a 16-kilobit[2] memory unit complete with addressing circuits, or a scanning circuits for an electronic camera.

Future advances in microelectronic LSI manufacturing technology will depend on improvements and innovations that can be achieved in:

(1) design of the basic elements (logic gates or memory cells) and their interconnection;
(2) manufacturing processes, techniques and apparatus;
(3) logic design and layout of the functional circuitry; and
(4) end use that can justify mass production of such devices and, thereby, maintain low price by absorbing design costs over the large number of units.

The general goals of LSI manufacturers of computer subsystems are to put on a single chip more computing capability or more memory capacity, and to obtain improved performance through higher speed. Increasing the number of components on a chip reduces the number of chips that must be used, reduces the number of interconnections among them, permits more automation in computer manufacture, and reduces the overall manufacturing and packaging costs. Even though the initial design, layout, and testing complexity and corresponding costs do increase, a sufficiently large production run recovers them and the prorated share per chip is negligible. Since advances in computer-aided design of a chip and automated testing both promise continuing reduction in the initial design cost, the size of economical production runs still remains within reason. To illustrate the payoff from increased element density, it is now possible—using 16-kilobit memory chips—to package a 256-thousand character high-speed changeable (random access) memory unit on a single 16-by-18 inch circuit card. Obviously, if only 4-kilobit chips were available—as was true only a year or two ago—several cards would have been needed. And density continues to increase.

[2]One kilobit is 1,024 bits; and a bit is a binary digit. This seemingly strange number is 2 to the 10th power. Use of powers of 2 is only natural when dealing with a binary machine and a binary numbering system. A character is typically represented by eight bits.

Circuit Element Density

To increase the computing or memory capacity on an LSI chip clearly requires more basic circuit elements—transistors, diodes, resistors, and capacitors—on a chip. There are four general ways to do this: (1) increase the chip area, (2) reduce the physical dimensions of the circuit elements, (3) reduce the area used by interconnections among elements, and (4) develop innovative logic design and placement of elements to minimize the number and length of interconnections.[3]

Since 1959, when the first planar transistors were manufactured, chip area has been increased by more than 20-fold to the present commonly used area of some 50,000 square mils,[4] or about one-twentieth of a square inch. Radical increases in size are not expected in the future, since the yield from the production line decreases as the chip area increases. More defects in the silicon substrate are likely to exist in a larger area and errors in layout alignment are amplified at the edges of a larger chip. A modest increase in chip area, perhaps a factor of four, can be expected by 1985.

Using elements in new circuit arrangements, as well as conceiving new ways in which to structure the elements, has had an important role in increasing the density of both processor and memory chips. For example, in 1974, when bipolar integrated injection logic was introduced, the improvement over the previously widely used bipolar transistor-transistor logic circuits was dramatic. The linear dimensions of a logic gate were reduced by a factor of 3.5 and, thus, density increased by a factor of 10; in addition, the power dissipation per gate was reduced by a factor of nearly 1,000 to less than 0.1 microwatts[5] per gate. The power requirement had been reduced to a point where a single 1.5 volt flashlight cell would suffice. Likewise, improvements in circuit element designs have continued to pour from laboratories in the United States, Europe, and Japan at an astounding rate. While the fastest logic circuit can switch in the .05 to .01 nanosecond[6] range, the cost of such operation is still relatively high since power dissipation of 20-50 milliwatts[7] per gate is required.

Circuit element dimensions can be scaled down by reducing the line width used in designing circuit elements and their interconnections. The present state-of-the-art is 1-2 micron[8] widths, which is essentially at the ultimate limit of optical techniques. However, with electron-beam technology it is possible to reduce the line width further, perhaps to a limit of 0.05 microns. X-ray techniques have surpassed even this limit; a width of 0.008 microns has been produced in laboratory and 0.004 micron width is considered possible. It has been noted that the latter represents more than a 100-fold reduction in the present dimensions of the basic circuit elements.

[3]To put this in perspective, it should be remembered that one chip will contain many thousands of elements; thus, it is an intricate task to minimize the number and length of interconnections among them.

[4]One mil equals one thousandth of an inch.

[5]One microwatt equals one millionth of a watt.

[6]One nanosecond equals one billionth of a second.

[7]One milliwatt equals one thousandth of a watt.

[8]One micron equals one millionth of a meter equals four hundredths of a mil.

Since area is proportional to the square of linear dimension, the corresponding reduction in the circuit element area could exceed 10,000.

In addition to the semiconductor circuits discussed above, there are a variety of others that can be used to construct logic circuits and memories; the leading contenders are charge-coupled devices (CCD), magnetic bubbles, and Josephson junction devices—the last of which must be operated at temperatures of liquid helium.[9] Each offers tradeoffs in simplification in circuit design, higher densities, or improved speeds; for example, 64 kilobits of CCD memory can easily be packaged on a single chip—as opposed to 16 kilobits with present semiconductor technology.

In summary, LSI circuit technology is advancing at an incredible rate. As illustrated in Figure 2, component density on a single monolithic chip is more than doubling every two years [12,13]. This trend can be expected to continue for the next 10-15 years as electron-beam and x-ray techniques are used to further reduce the widths of connection lines used in mass-produced LSI chips.

Circuit Speed and Cost

Reduction of circuit-element dimensions reduces their intrinsic signal propagation delays, as well as reducing the delays caused by the length of interconnections; consequently, the overall operating speed is increased. Figure 3 illustrates the historical trend in logic circuit speed and projects it into the future. As shown, speed increase cannot be expected to continue indefinitely, since fundamental limitations imposed by the laws of physics will be reached in the 0.02 to 0.005 nanosecond range.

Manufacturing costs of LSI chips tend to increase relatively slowly as density is increased, especially when the circuitry has a geometric regularity of structure. Therefore, as density increases the prorated cost per circuit element decreases more rapidly than the cost of accommodating additional complexity increases. Figure 3 depicts the expected cost reductions.

Projected increases in circuit element density and switching speed, plus reductions in cost, collectively imply that in the future an abundance of inexpensive, computationally powerful microcomputers, as well as high capacity memory chips, will be available for use in hundreds of new applications. An unprecedented spurt in record-keeping activities will undoubtedly result as a byproduct of the many new applications which advances in information technology make possible.

Trends in Processor Performance and Costs

The maximum data-processing rate of a computer depends on the speed of its basic logic circuitry, the access time of its memory hierarchy, instruction execution times, the hardware architecture, and the efficiency of the application and system software. Although the interactions among them

[9]Temperatures of approximately four degrees Kelvin (i.e., four degrees Celsius above absolute zero, or -269 degrees Celsius).

