SECURITY, PRIVACY, AND NATIONAL VULNERABILITY

Willis H. Ware

April 1981

P-6628

The Rand Paper Series

Papers are issued by The Rand Corporation as a service to its professional staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of Rand's contracts or grants. Views expressed in a Paper are the author's own, and are not necessarily shared by Rand or its research sponsors.

The Rand Corporation
Santa Monica, California 90406

SECURITY, PRIVACY, AND NATIONAL VULNERABILITY*

For just a little while let us examine a bit of pertinent history. It seems to be a universal compulsion that practitioners of every new technology insist that it is really different, and that its differences imply that experiences and insights from other times and other places somehow will not work. We in the computer field have been as guilty as anyone for we used to say: "Dr. Physicist, or Mr. Engineer, or Chief Operating Executive, you could not possibly understand programming. Just tell your problem to the professional programmer and he will do it for you." It was one of the earliest ripoffs that the computer field foisted on its users. We also used to say: "Mr. Comptroller, you could not possibly budget and plan for EDP. Just give your computer professionals money and all will come out well." It was another ripoff that we perpetrated. We have said to the engineering manager: "You cannot possibly manage software. It is so different and it is an art-form. Moreover we cannot even promise that we will meet a budget or meet a schedule. Just send money and have faith."

To put it that way is rather stark but regrettably realistic. We now understand that the examples above, among others, are not absolutes. There is some truth in each of them but there is a lot of myth in all of them. Some mythology is being replaced by fact and understanding, but I can be anxious that much is still around. I think I see it turning up in new places that give me concern.

*Presented at Honeywell Computer Security and Privacy Symposium, April 7, 1981, at the Pointe Resort, Phoenix, Arizona.

What has really happened in the last 25 or 30 years? For one thing, top level managers have come to understand computers well enough that they do financially plan for and control them; the prior mythology is fortunately gone. For a second thing, a broad spectrum of people have learned to program. As a third example, we just spent the decade of the 70s learning how to manage software, and we now understand that a lot of well-known management techniques are truly valid. The necessary advance was to understand why and how software was different, and to adapt management approaches accordingly. Thus, we now appreciate that software differs from hardware in complexity; and in order to deal with it from the management level, we have invented the walk-throughs, detailed design reviews, structured approaches, and such. Much mythology from the early days of programming has evaporated.

My line of argument is to suggest that we stop claiming once and for all that computery is different in magic and mystical ways. Let us acknowledge that there are analogs from history and from other fields that we can profit from, and that such analogs do bring valid insights. Let us direct our attention to understanding in what detailed ways computers do introduce differences.

I think I see the "computer is different" mythology at work in the transborder data flow matter. I see no evidence that the European debate on the transborder data issue reflects any of the established insights and lessons about international conventions and agreements that control the flow of people, telegrams, mail, packages, and even electrical communications across national borders. The world has learned how to handle such things over a period of time, and presumably the lessons have some value. More to the point though, the transborder data flow issue started basically as a privacy matter, but now it is mixed up with economic competition, national vulnerability, sovereignty, cultural infringements, and assorted other things. I submit that a debate which started in the belief that computers introduced radically new aspects to the passage of data across national borders has now created a potpourri that has become difficult to unscramble and to deal with. It would appear that the European community is busily creating new regulations on data flow just when this country is trying to minimize federal regulatory constraints. The decade of the 80s is likely to be a trying time for companies that have to deal internationally with data matters.

In the context of examining with care how computer-created issues differ, let us look at the national vulnerability issue. Let us identify in what ways it might be truly different and suggest what might be available to deal with such differences. It is no secret that the world has made an irrevocable commitment to computer technology; likewise, it is very clear that there is no way back. We will never again run the world with papers, pencils, tub files, and people wearing green eyeshades. We must accept without reservation that the commitment is made and we must accept whatever consequences might arise. We will have to live with them and learn how to deal with them.

The commitment to computers has not been a planned event; it came upon the world gradually. Computer technology came along at just the time when the world was growing rapidly in complexity and in affluence; and it filled an urgent need to keep records, to handle data, to do intricate planning, and much else. Moreover, it is readily adaptable to fulfill a broad spectrum of needs. There is some parallel I think with the use of oil as an energy source. When oil was discovered in Pennsylvania, it came along at just the time to subsequently facilitate the growth of an automobile industry that would soon emerge because it--oil--provided energy in a convenient, transportable, and readily usable form.

