COMPUTER TECHNOLOGY AND SURVEILLANCE

Paul Armer

June 1975

Center for Advanced Study in the Behavioral Sciences
202 Junipero Serra Boulevard, Stanford, California 94305

Computer Technology and Surveillance

Paul Armer*

Center for Advanced Study in the Behavioral Sciences

Stanford, California

Mr. Armer: First, I would like to say a bit about myself so that you can put my comments into context. I think of myself as a "computer-nik." I have been in the computer field since 1947, which was about the time that we began to realize the enormous potentialities of computers for processing information. From 1947 until 1968 I worked at the Rand Corporation, spending ten of those years as head of their computer science department. I am currently a Fellow at the Center for Advanced Study in the Behavioral Sciences, where I coordinate a National Science Foundation-sponsored "Program on Science, Technology and Society."

In 1962 I began to devote time to studying the social implications of information processing technology, and since 1971 that has been my major area of concern. Consequently, I am pleased to be here because the impact of information processing technology on privacy and on freedom has been a concern of mine for more than a decade. I feel that the possible uses of computers for surveillance may not yet be fully recognized.

*This testimony was given on June 23, 1975, at hearings held jointly by the Subcommittee on Constitutional Rights of the U.S. Senate Judiciary Committee and the Subcommittee on Science and Technology of the Senate Committee on Commerce.

This morning I want to talk about the state-of-the-art of computer technology--or, putting it somewhat more broadly, about information processing technology. I think that this is a most important sub-set of surveillance technology. I do not pretend to know very much about the technology of bugging and wiretapping, so I will not discuss it explicitly. However, I will be talking about the technology of microelectronics--bugging and wiretapping depend on that same technology.

People concerned with rapid change often find it useful to have a yardstick for measuring the amount of change. The concept of "an order of magnitude" is just such a yardstick. As you know, an order of magnitude is a "factor of ten." We can travel by foot at about 5 miles per hour, by automobile at something like 50 miles an hour, and by jet aircraft at about 500 miles per hour. Here we have 5, 50, and 500; each of these modes of transportation differs in speed from the previous one by a "factor of ten" or an "order of magnitude." (1) Thus, the last century has seen a change of two orders of magnitude in transportation speed. The capability of getting around at 50 miles per hour has profoundly affected our way of life. For example, it made the flight to the suburbs possible, and even influenced our culture. As we hear so often, jet travel has shrunk our world tremendously. With the context of two orders of magnitude change in a century before us, let's look at what has been happening with the electronic computer.

The speed of the electronic portion of computers has been increasing by an order of magnitude about every four or five years. During the last decade, the size of the electronics has decreased even faster than that--

computers are becoming incredibly small. Most importantly, the cost of raw computer power has declined by an order of magnitude every five to six years, and this trend looks like it will continue for at least another decade.

Computers are now being manufactured such that the entire processor fits on a single chip about an eighth of an inch on a side. To make the processor more useful you have to add another chip or two, or three, for memory and for communicating with the outside world. Systems of this kind can be purchased today for less than $100.

In my classes I often hold up such a device and point out to the students that 25 years ago that amount of computing power would have cost more than $1 million and would have occupied several large rooms.

Permit me to make another analogy to emphasize this point. It is estimated that the pyramid of Khufu at Giza in Egypt, built in 3000 B.C., required the labor of 100,000 men for 20 years. If the technology of pyramid building had experienced the same increases in speed and decreases in cost as microelectronics technology has over the last 25 years, a similar monument could be built by 20 men in a single year at a cost insignificant enough to make it reasonable as an outlet for many egos. One needs little imagination to picture how Washington, D.C. would look if this were indeed the case. (2)

We have all seen the impact on our society of an increase in the cost of energy by a factor of two or three. What kind of an impact could you expect from an increase, or reduction, of two or three orders of magnitude; that is, a factor of 100, or 1,000? I point out that our society runs on information as well as on energy.

Suppose I were able to predict that the cost of an automobile, or of housing, would decrease by a factor of 100 over the next decade? It is quite reasonable to predict that the cost of raw computer power will indeed decrease by a factor of 100 or more in that period of time.

There will be several microprocessors in every car; trucks will probably have one at each end of every axle; there will be one in most appliances, and there will be one pasted on the back of every typewriter. I am sure there are countless uses that we don't even dream of today.