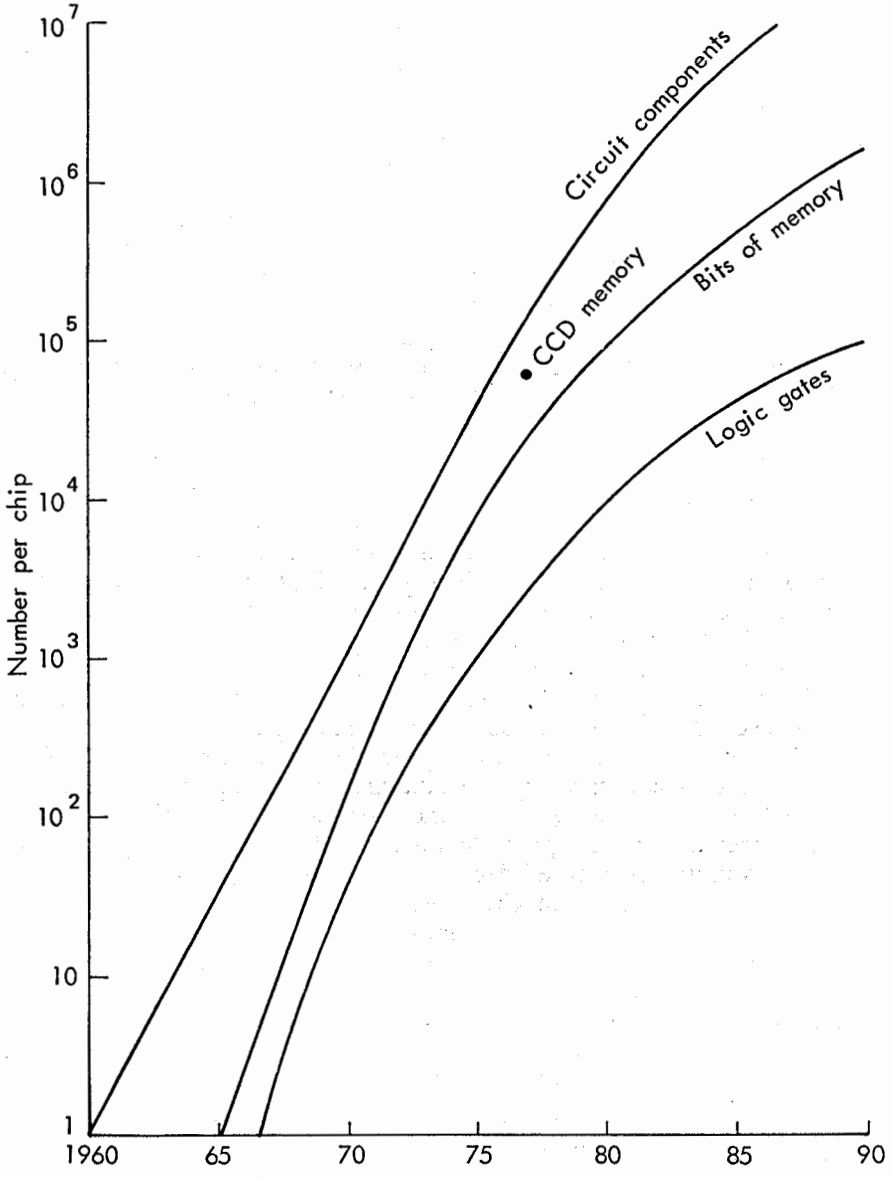

Fig. 2—Projection of semiconductor circuit density

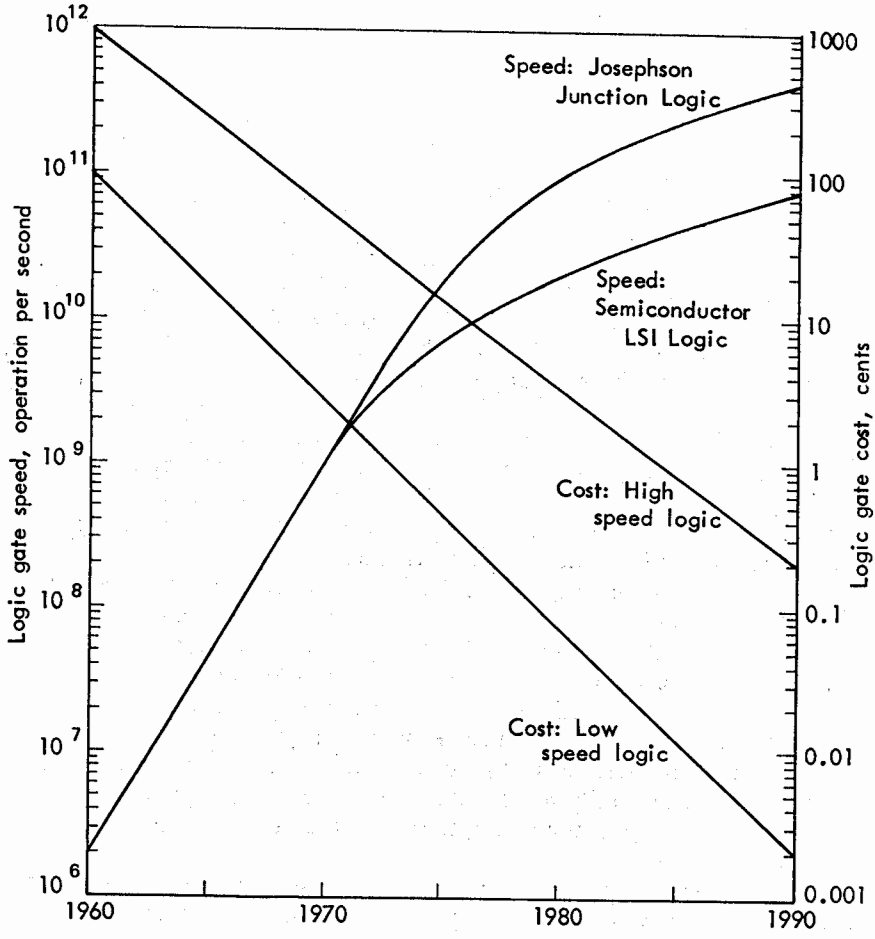

Fig. 3 — Logic circuit speed and cost projections

are quite complex, reasonable and credible projections of future processing speeds can be made.

It is customary to estimate the computing speed of a computer in terms of millions of instructions per second (MIPS) achievable by the hardware when it repeatedly executes a representative set of instructions. Typically, additions are used to represent instructions with short execution times, and multiplications to represent long times. In record-keeping applications, nearly all instructions are of the short variety and, thus, projections of attainable processing speeds can credibly be based essentially on the addition time. Figure 4 depicts projections of the fastest attainable addition and multiplication times in the 1980's [9,11], assuming that appropriate architectural improvements are made in arithmetic units, such as incorporating a high level of carry look-ahead in the adder and using special-purpose arrangements to facilitate multiplication.

For many years now, special arrangements have also been implemented in the control unit to increase the efficiency of fetching instructions and data from the memory hierarchy. While an instruction is being executed, the control unit will fetch from memory the next instruction (or group of instructions) and its associated data in order to maximize the efficiency of performing arithmetic and logical instructions.

Since the processing of textual information tends to involve a different mix of instructions—more short ones—than scientific applications, projections of speed will be correspondingly different. Maximum feasible speeds for general information processing and record keeping (as distinguished from scientific computations) are depicted in Figure 5 for two advanced computer architectures—large-scale uniprocessors and vector processors [9,11]. Other architectures that can operate even faster, such as array processors, are generally more suitable for scientific computations than for record-keeping applications and, therefore, are not included in the projection.

Mini- and microcomputer speeds will also increase at a comparable rate, because they use the same basic technology. However, they can be expected to remain about two orders of magnitude below those attainable by large-scale uniprocessors. Mini- and microcomputer applications are likely to be less demanding; typically, they will be embedded in intelligent terminals or will provide computational support to only a small number of terminals. They are likely to be used for special-purpose record-keeping applications in which ultra-high speeds are not required and where low cost is likely to be an important consideration. The highest speeds for mini- and microcomputers can be expected to follow the lower curve in Figure 5.

