REMARKS ON THE QUESTION OF PRIVACY RAISED BY
THE AUTOMATION OF MENTAL HEALTH RECORDS

Paul Baran

April 1967
REMARKS ON THE QUESTION OF PRIVACY RAISED BY
THE AUTOMATION OF MENTAL HEALTH RECORDS

Paul Baran*

The RAND Corporation, Santa Monica, California

Do the physician's, the guidance counsellor's, and
the social worker's oaths of secrecy cease once you fill
out a record card or must you continue to protect your
personal records forever?

Assuming the answer is "yes," how are you to meet
this obligation in a future era of amoral computers, which
may or may not be discreet, serving both as servants and
middlemen?

I would like to discuss the implications of technolo-
gical changes anticipated to place you in a better
position to meet this future obligation when it is thrust
upon you.

If you have an old Social Security Card, read the
fine print. It says "For social security purposes only--
not to be used for identification." But it is?

When the Social Security Program was created over
thirty years ago, Congress was concerned that people might

*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 or
policy of any of its governmental or private research
sponsors. Papers are reproduced by The RAND Corporation
as a courtesy to members of its staff.

These remarks were invited for presentation before
the American Orthopsychiatric Association Workshop on
"The Invasion of Privacy," held in Washington, D.C., 21-
23 March 1967.
be branded with numbers. To meet this quaint objection, assurance was given that Social Security Numbers would never be used for any other purpose than identification of an individual's Social Security record. Today it is a rare personal record form, whether from a credit bureau or the Department of Internal Revenue, that does not ask for this information. As time moves on, original intent becomes modified for new needs in the name of efficiency.

Future changes in record keeping must be anticipated. This is not today's problem, but tomorrow's. Today, from the viewpoint of the data-processing man, we are still in the green-eye-shade clerk area of record keeping. Your sensitive records are probably kept, personally, in manual form under lock and key.

The impact of new technology has not yet been felt. But, it is coming. It is important to address the future and face the issues created as we seek to acquire the full benefits of the tremendous improvements possible in future automated information systems. These systems offer so many obvious advantages over manual record keeping in both cost and performance that their advent in this field may almost be guaranteed.

A summary of the major changes expected during the next decade or two in information automation will indicate the nature of possible problems.

1) Expect a rapid expansion in time-shared computer file systems. We will have centralized computers feeding a large number of remotely connected electric typewriter consoles such as those used today for making and checking
airline reservations. You store information into the computer and any portions of it can be retrieved and recombined in any manner you wish. The cost for this form of record keeping will be less than our present manual methods and access will be better.

2) This new computational and storage service will be supplied as a utility. You will buy computation and file storage like electricity—from a utility. You pay for the amount you use. Today, about 200 offices at The RAND Corporation have wall plugs that tie into a central computer. The researcher plugs in a portable typewriter-like device and is able to perform computations and resurrect old files and previous work.

3) The first generation of these information networks does not have adequate safeguards commensurate with your type of sensitive information.

4) There will be constant economic pressure inherent in the "utility" nature of these future information systems to effectively centralize them by interconnecting them together for reasons of both economy and performance. It is in this eventual fully interconnected era where underdesigned systems could become most embarrassing—and, in some instances, downright dangerous to our present day concepts of a right-to-privacy. But, at the same time, we must acknowledge that such interconnected systems will make large files readily accessible and permit better research using statistical sample sizes that would be economically infeasible today. Thus, we face a balance problem. How do we obtain the greatest benefit with the least danger?
Just as this new corpus of data may be searched for socially beneficial purposes, we must also consider the ease with which files could be illicitly searched for derogatory information. To be the most beneficial, the new file systems must allow inquiry from a large number of geographically scattered points. It should be realized, however, that the communications network (normally telephone wires) is wide open to tampering.

While the invasion-of-privacy problem has always been with us, its magnitude and complexion is changing. In the past, personal, sensitive information was kept in separate manual files. Specific individual permission was required any time an outsider wished information. The innate high cost and nuisance of delving through the files made inquiries by outsiders rare and tightly controlled.

There are major changes underway in the financing of medical care that can greatly broaden the access of formerly private doctor-patient information:

1) There is the growth of prepaid medical insurance plans.

2) Industry is playing an increasing role in selecting and financing medical, disability, and life insurance programs as a fringe benefit. Preventive medicine is now regarded as a proper concern of a corporate personnel department.

3) The population increase and its mobility requires more widespread transfer of medical records.

4) Increased specialization in medicine requires more complex and subdivided diagnostic centers.

5) More computer on-line patient monitoring in hospitals and automation of tests may be anticipated. These produce larger volumes of records.
6) More and more government is entering into medicine. Starting with the care of the indigent, then into financing the bulk of medical research, and now the care of the elderly through Medicare.

7) The payoff for better research by better use of existing personal records is becoming more widely appreciated.

A colleague at IBM once said that the most important historic event in the growth of this company was the advent of the Social Security Program in the thirties. The vast volume of data that had to be processed could not have been economically handled if it were not for the IBM punched-card machine. A new technology allowed a new social function to be performed.

As we look to the future and foresee greater integration of medical information systems, it may not be premature to think of the evolutionary development of such systems and the new problems they will create if adequate safeguards are not considered early and leaky systems prevented.