Lest I leave you with the impression that information processing is about to become a free good, I must emphasize that I am talking about only the electronic portions of computers--there are many other activities associated with making use of a computer. There are mechanical devices for getting information into and out of computers; there are sensors which measure information such as a person's blood pressure or the acceleration of a truck and then feed the information into the computer. Another significant cost is the cost of programming the computer.

Now, the costs of all these other factors are not changing very rapidly, so, the total systems' cost is not going to zero; but the cost of the electronics, for all practical purposes, is going to zero.

Now, what does information processing technology have to do with surveillance? A great deal. However, to my knowledge very little information processing technology has been researched and developed as surveillance technology per se; rather, it has been developed with other motives in mind, like improving business data processing or guiding missiles or getting men to the moon. But surveillance is an information processing task just as much as a payroll application is. If you improve the efficiency of information processing technology for payrolls, you improve it for surveillance. Often systems that are put up for other reasons (as we shall see shortly) can also serve surveillance.

Before going to that, I want to talk about several areas of information processing technology which are of particular importance to surveillance. We have heard quite a bit about networks from Mr. Cooke this morning, due to the publicity given to them of late as though they represented a great new technological breakthrough.

The first networks consisted of many terminals connected to a single computer. Though there may have been earlier examples, I believe that American Airlines' first seat reservation system went into operation about 1952. It soon became clear that one could just as easily communicate from one computer to another as from a terminal to a computer.

Now, the most sophisticated computer network that I am aware of is the ARPANET, which was described this morning. It was put up by ARPA--beginning in 1968. The ideas behind the network had been known for at least five years--ARPA put them together in a system for the first time. As Mr. Cooke told you, the network consists of a number of computers (called "hosts"), communications lines, terminals, and devices called IMPs (for interface message processor). Since there are a number of dissimilar host computers in the network and an even greater variety of terminals, the IMPs must be capable of handling dissimilar host computers and terminals.

It has been said during the last month that "Setting up a computer network involving virtually any computer, government or private, is almost as easy as making a telephone call." (3) This statement is dead wrong. First of all, to get into a computer from a network, either the computer must be physically connected to the network, or the network must be able to establish a dial-up connection with the computer.

Most of the computers in operation today are not connected to any communication system. Of the few that are, most are connected to intra-company networks, using lines leased from a common carrier; and/or they may have telephone numbers which can be dialed by a terminal or by another computer. Even if two computers are connected to the same network, unless host-to-host protocols have been agreed to (and adhered to), no IMP will be able to transfer information from one computer to another.

Now, this is not to say that five government agencies couldn't agree on such protocols, and agree to inter-connect their computers, and then pass information back and forth. Mr. Cooke described just such a system when he discussed the COINS network earlier. But the notion that one computer could surreptitiously go around stealing information from any unsuspecting computer, government or private, is hogwash.

Five or ten years from now most computers will probably be attached to a network, or be reachable via a telephone number. And most will probably adhere to a standard protocol. But by then we should have been wise enough to develop safeguards that will make unwanted penetration from the outside difficult and expensive. Note that I didn't say "impossible."

Even if two computers are connected to the same network and adhere to a common protocol for exchanging messages, the problem of, say, collating together two files on individuals can still be quite difficult. Is Bill Jones the same as William E. Jones? If both records have the same address, it's probably a safe assumption, but if the addresses are different, you don't really know, for the two records may have been obtained at quite different times.

For this reason those who face the task of putting such files together would like to have a universal identifier; they usually suggest that we use the Social Security number for this universal identifier. Those who fear the results of the collation of several files into complete dossiers naturally oppose the use of any form of universal identifier. I mention this because I believe it is important that we understand the implications for privacy and surveillance before adopting a universal identifier or permitting the Social Security number to become a universal identifier.

I don't mean to imply that computers today are not penetrated by individuals with malevolent intent. One of the more publicized instances of computer crime involved penetration of a telephone company computer used for supplying equipment and spare parts needed by company employees. The penetrator would dial in, order large amounts of equipment, and have it delivered to a location from which he could subsequently remove it. Over time, he obtained equipment worth several hundred thousands of dollars.

On university campuses a favorite pastime of bright students is to attempt to penetrate the computer. And they succeed all the time.