LSI technology for computer logic and memories has dramatically reduced the hardware portion of the cost of computing power (e.g., as expressed in terms of dollars to purchase one MIPS of processing speed). Figure 6 depicts its effect for both large, very high-speed computer systems and for minicomputers [9,11,13]. It should be noted, however, that certain other hardware-related costs, such as electromechanical input-output devices, power supplies, and cabinets, as well as the labor required to

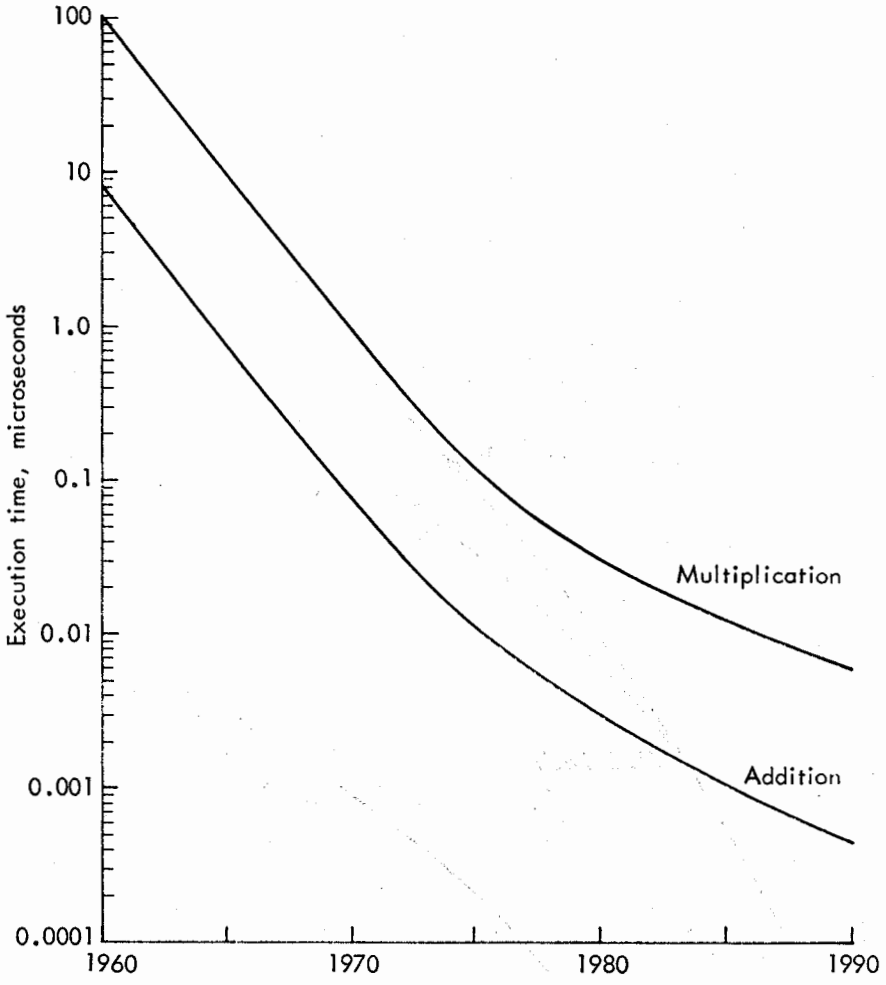

Fig. 4— Instruction execution times

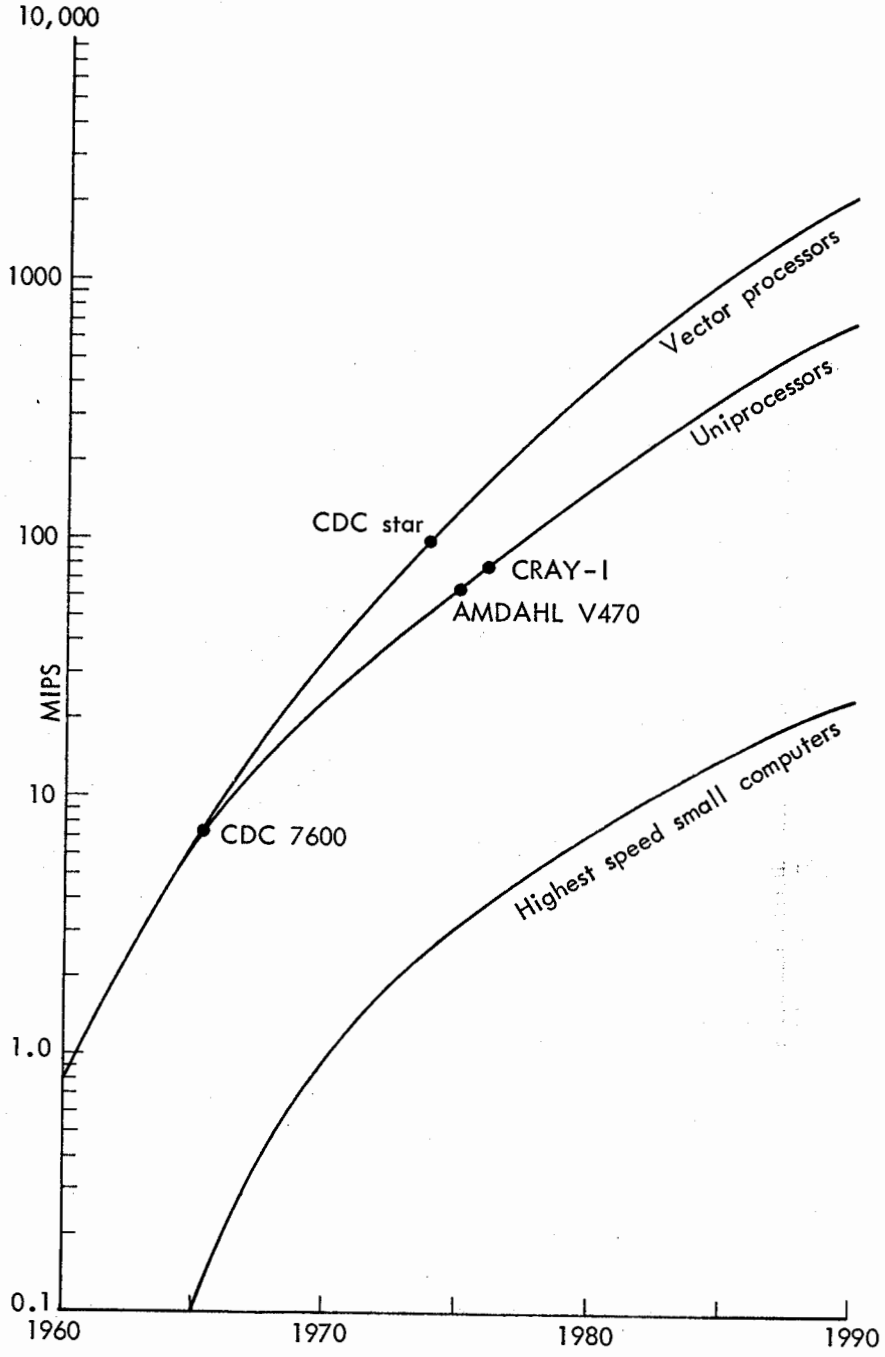

Fig. 5 — Trends in processing speed

package the various hardward components into a final system, are not decreasing as rapidly—if at all.

