Communications, computers and people*

PAUL BARAN

The RAND Corporation
Santa Monica, California

INTRODUCTION

Communications and computers are today becoming what the economists call "complementary goods"—one without the other is of much lesser value—like pen and ink, pretzels and beer, and gin and dry vermouth.

Let us first briefly consider the impact of the computer technology upon the communications business and, conversely, how good, widespread, low-cost digital communications will allow a dramatic increase in the creation of new types of computer systems. Then we shall get down to the meat of the talk—a few of the unappreciated social consequences possible and, lastly, we shall proffer remedies in advance of the time society realizes there is a problem. If the order of things appears backward, with remedies being offered in advance of the patient's complaining of an ailment, it is due to our belief that the lead time for the cure of social ills is often longer than the gestation period of the disease. Only we who appreciate what is happening to computer development may be in the best position to see the thunder clouds.

THE IMPACT OF COMPUTER TECHNOLOGY ON COMMUNICATIONS

Communications equipment is sometimes categorized into switching equipment, transmission equipment, or terminals. As we expect to be talking about digital uses which by definition are digital terminals, we shall confine our observation to telephone switching and transmission.

At present, the telephone plant, our prime data carrier, is almost exclusively based upon electromechanical switching—that most primitive form of computer logic —and one that we in the computer business haven't seen around for years. Transmission is by means of frequency division multiplexing—or about as analog (or undigital) an operation as we computer types can envision. The only kind words a computer man can have for this system is that it works; it works well and has been working well for many years—for the purpose for which it was designed.

While perhaps slow by pace, electronic switching has arrived on the scene for the telephone company. At least two separate systems in this country have now passed field trials and are being installed commercially. This new equipment may be representative of the future telephone local central offices. At present, these electronic switches are not believed to be more economical than their earlier electromechanical switch counterparts. But their prime advantage lies in the *new additional services* that they offer because of the general computer nature of the control mechanism of the switching center. For example, it will be possible to dial only two digits to reach the few numbers that you call often. It will be possible to relay a call to another telephone if you are temporarily away. Automatic diagnostic routines will permit repair and mainte-

*Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of The RAND Corporation or the official opinion of the policy of any of its governmental or private research sponsors.

nance by inexperienced personnel. Further, electronic switching is a new technology whose price is expected to decline rapidly in the future.

So much for switching. We also see computer technology creeping into the picture in transmission. The Bell System T-1 multiplexing system samples 24 analog voice channels about 8,000 times per second producing, together with synchronizing information, a data stream of 1.54 megabits per second which can be transmitted over ordinary copper pairs using pulse regenerative amplifiers. This pulse code modulation technique is being developed simultaneously in many countries and is in use but presently restricted for links on the order of magnitude of about 20 miles.

As pulse code modulation is the most economical of the multiplexing systems, it appears destined as the transmission direction of the future. Even though digital technology is entering the telephone plant slowly and in a piecemeal fashion, it is arriving and will make its impact felt. Specifically, most of the growth of the telephone plant may be expected to occur within these digital techniques areas. The implications to us are severalfold.

First, as we expect to see a rapid drop in the cost of digital circuits, we may expect continued drops in the price of digital communications in the future. We would also expect to see even more marked savings to the digital communicator as systems evolve which are more amenable to the all-digital processing of information from user to user. Today emphasis must be given to complete compatability with the large existing analog system in being where periodic reconversion to analog signals is required. Thus, one day we envision the bulk of the telephone system being built entirely of digital processing assemblies in lieu of the all-analog systems as of today. When this day comes, we computer types would view the telephone system as merely another particular computer application and not necessarily a specialty field unto itself. If the old-time telephone engineer fears that the computer types are taking over, he is probably right. So much for what computer technology might do for or to communications, depending on where you sit.

THE IMPACT OF COMMUNICATIONS UPON COMPUTERS

Using telephone lines modified to handle digital data, we are able to build an increasing number of geographically distributed time-shared computer systems. Many individual users are connected to a common computer data base. Examples of such systems include airline reservation systems for civilians and fancy display "command and control" systems for the military.