For the above reasons I believe that those in charge of military security still (with only a few exceptions) will not permit the storage of classified material in a computer which can be accessed from the outside. Thus, if one has personal data files with sensitive information therein, they should be treated like classified material.

Let me say a bit more about security in computer systems. Security was recognized as a problem only recently. As a result there are practically no computers in use today that were designed and built with the security problem in mind. Security precautions that have been incorporated into computer systems are invariably only in the software, or in control of physical access to the computer and terminals. Software is indeed soft. Good security requires that both the hardware and software be designed with security in mind.

It is interesting that the sole exception to the above, that I am aware of, other than cryptographic devices, resulted from ARPA-supported research in the MULTICS project at MIT. ARPA has been a major source of support for research on computer security.

As you will soon see, I am greatly concerned with the application of information processing technology to surveillance. That being so, why have I defended networks? The answer is simple--I think they have been getting a bad rap.

I understand there is some sentiment for legislation forbidding the inter-connection of any government computers. I personally think that's throwing the baby out with the bathwater. If there is concern about the FBI computer being programmed to penetrate the Social Security computers, and the

Census Bureau computers, then treat the files of Social Security and the Census like classified information. That is, don't let them be accessible from the outside until the technology exists to satisfy those concerns necessary to safeguarding classified information. But don't generalize to all government computers.

Note that the FBI computer is already on a network. While I suspect that as much security was built into that system as could be reasonably purchased at the time, the chief source of leaks from those files is that tens of thousands of law enforcement personnel have a legitimate reason for access to the files. While the wholesale transfer of information may be difficult, individual files can be copied rather easily.

Let me briefly mention another area of research in information processing which, though being carried out for quite other reasons, is also related to surveillance. I refer to speech understanding, sometimes referred to as voice recognition. By this I don't mean the identification of the speaker as in voice prints, but rather the recognition by a computer of what words have been spoken, so they can be entered and stored in the computer just as though the words had been typed on a terminal connected to the computer.

One reason for wanting this capability is so that we can input information into a computer orally. The goals of research in this area today are not terribly ambitious, yet even so, they are elusive. The hope is to get the computer to be able to understand a few dozen words, spoken by a small number of cooperative people whose voice characteristics the computer knows in advance.

This technology is related to surveillance because a bug, or a tap, results in miles of tape-recordings, most of which is of no interest to the goals of the surveillance. Transcribing all that tape is expensive--just listening to it is expensive.

I do not mean by the above to suggest I believe that research in speech understanding should be stopped because it might be used in surveillance, though I am aware of computer scientists who have refused to work on such projects for exactly that reason. But, as speech understanding capability increases, we must recognize that surveillance capability does, too.

Before leaving this topic I should also observe that the surveillance situation is usually more difficult than recognizing a few words for computer input, because here the speakers are not trying to cooperate and their voice characteristics may not be known in advance.

Let me now turn to a new topic. Several times I have referred to situations where the technology under discussion was developed for reasons other than surveillance, but it happens that it is useful for surveillance purposes. As a prime example of this I want to talk about electronic funds transfer systems. I can't give you a detailed definition of an electronic funds transfer system (usually referred to as EFTS) because the system hasn't been built. Its final form will be an outcome of intensive competition, and also of government regulation. But the general form is reasonably clear. Terminals will exist in stores, hotels, restaurants, etc. (where they are referred to as point-of-sale terminals), and in financial institutions, including unattended terminals miles from the nearest office of the institution. In short, terminals will be at any location apt to have a large number of non-trivial financial transactions.

Let's look at one way it might work. Say you are about to buy a book. You present your card (sometimes called a "debit card," although National BankAmericard calls theirs an "asset card") to a clerk who puts it into a terminal which reads it and then calls up your bank. If you have enough money in your account, or if your bank is willing to grant you that much credit, the transaction is okayed; your account is debited; and a credit is dispatched from your bank to the book store's bank account.

The dimensions of the final form of EFTS which are of importance to its potential surveillance capability are such things as the percentage of the transactions recorded; the degree of centralization of the data; and the speed of information flow in the system.

Suppose for a minute all transactions over $10 must go through the system and that they are immediately debited to your account in your bank's computer. Thus the system not only collects and files a great deal of data about your financial transactions--and that means a great deal of data about your life--<u>but the system knows where you are every time you make such a transaction</u>.