Computer programming is another area in which cost reduction is progressing rather slowly—if at all. It is labor intensive, rather than technology intensive, and is not affected directly by a decrease in hardware cost. Correspondingly, the fraction of total system costs attributable to software is continuously increasing. In the 1960's, software costs were estimated at 25 to 40 percent of the total cost; but in the mid-1970's, software costs were in the 60-70 percent range. By the 1980's, software production costs are expected to be nearly 90 percent of the system's cost, principally because hardware costs are declining dramatically while software costs are dropping very slowly.

A part of the relatively high software cost is due to difficulties in improving programmer productivity. At the present, it is estimated that the cost to produce one correct and tested line of reasonably complex computer program code is $10; the outlook for the 1980's promises only a modest reduction—perhaps down to $5. Even here, however, such a reduction is possible only because of greater use of hardware to reduce the complexity in programs (e.g., by providing built-in features, such as virtual memory, enhanced instruction sets, and subroutines implemented in microprograms). Another aspect of the high software cost is the intrinsic difficulty of describing completely and unambiguously the sequence of detailed steps required to achieve some desired result. Thus, high software costs stem in part from productivity limitations and partly from the genuine inherent intellectual difficulties of identifying the details of the process. Finally, a large percentage of many programmers' time is often spent on maintaining "old programs" rather than in developing new ones.

In summary, the implication for record keeping of the trend projections in Figures 5 and 6 is that computer systems will be available which can provide—for practical purposes—any desired amount of computing power at costs significantly less than those associated with present systems. Hence, generally speaking, hardware cost will no longer constrain management decisions to establish new record-keeping systems. On the other hand, software costs, as well as problems in producing and maintaining reliable software, are likely to remain an important consideration.

Trends in Data Storage Technology

A basic objective in the design of a data storage system for a high-performance computer system is a very large storage capacity plus the system architecture to provide very rapid access to it. To date, this objective has not been achieved adequately, principally because the access time to a memory unit tends to increase when storage capacity increases. It has been necessary, therefore, to resort to architectural means, such as:

(1) organizing the memory into a hierarchical structure of progressively larger but slower memories (e.g., buffer memories, high-speed main memories, on-line direct-access memories, and very large mass memories)—buffer memories have

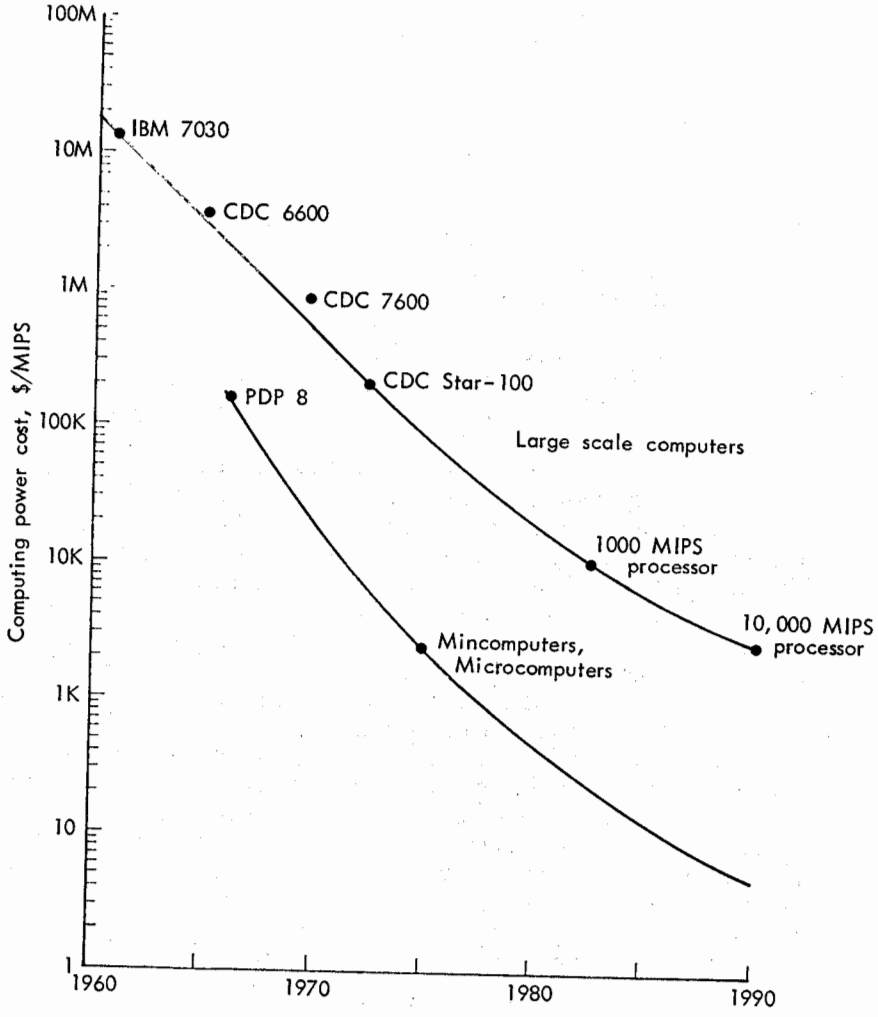

Fig. 6 — Computer power cost

the fastest access speed and smallest capacity, while mass memories are relatively slow but can store billions of characters;

(2) establishing high-speed data paths between the processor and the memory hierarchy, and, within the hierarchy, by transferring many data words simultaneously;

(3) organizing memory units at a particular level in the hierarchy into several independent ones which can be operated simultaneously in an interleaved manner so that, if the data are properly distributed, the effective data transfer rate is increased; and

(4) compensating for memory speed limitations by sharing the processor with other tasks.

Several storage technologies are available for each level of a memory hierarchy. For buffer memories, very fast LSI memory chips can be used; random access main memories can be constructed from magnetic cores or from slower speed semiconductor memory chips. Direct access memories might use magnetic recording of tapes or discs, solid state charge coupled devices (CCD), or magnetic bubble memories; mass memories might employ magnetic tape, magnetic cartridges, or electron beam, holographic, or video disc technologies. Figure 7 illustrates storage capacity and access time attributes of available memory technologies [9,11].

In 1977, it is possible to deposit on a single, quarter inch square chip of silicon substrate a 16-kilobit semiconductor memory unit or a 64-kilobit CCD memory, or 100,000 bits of magnetic bubble memory in the same area on a garnet substrate. Since the latter two are realized as circulating memory loops, access time is greater than in the semiconductor random-access memories. Thus, they are being developed as replacements for the rotating storage devices, such as magnetic discs or drums. The storage density achieved (i.e., the number of bytes[10] per square inch) is an important design parameter, since it ultimately determines the cost of the memory and its physical size.

The three examples cited above represent storage densities of 28 kilobytes, 110 kilobytes, and 170 kilobytes per square inch, respectively. Future reductions of the interconnection line width, as discussed in the earlier section on Circuit Element Density, will increase achievable densities in all three memory technologies, and improve their competitive position in the memory marketplace versus present magnetic disc and tape units. Further storage density increases are expected from simplification of memory cell design; for example, new approaches to magnetic bubble memory loops, the so-called contiguous disc and bubble lattice techniques, are expected to increase bubble memory storage density by a factor of ten, even with present optical techniques for circuit layout [14]. Figure 8 is a projection of future storage densities for solid-state memory technologies, as well as for competing magnetic recording memory systems. Figure 9 compares unit costs—cents per character [11,13,14].

[10]One byte typically corresponds to eight bits, or one character.