These problems are not new ones; only their magnitude will increase. But the change may be so great that a change of quantity may well mean a change in the quality of life.

I would like to recount a few stories which touch upon the weakness of present-day practices, and also one which shows how easy an automated system can be misused. This will give you an indication of the impending problems.

I need not tell you, as psychiatrists, counsellors, and social workers, that in many parts of our culture acquiring a venereal disease is regarded as a much lesser
offense than a visit to a psychiatrist. (In some groups, a venereal disease is a status symbol.) Normally, we like to feel that discussions with patients are private affairs. But with the growing number of company-sponsored group medical programs, some information is caused to be spread well beyond the privacy of your offices and used to the detriment of your clients.

For example, I knew a young career woman employed by a highly benevolent, stuffy, blue-chip company which gives all its key employees free annual medical examinations. During her routine physical examination she mentioned in passing that she had been undergoing psychoanalysis for several years. The woman refused to discuss the matter further but was badgered into accounting all the details because the examining physician insisted that it was impossible for him to complete his medical examination without this information. She was assured that the material would, of course, be kept private. Within two weeks, her immediate supervisor knew of the details and within three, all her co-workers.

I have heard other cases of this same thing occurring. For example, a major Eastern electronics company also provides mandatory physical examinations for its top executives. One very competent engineer was tentatively selected to head a new major program. The man's supervisor, reluctant to loose his most valuable asset, stated that the company's physician had told him that during the previous annual physical this man was found to have suffered a minor stroke. Upon checking with the company's legal staff, an opinion was given that if this man were allowed to take the new job
with its responsibilities and suffered a major heart attack, the company may be liable because it knew of this situation. I do not believe the man ever knew he was considered and that chances for advancement in his company are bounded. Here we have a case of a man being protected from himself by a benevolent corporation.

My own employer, The RAND Corporation, has a major medical plan which reimburses the employee for medical and prescription drug bills. However, it is necessary to obtain complete statements of all visits to physicians and all pharmaceutical bills, including prescription numbers. These are not filed with the insurance company, but rather with the corporation itself which in turn forwards the claims. Token pretense is made of information privacy by mailing the forms in sealed envelopes.

What are the rights of a recipient of a free good? Can one look the gift horse in the mouth without being accused of base ingratitude? Such growing medical plans could erode an individual's right-to-privacy from his own employer. Of course, one can be old fashioned and pay his own medical bills and throw away prepaid handouts. But let's consider that impoverished generation attending colleges and universities where medical care is prepaid and who cannot afford the luxury of purchasing privacy.

Although I must confess my age and admit being a member of a generation whose social morals appear to be slightly different than those at present, I can imagine situations where a young lady in the midst of a love affair may ask the student health office for contraceptives and may not know that a record of her request is carefully
recorded along with information about her grades, her religion, and her parents' economic situation. This may seem farfetched to you, knowing how carefully you preserve your records from the prying eye of the curious. But let us understand that we will live in a new world where pressures to automate records and make them more widely available will be great. The economic and social benefits that more complete records can provide are compelling reasons that can put one on the defensive. Further, we may like to believe that all we will do is to automate a manual procedure that is today satisfactorily secure. But as one acquainted with data processing, I would be inclined to move cautiously at this time in response to the inherent weaknesses and limitations of the technological design of some interconnected systems that I have seen being used and proposed today. For example, the remote location consoles of present time-sharing systems convey their information over telephone lines. A sophisticated curiosity seeker (or worse) can create signals to counterfeit a valid station and/or eavesdrop on the digital communication. The amount of sophistication and equipment required to play the game with some of our time-sharing systems should not be overestimated.

A few years ago, a freshman fascinated by a computer used at M.I.T. (and possibly in response to the reputation of M.I.T. freshmen to dream up pranks) programmed the computer to dial up every telephone extension in the school at the same time. The telephone switchboard operator saw her switchboard light up like a Christmas tree and acted
instinctively. Instead of waiting to answer any of the calls, she immediately called the fire department.

I hope I am not shouting fire when there is none, but many of my colleagues smell smoke. I personally would hate to tempt some freshman prankster to probe the college's computerized file to find tidbits of information about his friends.

According to a survey made by the American College Health Association, approximately 10 percent of the student health services already issue contraceptives to unmarried coeds. I am sure the prescription files which will contain this information may be expected to be computerized in the future. Can you imagine what our M.I.T. freshman might be able to do if he were able to interrogate these files? It would only take little more of the same imagination used in writing a program to ring all of the school's telephones. College freshmen have not always been known to exercise the highest degree of discretion.

It may seem bizarre to be thinking about such problems while we are still writing our records on sheets of 8½ x 11 paper to be stored in locked file cabinets. But to one in the computer field, it isn't too early to look forward to the new day when a sufficient amount of embarrassing information will end up in computers. You are not the only one to have this problem. Your records are merely some of the vast sets of records which could describe an individual to his possible disadvantage—a form of unwritten self-incrimination.

But, as the initial intention of the Social Security number evolved in the interest of efficiency, let us consider the consequences of a similar evolution that can take
place during the automation of some of your sensitive records. None of us are against progress. It is only the realization that as we acquire better statistical information tools and seek the advantages which better statistics about people will offer, we must be cautious of the implicit danger present in statistical systems misused to extract "intelligence data."