Suppose that the rule for all transactions over $10 is not compulsory, but voluntary. And further suppose that you have gotten into the habit of using the system because, one, it is convenient; and two, it may be cheaper than other payment mechanisms. Now comes an instance in which you want privacy and decide to use cash. If you have to obtain the cash from the EFT system, that cash transaction will stand out like a sore thumb. The point here is that it's not enough just to have the option of using cash, the cash option must be used frequently or it becomes useless as a means for privacy.

To give you an idea of how powerful a surveillance system an EFTS would be, consider the following. In 1971 a group of experts in computers, communication, and surveillance was assembled and given the following task: Suppose you are advisors to the head of KBG, the Soviet Secret Police. Further, suppose that you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. Further, the system is not to be too obtrusive or obvious. What was the group's decision? It was to build an EFTS system. Not only would it handle all the financial accounting and provide the statistics crucial to a centrally planned economy; it was the best surveillance system we could imagine within the constraint that it not be obtrusive.

That exercise was almost four years ago, and it was only a two-day effort. I am sure we could add some bells and whistles to increase its effectiveness somewhat. But the fact remains that this group decided that if you wanted to build an unobtrusive system for surveillance, you couldn't do much better than an EFTS. (4)

Naturally, the EFTS proponents believe that laws could be written to prevent abuse of the system. I am less sanguine. I'm not concerned about the bankers invading my privacy or using the system for surveillance purposes; but I am afraid that EFTS system operators may be unable to resist pressures from government to let the EFTS be used for surveillance.

There are in existence today computer systems which could be used in exactly this way, although the number of financial transactions involved is comparatively small. What I have in mind here are the credit authorization systems of National BankAmericard, Master Charge, American Express, and various check authorization systems. All can have individual accounts flagged. If an individual tries to make a purchase, or tries to cash a check, the system is interrogated. If the account has a special flag the police (or whoever) can be notified where that individual is at that very instant. Check authorization systems are especially subject to such abuse because they depend on the police for information about bad check passers and for information on forgers for their computer data bases. I have no doubt that such systems have already been so abused.

Why should we be so concerned about surveillance? I don't think I can put it any better than Henry Goldberg did in a recent speech. "... 1984 is really a state of mind. If you are always tied to the consequences of your past activity, you will probably adopt a 'don't stick your neck out' attitude. This would create a pressure towards conformity, which would, in turn, lead to a society in which creativity would be an early victim and the democratic ideal of a citizenry with control over its own destiny would not flourish for long." (5)

In a recent speech Professor Philip B. Kurland pointed out that we will not celebrate the 200th anniversary of the U.S. Constitution until 1987, and that before we can do so, we must successfully get past 1984. He further said that if he were in charge of some Bicentennial celebration, he would require all participants to read Orwell's "1984" to show what the new nation was created to avoid. (6) I would extend the advice to those concerned about electronic funds transfer systems. And to "1984" I would add the recently published "The War against the Jews--1933 to 1945" (7), and Tom Houston's memo on domestic intelligence, which was issued to all American intelligence agencies in President Nixon's name on July 23, 1970. The book "1984" shows what might happen; the latter two documents detail actual events.

Thank you.

References

(1) Adapted from R. W. Hamming, "Intellectual Implications of the Computer Revolution," American Mathematics Monthly, Vol. 70, No. 1, Jan. 1963.

(2) Adapted from W. H. Davidow, unpublished paper presented at a conference of the Computer Society of the Institute of Electrical and Electronics Engineers, Inc., Washington, D.C., Sept. 10, 1974.

(3) W. Raspberry, Washington Post, June 18, 1975, quoting Ford Rowan of NBC News

(4) The Center for Strategic and International Studies, Georgetown University, Oct. 29-31, 1971.

(5) H. Goldberg, "Impact of the Less Cash, Less Check Society," presented at a meeting of the Computer and Business Equipment Manufacturers Association, May 28, 1975.

(6) P. H. Kurland, The Unlearned Lesson of Watergate," Wall Street Journal, June 17, 1975.

(7) L. S. Dawidowicz, The War Against the Jews--1933-1945; Holt, Rinehart and Winston, New York, 1975.