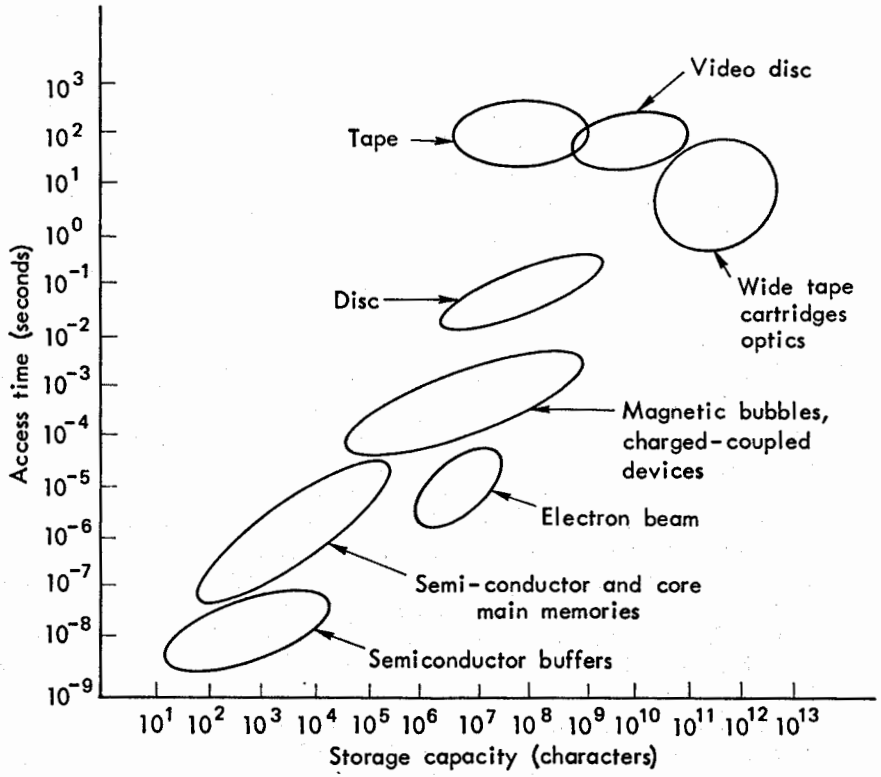

Fig. 7 — Storage capacity and access time of memory technology

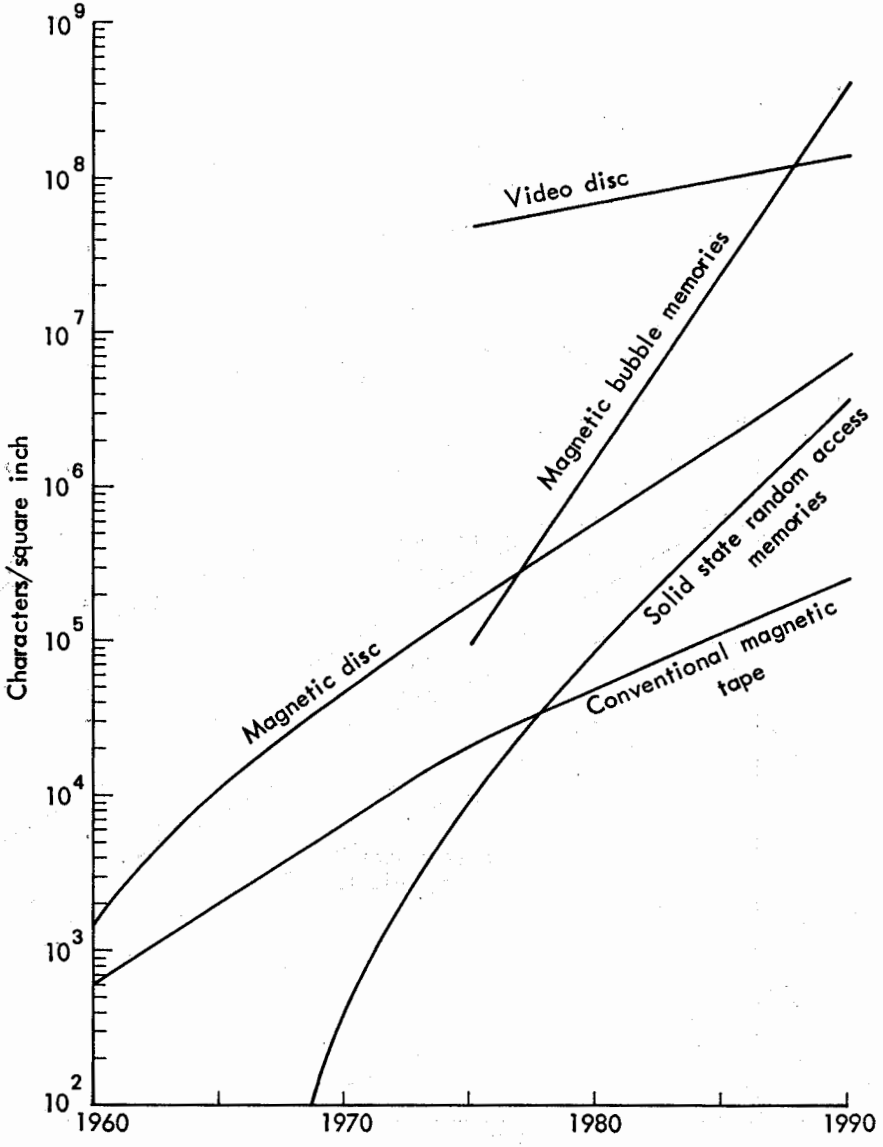

Fig. 8—Projection of storage density

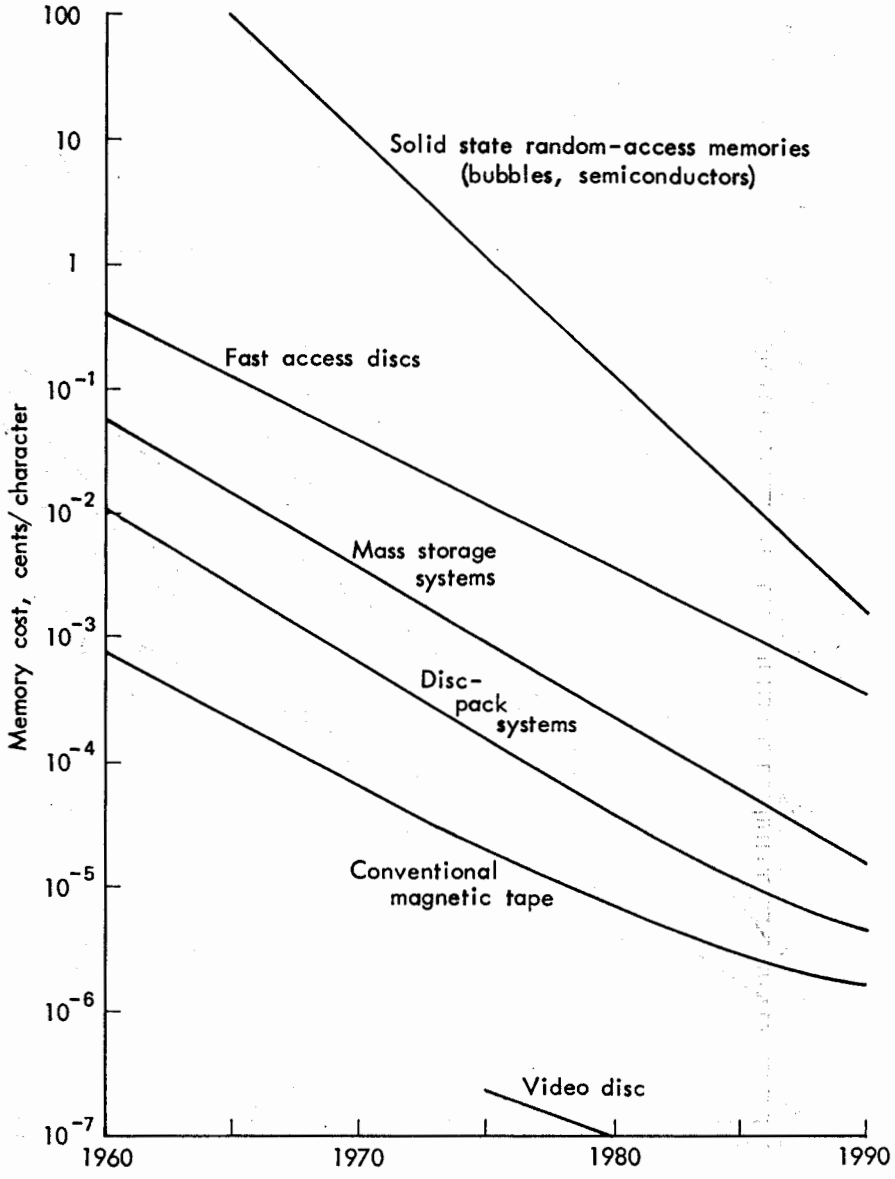

Fig. 9—Memory cost trends

For low cost, very long term storage, mass memory units are presently available with a storage capacity of nearly a trillion characters, and a 10-15 second average access time to any desired record. As an example, the Ampex Terabit system uses two-inch wide video tape reels that can store 5.5 billion characters each and can be searched at a rate of 1,000 feet per second; the IBM 3850 data cartridge system stores over 470 billion characters, and the average access time is 3-8 seconds. Even larger mass memory systems can be developed in the next 5-10 years as improvements are made in storage density on magnetic media. Other technologies will also become available—electronic-beam and holographic memories are now in prototype stages. There is no question that very large and very low cost computer-readable mass memories will be widely used in tomorrow's systems. It is reported, for example, that 700-1,000 orders have already been placed for systems such as the IBM 3850 [16].

Present computer systems are characterized by functional specialization; there is an arithmetic-logical unit, a memory unit, input/output units, and mass storage. Since the same basic technology is used to manufacture memory chips as to produce logic circuits, new opportunities arise for combining memory and processing into "intelligent memory" systems [17], where some processing can be done in the same monolithic unit with data storage. Indeed, there is often no reason why data should be collected and maintained in a special repository and then sent to some central location for processing. Elimination of time-consuming data transfers between a processor and a memory unit can produce truly significant improvements in performance, simplify designs, and reduce costs.

Data Communications

In the course of the last decade, data communication systems have become inextricably involved with data-processing systems; sometimes, it is difficult to determine where one ends and the other begins. The merging of data processing and data communications is occurring because of the technical advances now being made in the communications technology—rapid growth in availability of communication channels for short, as well as long, distance traffic, increases in transmission speed, reduction in cost, and increases in reliability. The drive for advances in communications technology has come from the marketplace, where users of data-processing systems have pioneered new uses of computer systems that depend heavily on data communications [17], such as:

- real time processing of transactions originated at terminals geographically distributed at many locations;
- extension of centralized processing power to users at remote locations;
- communications between processing centers and data bases;
- sharing of special processing capabilities and data bases with users at many locations;
- balancing of computational loads on individual processing systems by directing computing loads to other systems; and