Simple record keeping, a mark of a highly developed economy, has been a prime area of development of these large computer file/communications systems where much of the routine clerical work is transferred to the computer with human interrogation of the system. As time moves on, the number of people who will be able to interrogate the system and the geographical distance between them and the machine will increase.

SOME INDIVIDUALLY USEFUL SYSTEMS

Today we see time-shared file systems used for insurance records, for checking automobile tags, to locate outstanding criminal warrants, and for credit check investigations (using drivers' license numbers) in cashing checks. The systems built to date pose no overt social problem. The information handled is not highly sensitive and access to it is generally limited.

THE TRAIL OF ARTIFACTS IN A CIVILIZED LIFE

As we pass through life, we leave a trail of records widely dispersed and generally inaccessible except with a great deal of effort and diligence.

We start with a duly recorded birth certificate. We leave behind hospital records and our pediatrician adds to our medical records. We are deductions on our parents' income tax. School is a place where we busily generate record upon record of our scholastic grades, our attendance, our IQ test records, our personality profile records, volumes galore. With automated teaching coming to the fore, we can expect better record keeping. The volume of data we will record per child may be expected to increase even more markedly ("in the best interests of the student"). Between terms we get our social security card and a job, and we start leaving behind us a long history of employment records. We reach age 18 and are entered upon the records of the Selective Service. We get a driver's license and, if we are lucky, we will be able to avoid having arrest and jail records. Most of us will apply for a marriage license, some of us will collect divorce decrees which will end in voluminous court records. We move from job to job in a mobile economy creating moving-company inventory records of our goods. Even as we move from place to place we leave behind short records of our airplane reservations and for some reason every hotel makes a ritual of acquiring and preserving the names and addresses of its guests for posterity.

This list is only a partial one. Play the game yourself

and think of all the records you leave as you go through life.

WHY SO MANY RECORDS?

One does not create records merely for the sake of creating records. But rather there is the implicit assumption that the records will be of some use some day. In order to be of use, there must be some means of interrogating the files to resurrect the information sought. Thus, we envision large families of systems, each individually useful. For example, an Internal Revenue Department investigator might wish to have immediate access to the tax returns of the associates of a man who is being audited to check for consistency of financial relationships.

A company may wish to have rapid access to its personnel files to know whether to give a good reference to a former employee.

A doctor may wish to trace the entire medical history of a patient to provide better input into a diagnostic computer.

The Veterans Administration may wish to examine a man's complete military record and *possible other* previous medical records to see whether the ailment claimed as being service-connected really is.

A lawyer for the defense of a man will wish to search for jail records, arrest records, and possibly credit records of *all* witnesses for the plaintiff.

Professional licensing boards may wish to delve into *any* records that may indicate the applicant lacks an unblemished character.

The military in filling extremely sensitive positions may even wish a record of all books borrowed by the prospective applicant to insure that his interests are wholesome and he possesses the proper political bias desired.

ACCESS TO THIS INFORMATION

Today one does not gather such information about the prospective examinee easily. If one went through the direct channels and asked most sources for their records about a person, he would most likely be told to go jump in a lake, if for no other reason than the information is not available—cheaply. Even if the information were a publicly available record, the investigator must be expected to spend a great deal of time and effort delving to discover pertinent data. Today, as through a practical matter, if one wishes to obtain much of this information about a person, he hires a private detective who charges a great deal of money and expends a great amount of time obtaining a little information available from a portion of these potential records. The price for a fishing expedition for information is high and most of the fish are inaccessible.

THE IMPENDING PROBLEM

So much for the pleasant past. Consider the following argument:

1. A multiplicity of large remote-access computer systems, if interconnected, can pose the danger of loss of the individual's right to privacy—as we know it today.
2. The composite information data base may be so large and so easily accessible that it would permit unscrupulous individuals to use this information for unlawful means.
3. Modern organized crime should be expected to have the financial resources and access to the skills necessary to acquire and misuse the information in some of the systems now being considered.
4. We are concerned not only with the creation of simple "automated blackmail machines" using this information, but with the added implication of the new "inferential relational retrieval" techniques now being developed. Such techniques, when fully refined, could draw chains of relationships from any person, organization, event, etc., to any other person, organization, or event.
5. Humans, by their day-to-day necessity of making decisions using totally inadequate evidence, are innately prone to jump to conclusions when presented with very thin chains of inferred relationships. For example, merely plastering a man's name on billboards will markedly change the outcome of an election, if the other candidate's name is not equally displayed.
6. The use of private detectives to unearth derogatory information on political candidates *and* their associates has become an increasingly prevalent feature of elections. This practice is expected to increase in the future.
7. The cost-per-unit-dirt mined by unautomated human garbage collectors can be cut by orders of magnitude once they obtain access to a set of wide-access information systems which we now see being developed. It is the sophisticated form of chain-relation blackmail that may be of most social concern. We generally pass through three stages of information storage development. First, we start by keeping manual records employing clerks. Next, we get rid of some of the clerks when we put all the records into a single central computer file with the readout controlled from a single point. The next step is the creation of remote interroga-

tion devices to interact with the file from a large number of points. The payoff for instant access is often high as it eliminates all delay to the file user.

8. This development of geographically widespread access systems requires the use of communications lines to connect the users into the computer. There is a widespread belief that somehow the communications network used will possess a God-given sanctuary to privacy, but "it ain't necessarily so . . ."

DIRECTIONS TOWARD A SOLUTION

1. Assume that not everyone is as honest and as trustworthy as ourselves—but is just as diabolically clever.

2. Appreciate that we will be increasingly dealing with complex and, hence, difficult-to-understand-all-the-details types of systems in the future.

3. Probably the only people who best understand the operation of each system will be computer design engineers who build the system in the first place.

4. Often the only time that the fundamental safeguards that we seek can be applied is at the time of the initial system design. "Software patch-ups" at a later date may generally be relatively ineffectual compared to good initial design—good design being defined as including an awareness of the existence and importance of the problem.

5. Do not expect help from the legal profession in lieu of good design. Even ignoring the social lag of the legislative/judicial procedure, the detailed subject matter verges on or beyond the limits of their comprehension.*

6. Laws and laws alone have been almost totally ineffectual in the growth of widespread electronic eavesdropping and wiretapping. At most, all the courts have accomplished is to prevent the police from using the same techniques available to the private detective or the criminal—or even casual readers of an electronics technician magazine.

7. While I have little faith that laws in themselves will *solve* the problem, laws could be helpful in two ways: (a) Laws outlawing certain practices will be of minor help in increasing the price of the act and making its commission less flagrant; and (b) laws can be written so that potentially weak systems cannot be built unless adequate safeguards are incorporated throughout for the protection of the information stored.

8. This last direction is to me viscerally unsatisfying as it carries with it a built-in loss of freedom. The thought of the creation of another governmental agency peering over one's shoulder contains the seeds of the possibility of bureaucratic decay and arbitrary conclusions based upon an incomplete understanding of complex problems.

9. Historically, government regulatory agencies start as highly effective bodies but lose momentum as the original personnel leave and their replacements come from the industry being regulated. (Where else are you going to get competent people who know the business?) The extreme competence that we need in a regulatory agency of this type is too rare a commodity.

10. If we are to avoid external regulation, then it behooves us computer-communication system designers to start working, or at least thinking, about the problem. We should take the initiative and the responsibility of building-in the needed safeguards *ourselves* before Big Brother is forced to do it himself and we are not too happy with the way he might want to do it.

11. Safeguards, whether they be screens around moving machinery or circuit breakers, cost money. Every design engineer is reluctant to add anything that costs money and buys little *visible* protection. But the writer believes that it is time to start regarding such added costs as *necessary* costs—a price to society for the privilege of building a potentially dangerous system.

12. This is not a new concept. We have, for example, been practicing this in the design of sewage systems and in electrical distribution systems for some time. But, historically, it has generally taken an epidemic to build a local sewage disposal system. It took a series of disastrous fires to get our electrical codes.

13. The national geographical extent of the new data systems, their impact, and their investment are so large that the price of a "retrofit" after the calamities occur may be a higher price than we need have paid if we had used some preplanning.

