COMPUTERS IN SOCIETY'S FUTURE

W. Ware

August 1971

COMPUTERS IN SOCIETY'S FUTURE*

W. H. Ware

The Rand Corporation, Santa Monica, California

I very much appreciated the opportunity of speaking last year at
the Kingston Conference on Information and Personal Privacy.[†] I also
appreciate the opportunity to talk again about essentially the same
subject: computers in our society. I feel very much indebted to Canada
and its professional and learned societies for stimulating me twice in
slightly over a year to organize my thoughts on this matter. I proba-
bly would not have done so otherwise, given the normal press of business.
Also, I'm getting very fond of the idea of coming to Canada every spring-
time.

Today, I would like to describe briefly some of the reasons why the
computer has attained its present position relative to society and to
suggest ways in which it is already touching the life of each individual--
in some cases very extensively, sometimes for our good, sometimes with
ominous overtones. I want to indicate why I think there is a problem,
and if my discussion is persuasive, I will succeed in making you realize
that the problem is real--and is here now.

Let's begin by asking the question: Why is it that information
has become so increasingly important to society? Some of man's needs
increase roughly with his numbers. Food and clothing are obvious ex-
amples; approximately twice as many people will require twice as much
food. Other needs, too, increase with the number of societal units.
For example, as the number of families increase, so does the demand for

housing and household appliances. But the information needs of society
are multiplying much more rapidly. Take, for example, your own case:
How many credit cards do you have? insurance policy accounts? bank or
other financial accounts? magazine subscriptions? Do they number
fifteen? twenty-five? fifty? Each one of these represents an infor-
mation packet of some kind that has to be dealt with. Thus, any one of
us is responsible for increasing the information needs of society by a
few tenfold. Even if the need for information is proportional to the
number of individuals, it has a very large multiplicative factor. One
might even argue that information need is related to all the possible
interactions that can take place among societal units. If so, society's
information requirements are increasing according to some combinatorial
function. Whatever the case, society has created a vigorously expand-
ing consumer market for information.

I'd like to emphasize that society's size alone is sufficient to
drive the problem. You all know the classic statement about the tele-
phone company: If the telephone company had not invented automatic
switching and direct-distance dialing, then every woman would be re-
quired for a long-distance operator. Therefore, as industry supplies
society with services and products, it must also automate in order to
deal with the information that these services and products generate
and imply.

Consider the notion of an *information vector*, which is some quantity
of information that describes something about one of us personally,
about something we do or about some interaction between one of us and
another member of society. In this context, the number of information
vectors needed to control, to govern, and to describe society and its
members is increasing at a staggering rate. The number increases not
only with the size of society but also with the affluence of society;
as we acquire more and more disposable wealth, we want and do more
and more things.

Where does the computer fit into all of this and, especially, why
has the digital computer become so important? Because it's all we
have. It is the only technology that we possess that can store, re-
trieve, and manipulate data of any kind in very general ways. Let me

point out in this context that the communications art, for all its usefulness, for all its advanced state of technology, is simply a transportation system for information. Thus, while communications technology provides us with a means of moving information from place to place, it does not process it. It is computer technology that enables man to really manipulate and process information in either simple or involved ways, and to derive new information from the original. Digital computer technology provides us with the tool we need to accommodate our growing information requirements; it lets us do the things we have to do as a society, economically and efficiently. The result is that we are today experiencing an almost chaotic proliferation of systems that deal with information about people, and that exploit the computer to do it.

To put this in perspective, let me remind you that the computing business is only about twenty years old. In the 1950s, the industry really got its start, but the applications in that decade were largely to science, engineering, and technology. Then, in the 1960s, the applications turned to business data processing and we learned how to do payrolls, how to keep financial ledgers, and how to do inventory control; we learned how to run a business with a computer. Now, in the 1970s, we are turning to information systems in which the computer is dealing increasingly with natural language and with the semantics of language. The important point is that the information systems that surround us today are for the most part first-generation ones. While computing has been with us for a little over twenty years, we are just now implementing information systems, particularly those that touch each of us personally. So we really ought not to be surprised if these systems have faults. When anything of great complexity, and especially of novel design, is implemented for the first time, it is almost always troublesome and almost never ideal. Society, and the industry that supports society in this direction, are both still very much on the learning curve so far as understanding how to conceive, how to design, and how to implement such information systems.

Let's consider what these information systems are doing for us--and what they are doing to us. There are information systems essentially

for public safety. For example, there are systems that control street traffic; those that control air traffic; those that dispatch fire or other emergency equipment; and those that control or monitor an industry, perhaps a pipeline or a power-generating station. Although these systems have been devised for safety, often there is an economic motivation. There are information systems for public convenience. These systems process reservations for motels, hotels, automobiles, airplanes, etc. In Los Angeles, we have computing systems that sell tickets to public entertainment events. There are information systems for public service, such as those used for utilities billing, or to process magazine subscriptions. There are also systems that provide private service, such as those that serve the legal profession, or the medical profession, or the hospitals, or clinics.