- providing reliability, backup, and recovery to participating systems by shifting the computing task to other processors should the originally assigned processor fail.

To provide each service, a modern data communication system not only must provide sufficiently capable communication channels, but it also must be able to maintain adequate connectivity among all parts in a network. Ideally, any necessary switching operations for the purposes of network management should be done in a way that is transparent to the user.

The history of telecommunications is one of continuing progress. In the last 50 years, data transmission capacity of major telecommunications systems has increased three orders of magnitude: from 3,000 characters per second in the early 1920's by multiplexing 12 voice channels on a single wire pair, to 8 million characters per second in today's coaxial cable and microwave systems carrying 32,000 voice channels simultaneously.[11] Helical waveguide and optical-fiber systems are now in pilot operation and will provide even larger capacities, up to 100,000 equivalent voice channels, in the 1980's.

Communication channels are either land-lines, including microwaves, or satellite systems. Land-line communications capability in the United States, expressed in terms of voice channel-miles, has been increasing by a factor of 10 every 12 years, and is expected to continue growing at the same rate for the next 20 to 25 years [14]. Besides the increasingly more efficient use of voice channels, special digital channels have been developed which provide for even more efficient data transmission. The number of communication satellite circuits has also grown impressively. For example, the first INTELSAT communication satellite in 1965 provided 240 circuits at a cost of $22,000 per circuit per month, with the satellite lifetime of 1.5 years; 10 years later, INTELSAT IV provides 6,000 circuits at $600 per circuit. Moreover, present satellite lifetime is expected to exceed seven years, and INTELSAT V is expected to provide 100,000 circuits for 10 years at $30 per circuit [17]. Figure 10 depicts expected increases in data transmission rates; and Figure 11, the associated cost projections [18].

Data Input, Output, and Man-Computer Interaction

Devices for data acquisition and dissemination and for man-computer interaction are also benefitting from advances in LSI technology. Microprocessors and memories are now available for installation in data acquisition and dissemination devices to increase their speed, versatility, and reliability; inexpensive high-speed computing capacity also makes feasible the use of entirely new means for man-computer communication. For example, limited recognition by computers of individually spoken words is now possible; likewise, computers can synthesize spoken word responses [19].

[11] By way of comparison, a very fast typist can type at the rate of 15 characters per second, or approximately 140 bits per second. Computer-to-computer transmission typically occurs at the rate of 1,200 bits per second, although higher and lower speeds are possible. A typical television channel ranges from 1-6 million bits per second.