PROPOSED SPECIFIC SAFEGUARDS

To be more specific, what safeguards do I envision? Of course, we don't know all the answers yet. But, clearly, there are several steps that we should be considering, including:

1. Provision for minimal cryptographic type protection to all communications lines that carry potentially

*Eight months after this talk was presented, a special Subcommittee of the Committee on Government Operations headed by Representative Cornelius E. Gallagher looked into this problem. (These hearings, entitled "The Computer and the Invasion of Privacy", by a Subcommittee of the Commitee on Government Operations House of Representatives, Eighty-ninth Congress, Second Session, July 26, 27 and 28, 1966 are available from the U.S. Government Printing Office for $0.75.) Because of these hearings and the resulting interest and action, many of these words are now obsolete.

embarrassing data—not super-duper unbreakable cryptography—just some minimal, reversible, logical operations upon the data stream to make the eavesdropper's job so difficult that it isn't worth his time. The future holds the promise of such low-cost computer logic, so this may not be as expensive as it sounds.

2. Never store file data in the complete "clear." Perform some simple (but key controllable) operation on the data so that a simple access to storage will not dump stored data out into the clear.

3. Make *random external* auditing of file operating programs a standard practice to insure that no programmer has intentionally or inadvertently slipped in a "secret door" to permit a remote point access information to which he is not entitled by sending in a "password."

4. When the day comes when individual file systems are interconnected, let us have studied the problem sufficiently so that we can create sensible, precise ground rules on cross-system interrogation access.

5. Provide mechanisms to detect abnormal informational requests. That is, if a particular file is receiving an excessive number of inquiries or there is an unusual number of cross-file inquiries coming from one source, flag the request to a human operator.

6. Build in provisions to record the source of requests for information interrogations.

7. Audit information requests and inform authorities of suspected misuse of the system.

This list is open-ended, and it is hoped that more suggestions will be forthcoming. But, to serve as an example of the need for and type of safeguards we are talking about, to illustrate how such thinking can ameliorate the problem of loss of privacy, consider what we might do in the case of our present telephone system.

ONE EXAMPLE OF INCLUSION OF PROTECTIVE MEASURES: THE TELEPHONE SYSTEM

Today we are deluged with bogus telephone advertising, crank calls, bomb threats, false fire and police alarms. Obscene telephone calls, particularly to single women, have become so prevalent that it has been publicly suggested that female names be listed only as initials.

In Washington, the number of these calls has become so great that after much Congressional and press discussion, the penalty for making obscene calls was raised from $10 to $500. Of course, it is a rare event when a person making an obscene telephone call is caught, so the deterrent effect is almost nil. But an increased penalty hidden in a law book is the standard legal response to a basically technological/social problem. This writer would prefer to see *technology* which *created* this problem be required to provide more effective safeguards.

For example, each telephone (or at least those plagued with these calls) should have a button which when pressed bridges the call to a bank of recorders at the police station and a teletypewriter message with the name, address, and telephone number of the calling party transmitted to the nearest police car. It wouldn't take long to clean up the undesired callers.

If you were to make this suggestion today you would be told that this is not practical because it would be prohibitively expensive since this requirement did not exist when the original electromechanical telephone system was set up. This is true, but let us look at the emerging use of the all-electronic switching centers we have been talking about. It will be relatively easy now to add such an immediate track-back feature. Will we do it? I don't know. It would cost money and there are many reasons telephone companies would wish to avoid getting involved—but here is a perfect example of the social implication of the instrument which can violate our right to be left alone. The telephone can be designed (at a somewhat higher cost) to provide safeguards forming added protection to prevent it from being socially misused.

Clearly here is an example of the trade-off between dollars and the type of society we want. It will fall to the computer system engineers to make such decisions more and more often in the future.

What a wonderful opportunity awaits the computer engineer to exercise a new form of social responsibility. The advent of the new computer-communications technology need not be feared with trepidation as we approach 1984. Rather, we have in our power a force which, if properly tamed, can aid, not hinder, raising our personal right of privacy.

If we fail to exercise this unsought power that we computer engineers alone hold, the word "people" may become less a description of individual human beings living in an open society and more a mere collective noun.

It may seem a paradox, but an open society dictates a right-to-privacy among its members, and we will have thrust upon us much of the responsibility of preserving this right.