The impact of such systems is felt by all of us, directly or indirectly. Obviously, for our discussion today, I have excluded computing as it relates to science, to technology, and to engineering, because in these areas the computer is really a tool and its impact on society is felt through its contribution to science, engineering, or technology; this is a kind of second-level effect.

Most of the computer information systems I've mentioned are largely benevolent, although they can be annoying at times. We generally accept the magazine subscription system because it helps to keep down subscription costs, but we become annoyed with it when the magazines are not delivered or the renewel notices are not processed. We are especially annoyed when a subscription list is sold to a second party for unsolicited mailing. Reservations systems for hotels, air travel, and such are generally quite benign, although occasionally they too can be annoying.

Crime information systems provide a good public service because they presumably lead to better, more complete, more efficient law enforcement. While they are hard on the criminal, they are generally beneficial to society, unless an innocent citizen inadvertently becomes involved, in which case there is potential danger to him. Computer systems in banking are taken pretty much for granted until they make a mistake by missing a deposit, or show an incorrect balance, or charge one person's check to another's account. Computer systems that serve

the tax collector can be annoying too, especially when we have tried
to cut a corner or have been a little careless with our arithmetic.
But I think one would argue that they are good for society because
they lead to more accurate, more equitable collection of taxes.

An information system that we believe to operate for our benefit
can be detrimental when the information is used maliciously or im-
properly. Let me give you some suggestions.* From immigration records,
for example: "So, that's what his name really used to be." Or, from
magazine records: "Reads a lot of left-to-center stuff, doesn't he?"
Or, from the hotel registration: "The records said Mr. and Mrs. but I
happen to know his wife was home that week." Or, from marriage records:
"So, it's the third marriage." Or, from college records: "He had to
take all those courses three times; slow learner; let's not hire him."
Thus, even systems that we automatically accept and willingly cooper-
ate with can work against us.

There are some information systems not generally open to the public
that can contain a great deal of information about any one of us.
The alarming fact is that as these information systems begin to exchange
data, more and more information will be accumulated. What are they?
Credit reference systems are examples and are probably the most maligned.
The two largest in the United States contain about 70 million individual
dossiers, and are growing by more than 7 million new dossiers annually.

The credit reference data bank was originally conceived and designed
to deal only with merchant credit and to serve only local clientele.
In that role it was not really too bad. The credit reference agencies,
however, have broadened their purview extensively; they have moved into all
kinds of ancillary activities. For example, credit data banks are now
used by employers for reference checks prior to employment and by in-
surance companies for insurance application checks. Some agencies sell
dossier information for mailing lists. Also, many credit reference
banks are now in the habit of freely exchanging data among themselves,
and so more and more of the information that we as individuals think
is in one place is in many places.

---

*See Paul Baran, *On the Engineer's Responsibility in Protecting
Privacy*, P-3829, The Rand Corporation, May 1968.

Another frightening aspect of the problem is that the information sources are not always accurate. Often, an individual's dossier in a credit reference bank will contain hearsay that was acquired from a neighbor or from an acquaintance; it may contain very personal information about the person's drinking habits or marital situation. Sometimes the credit bank fails to follow through on items of information, the classic example being that of the arrest record which finds its way into the dossier with no information on the subsequent disposition of the case. So there are real reasons why credit reference banks have become a serious problem of grave concern.

Some other information systems that are largely hidden are those that belong to government agencies, both state and federal. The United States Customs Bureau, for example, maintains a computerized suspect file of individuals that might illegally attempt to get into the country or cause harm. The United States Passport Agency has similar suspect files, consisting of about 250,000 entries. The United States Justice Department has a computer file of about 14,000 dossiers on militants and subversives. The United States National Crime Information Center has dossiers on about 2.5 million suspects, prisoners, and witnesses. There are voluminous files of military records; anyone who has ever been in the U.S. Military Service is in some file. There are corresponding U.S. Civil Service Commission files. Canada must have its version of some of these.

As an individual, I know of certain files that contain information about me. Since I pay income tax, I definitely know that I am in the Internal Revenue Service files. I know that I am also in the Social Security files, because one can't escape that system. I certainly must be in the Bureau of the Census files, because I'm obligated by law to respond to census questions.

My concern really increases when I realize that I might be in some files and not know it. The medical system is an example of what can happen. While it might only cause personal embarrassment if it were to leak the fact that a person has mild epilepsy controlled by drugs, a career could be damaged if it became known that a person has suicidal

tendency or that he has picked up six cases of venereal disease in four years. It is possible for medical information to find its way into a government data system, because a physician is required by law to report treatment for communicable disease or gunshot wounds. The individual might not know of this automatic forwarding of information.