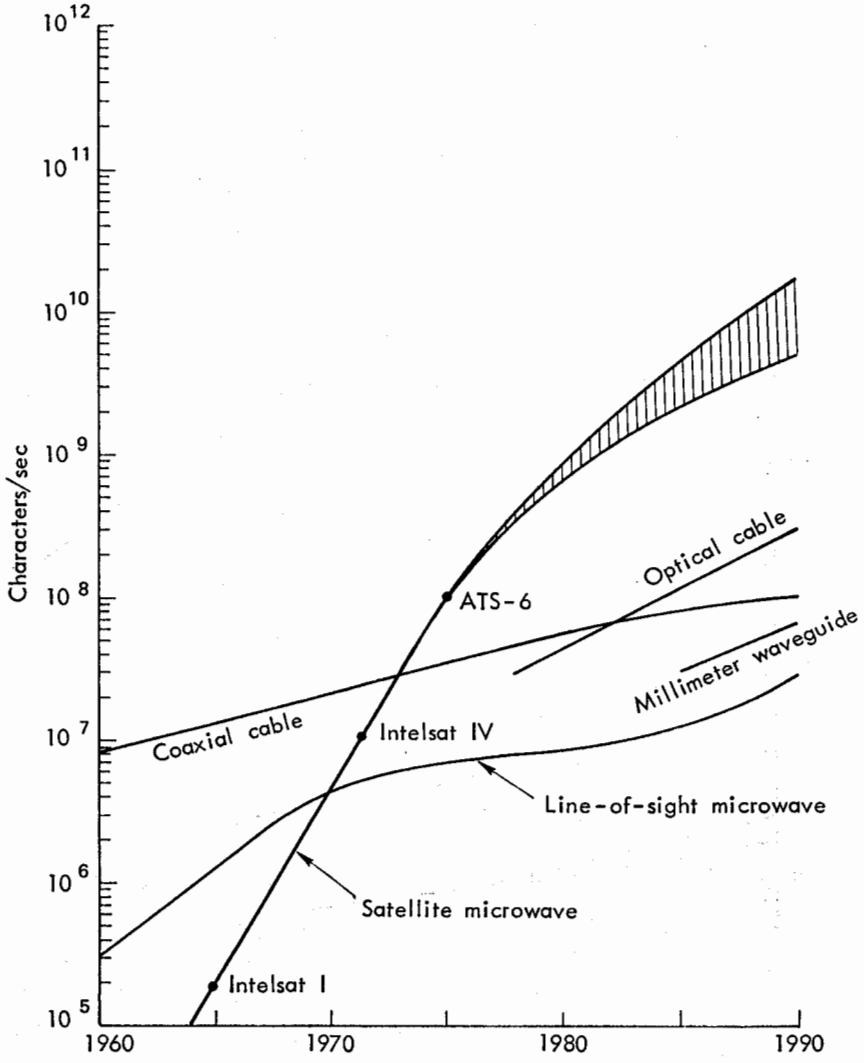

Fig. 10 — Trends in data communication speed

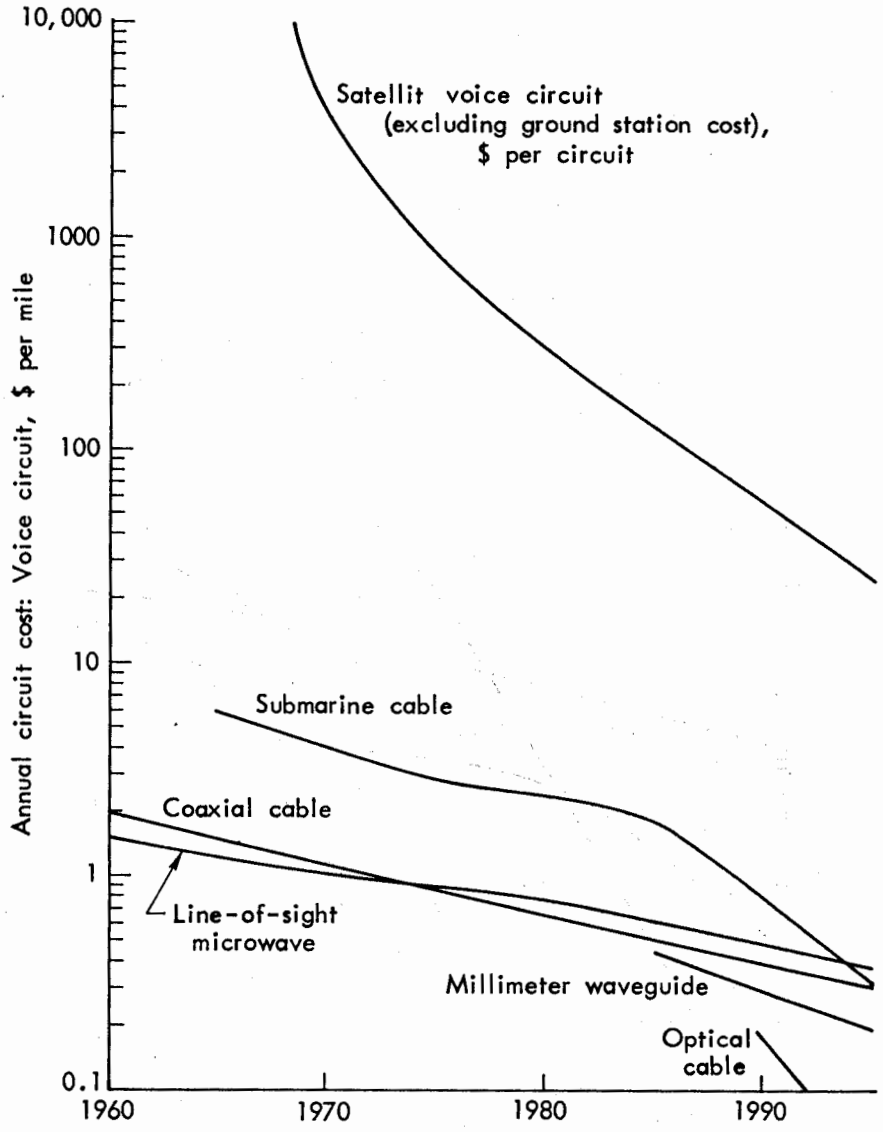

Fig. 11 — Trends in communications costs

Data Entry and Conversion

Historically, all input data and programs were first punched into cards for processing by electromechanical readers, initially at rates of 300-400 characters per second and later as fast as 2,000 characters per second. However, the necessity to use human operators to convert data into machine-readable form remained a bottleneck, since manual keying rates seldom exceeded 3-4 characters per second. Hence, large numbers of operators had to be used, and data entry costs could at times be much greater than data-processing and storage costs. Subsequently, direct key-to-tape and key-to-disc data entry devices were developed; while they doubled the data entry rate, they could not significantly alleviate the cost and speed disparities.

Development of optical character recognition (OCR) devices was an important advance in data entry and conversion capability. Such devices could read text (in certain acceptable printing fonts only, otherwise the error rate would be intolerably high) a page at a time at rates of 2,000 to 10,000 characters per second—with a potential of 60,000 characters per second in the future. Interestingly, the principal technical problem is the mechanical one of transporting documents through the reading station at sufficiently high rates (at least 2,000 pages a minute) to fully utilize the available reading rate. At such high rates of data conversion, it would be theoretically possible to fill a billion-character storage unit in five hours. By 1980-85, the present cost of high speed OCR devices—$20,000-$80,000—is expected to be much lower. Hence, conversion of manual record-keeping systems into computer-processable form will become increasingly economical. This is an important portent for manual systems that will become automated, and will significantly reduce the cost of data transcription for textual material, such as reports, letters, and memoranda.

Automated Data Acquisition

Acquisition—or capturing—of input data directly in computer-readable form eliminates the need for data conversion and further improves the economics of computerized record-keeping systems. The use of mark-sense[12] machine-readable answer-sheets for exams and for a variety of data collection forms illustrates one approach. Other techniques now in use or in research laboratories include:

- optical scanners for reading stripe-coded information (e.g., on merchandise with the "universal product code" scheme);
- characters printed in magnetic ink;
- digitization of TV camera output, and output from solid-state electronic cameras;
- digitized speech signals for man-computer communication and in telephony; and
- use of miniature transmitters that emit coded signals continu-

[12]The term "mark-sense" refers to a scheme for marking a document by pencil in such a way that it can be read by a special device.

ously or in response to queries for identification or position tracking.

With the use of the latter sensor systems, it is possible—technically and, in many cases, economically and practically as well—to assemble large amounts of information on individuals and their activities in record-keeping systems that can support surveillance functions. A recent congressional report explores the possibilities in detail [20].

In the future, minaturized computational power can be used directly in a sensor itself for initial processing before data are transmitted to larger systems for sophisticated processing and manipulation. Recent advances in pattern-recognition algorithms—and the programs to implement them—permit limited understanding of speech signals, detection of selected words or phrases in conversations, identification of human faces and fingerprints, and analysis of biomedical signals and images [21].

There are now installed in the United States over 120 million telephone instruments; very few households do not have one. Hence, if they were converted to touchtone instruments, there would be theoretical a capability in nearly every household to dial into a computer system and to input digital data into it (without any additional hardward devices), as well as to receive computer-generated spoken instructions or responses from it. It would be theoretically possible to respond to a questionnaire, such as the U.S. Census, directly in computer-acceptable form. Questionnaires and instructions could also be presented visually on a standard home television set, and the telephone instrument used as a terminal for responding. With such capabilities, computer systems could be programmed to automatically contact by telephone or by cable TV, using selective addressing to subscribers, desired population samples for obtaining a response to some government or commercial inquiry. If such activities were to become sufficiently economical—they already are technically feasible—and were permitted to occur without control, record keeping would take on new and vastly enlarged dimensions. With only a little more technical progress, low cost solid-state cameras could be incorporated in TV sets or telephone instruments so that graphical data could be collected from individual homes in addition to textual responses.

Data Dissemination

In the last year or two, printer technology has made several significant breakthroughs so that speeds of 12-15,000 lines per minute are now available [22]; the cost is less than a half cent per page. Even more economical, however, is computer-generated microfilm or microfiche output which can be produced at 20-25,000 lines per minute and which consumes much smaller quantities of expendable materials.

Rapid advances are now occuring in facsimile equipment which, at the present time, can transmit a standardized page of text or graphical images over a telephone line in four minutes. There are presently several hundred thousand facsimile units in use in the United States [11], but the quantity is expected to exceed one million by 1990. In the future, such units are

expected to transmit a page of text over a broadband communication circuit in 10 seconds. Since the material used for such service costs a small fraction of a cent, it will be feasible, both technically and economically, in 10 years to use facsimile units in homes to receive the daily news copy (assuming that there were broadband communication circuits to every home).

Man-Computer Interaction

There is no doubt that future computer systems can and will be used to perform much more sophisticated data-processing operations than is done now. The man-computer interfaces across which data, instructions, or results of computations must flow may still be a major barrier for effective use of them, and it takes on great importance when the system is used in real time, cooperative man-machine control operations, or in a human-to-human exchange, such as with computerized interpersonal communications.

An essential difficulty is the differing capabilities and characteristics of humans and the computer. For example, a person communicates not only through speech, but simultaneously also with gestures, facial expressions, voice inflections, and other body language. Such supplementary cues can not be sensed by contemporary computers for transmission to another person in a computerized system. Thus, individuals presently must restrict themselves unnaturally to a single mode of expression or to written messages, and learn how to convey intentions in a single dimension. In the future, it will be possible to equip computer terminals not only with speech recognition capability but also with sensors for transmitting visual images of the user.

The Imperative

The brief descriptions and graphs presented have attempted to convey the vigor and dynamics of the computer-communications industry in the United States and other industrialized nations. It is evident that ample technology is already available for supporting most of the automated record-keeping systems that an organization may wish to have. Laboratory prototypes of new data-processing equipment, plus pilot systems of new uses, cannot help but spur increases in record keeping. While there is always a substantial latency time between the laboratory prototype or demonstration model and its operation use, this period seems to be shortening steadily. This is occuring partly because the pace of affairs in the world is faster, partly because escalating costs are driving labor-intensive systems into automation, partly because the mere existence of a device or a technical capability spurs innovative applications, and partly because the use of information by automated means caters to any organization's inherent motivation to function better, to move in new directions, and to make decisions based on the largest amount of relevant data. Thus, there can easily be less and less time to evaluate new directions in record keeping and to perceive or anticipate their effects on individual rights and freedoms. When systems are implemented and in place, it is often too late to prevent

harmful uses or intrusions into privacy. Progress in information technology, and its inevitable use to support a country already large and complex and always striving for efficiency, innovation, and progress, make it mandatory that proper safeguards for personal privacy must come before, not after, the fact.

References

1. Martino, J. P., *Technological Forecasting and Decisionmaking,* American Elsevier, New York, 1972.
2. Weik, M. H., *A Second Survey of Domestic Digital Computing Systems,* Report No. 1010, Ballistic Research Laboratories, U.S. Army Aberdeen Proving Grounds, Md., June 1957.
3. *Records, Computers and the Rights of Citizens,* Report of the Secretary's Advisory Committee on Automated Personal Data Systems (U.S. Department of Health, Education, and Welfare, Washington, D.C.), July 1973.
4. *Transaction Network,* Vol. 55, No. 1, pp. 8-14, Bell Laboratories Record, January 1977.
5. Head, R. V., "Rise and Fall of FEDNET," *Journal of Systems Management,* pp. 7-13, October 1975.
6. Miller, A. R., *Assault on Privacy: Computers, Data Banks and Dossiers,* University of Michigan Press, Ann Arbor, Michigan, 1971.
7. Westin, A. F., and M. A. Baker, *Databanks in a Free Society: Computers, Record-Keeping and Privacy,* Quadrangle Books, New York, 1972.
8. Martin, J., *Computer Data Base Organization,* Prentice-Hall, Inc., Englewood Cliffs, N.J., 1975.
9. Turn. R., *Computers in the 1980s,* Columbia University Press, New York, 1974.
10. Dolotta, T. A., et al., *Data Processing in 1980-1985,* John Wiley & Sons, New York, 1976.
11. Clayton, A., and N. Nissenoff, *The Influence of Technology Upon Future Alternatives to the Scientific and Technical Journal,* Final Report, NSF Contract GN-42204, Forecasting International, Ltd., Arlington, Va., October 20, 1975.
12. Pullen E. W. and R. G. Simko, "Our Changing Industry," *Datamation,* January 1977, pp. 49-55.
13. Edwards, N. P., IBM Corporation, Yorktown Heights, N.Y., private communication on technological advances.
14. Torrero, E. A., "Bubbles Rise from the Lab," *IEEE Spectrum,* September 1976, pp. 29-31.
15. Greenblatt, B. J., and M. Y. Haiao, "Where is Technology Taking

Us in Data Processing Systems?", *AFIPS Conference Proceedings, Vol. 44, 1975 NCC,* pp. 623-628.

16. Edelberg, M., and L. R. Schissler, "Intelligent Memory," *AFIPS Conference Proceedings, Vol. 45, 1976 NCC,* pp. 393-400.

17. Branscomb, L. M., "Trends and Development in Computer/Telecommunications Technologies," *Conference on Computer/Telecommunications Policy,* OECD Informatics Studies 11, Organization for Economic Co-Operation and Development, Paris, 1976.

18. *A Forecast of Space Technology 1980-2000,* Report NASA SP-387, Scientific and Technical Office, National Aeronautics and Space Administration, Washington, D.C., 1976.

19. Flanagan, J. L., "Computers that Talk and Listen: Man-Machine Communication by Voice," *Proceedings of the IEEE,* April 1976, pp. 405-415.

20. *Surveillance Technology - 1976,* Report by Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, U.S. Government Printing Office, Washington, D.C., 1976.

21. Chien, Y. T., "Interactive Pattern Recognition: Techniques and Systems," *Computer,* May 1976, pp. 11-25.

22. Butler, M. K., "Prospective Capabilities in Hardware," *AFIPS Conference Proceedings, Vol. 45, 1976, NCC,* pp. 323-336.

☆ U.S. Government Printing Office: 1977—246-000/6582