I become especially concerned for my welfare when I contemplate how much information about me could be available, having been collected little by little from different sources. Each of us undoubtedly has something in his past that really ought to stay out of sight. To reveal it would serve no useful purpose for society and it could be detrimental to the individual. Yet the opportunities for the malicious misuse of personal information obviously become greater as dossiers become more comprehensive. This is bound to happen as more and more data banks begin to operate and to exchange information automatically. As members of society we must face three facts: We are surrounded by systems that deal with information about all of us; the information can be used for a variety of purposes; information systems might leak or be maliciously penetrated to reveal information to our disservice.

Now that we know what the problem is--and that we should be concerned about it--let us ask: Why does the problem exist?

First of all, today's systems are first-generation ones. They have been implemented once, and for the most part they have not been through major improvement cycles. So they are bound to be less than ideal. Second, there are technical problems. We only partly understand how to design systems that properly and adequately protect the information contained in them. We in the computing field *do* know how to provide some protective mechanisms, but they are not universally applied. In many cases the existing art is conveniently ignored or poorly applied. I would argue that we are not even doing as well as we know how to do. A further difficulty, technically, is that we don't know how to test a system so that it can be certified to have effective safeguards. Technologists don't know whether they have done an adequate job.

A third aspect of the problem is that there is not yet a legal framework to protect the individual, to fix liability in case the system leaks, or to provide for the award of damages. The Fair Credit Reporting Act

recently passed in the United States is a start, but, it is really only
one small corner of the problem.

In defense of the computer art, I would like to make this comment.
It is often alleged that the computer per se is the problem. In a sense,
this is true. While an equipment malfunction can lead to information
leakage, it is also true that the computer is often the scapegoat for
a much deeper problem. Unfortunately, our information systems are poorly
designed from an overall system point of view. Bad or even nonexistent
engineering practices during implementation magnify the fact. I really
think the technical people can do better, and that they should.

Is this overall situation a big problem or just a little one that
will shortly pass? I admit that it is hard to say. Certainly, inci-
dents of individual damage and examples of poor operational practices
come to light from time to time, but I've also found that people have
a way of not talking about them. I don't really know--and I don't
think anyone does--just how many examples go unreported. It is true
that one man in California was denied his insurance coverage because
the motor vehicle computer system erroneously charged him with auto
theft. It is also true that in the greater Washington area, some 175,000
people got arrest warrants automatically printed by a computer on
the basis of parking violations. All of us have experienced faulty
billing, and know how difficult it is to unscramble the mixup. If
someone has been personally affected by a computing error--lost a job,
or experienced a damaged reputation, or has been denied credit--it is
a very real problem to the individual. When it happens to the man down
the street, however, the problem seems remote. I like the way that
Professor Charles Wright, of the faculty of Yale's Law School, puts it:
"It seems a very terrible society, in the sense of being both frighten-
ing and terrifying, when information given to one man or agency becomes
available to anyone."

What can we do? We should not call a moratorium on people-oriented
data banks; it would serve little useful purpose and society would be
set back. Moreover, historically, mankind has advanced by living danger-
ously, trying things, and after the fact, learning how to control

what he has done. Perhaps that is the best way to do it--best because
we seemingly cannot foresee the consequences of new technologies that
we conceive. If we *were* that perceptive, we might not be sufficiently
adventuresome and thus might not progress as rapidly as we ought to.
So I think we should not panic and cry "let's hold everything until we
know what we are doing." There is technical work to be done, and this
is the responsibility largely of the computing industry and its tech-
nical people. Certain system design problems need to be understood so
that we can conceive overall systems with complete and adequate safe-
guards. Legal issues do need to be resolved. They will involve pro-
tective measures for the individual and means for fixing liability;
they may also involve regulation of operators of information systems.

Have I succeeded in presenting a convincing case? In a sense, it's
as though this discussion is taking place in the middle 1920s. We
are looking at a Model T chugging down the road and I am trying to con-
vince you that in some number of years the device will be responsible
for carpeting the countryside and the cities with acres and acres of
asphalt and concrete and will be dumping megatons of pollutants into
the atmosphere every year. I'm not sure that such an argument would
have been convincing in the 1920s; probably not. Maybe I can't make
an equally convincing argument today, but I would like to point out
that there is a difference between yesterday's automobile problem and
today's data-bank problem. We don't have fifty years to procrastinate
on today's problem. The pace of society vis-à-vis technology is far
too fast to allow for such a time lag. While the public-oriented data
banks that we're talking about are now only a few years old, my feeling
is that society has a maximum of five years or so in which to get on
top of the problem. Otherwise, I think that we will be faced with an
information industry that has developed and is operating without the
controls necessary to safeguard us either as individuals or as a society.
So, in my view at least, the problem is real, the urgency is great, and
we have to act.