What I see now taking place in the transborder area and in other issues connected with computer technology is that we are struggling with the consequences of the wholesale commitment to computer technology, just exactly as we are struggling with the consequences of a wholesale commitment to oil as an energy source. My frame of mind though is to search for useful parallels in trying to understand things which inevitably arise from the steadily increasing use of information. In that context let me try to structure the dimensions of societal vulnerability.

There are some dimensions of vulnerability that are not pertinent to deal with at this conference because they are tangential; for example, the legal vulnerability of a company that used some computer package to design a public structure that subsequently failed and caused death and suffering; or the vulnerability of a company whose corporate life depends on the data in a computer system but catastrophe strikes. On the other hand, there is a personal vulnerability of concern to the symposium because each of us is susceptible to misuse of data in recordkeeping activities, whether the misuse of data or the subversion of the recordkeeping activity is in the private sector or in government. Recordkeeping about people is the essence of privacy.

From other discussion you already know of privacy activities here and abroad. You know of the Federal Privacy Act, the Fair Credit Billing Act, the Fair Credit Reporting Act, and of the many European privacy acts as well as many state acts. In spite of so much activity, the matter is not fully resolved because there are aspects of privacy yet to emerge. For example, there are pockets of data that will have a privacy overtone, but it is not clear what we should do about them. Recently, an item in the *Los Angeles Times* discussed the issue of a law suit threatened by the Moral Majority against the librarian of the State of Washington. The Moral Majority has objected to a 21-minute movie entitled *Achieving Sexual Maturity*, and it seeks the list of borrowers of the film so they could be approached and their views influenced. The librarian has resisted on the grounds that it is accepted library policy not to give out information about borrowers.

However, the issue is uneven. Libraries in some states do have such a policy, but libraries in other states do not. Furthermore, it is not clear how libraries in private corporations might feel about the matter. Here is an example of an aggregate of data about people that is unprotected by law. Perhaps we ought to do something about it, yet it is not clear that who-borrowed-what deserves special legislation. There must be many pockets of data of similar nature that are potentially harmful to individuals, probably do not deserve specific legal action, but somehow need protection. In principle, we need to build a general umbrella under which such diverse things can be protected as each materializes.

Pockets of data are bound to emerge in electronic fund transfer systems as they develop. They are bound to emerge in electronic mail as the U.S. Postal Service and private industry both move forward in the area. They are bound to emerge in point-of-sale systems as these become more and more popular. I have come to call such miscellaneous aggregates of information about people "data puddles" because they exist for short periods of time just to make some computer-based system work, and then dry up and go away. They are unlike data files which have an extended life; so to speak they are short-time or limited-life files.

The question is: What do we do about them? Do we create special law for every one of them as it emerges? Do we create some general purpose law which somehow throws a blanket over all of them? Or can we count on case law or organizational policy to take care of it? It is a latent issue that is bound to come upon us in the 80s, plus a potpourri of matters revolving around microcomputers.

To be sure, there is both corporate vulnerability and personal vulnerability, but there is also national vulnerability. A country is vulnerable also and it comes in two parts. One aspect of national vulnerability is what happens if computerized services are denied to the country or to some major industrial segment within the country. The other one is what happens if computerized systems are used deliberately for national subversion or manipulation. It is not a subject that has been very well developed, but I can offer you some provisional thoughts.

The only study that I know of comes from Sweden, which happens also to be the first country to have had a privacy act. We will come back to the so-called SARK report in a moment, but consider first the denial issue. What would happen if computer systems were not available to their users? It does not take much imagination to conceive the consequences. Suppose airline reservation systems shut down for twenty-four hours; or suppose the computerized system behind VISA or Master Charge stops for the workday hours of a week or so; or suppose the computerized handling of bank checks were interrupted for a few days. It is easy to imagine the consequences of such events, but computer security, or perhaps the better phrase computer defense, is intended to avoid such denial difficulty. Presumably, thoughtful and concerned institutions of business and government do think about such things and will design their defense safeguards appropriately.

The SARK* report from Sweden raises a number of issues. The full text of the report is not available yet in English; moreover, it is not clear whether the translation is a summary of the report or a summary by a translator who read the report. In any event, a number of very important issues are raised, and the question is: What can we do about them with the technology on hand and with our insights from having run the world for a few thousand years? At the same time we should be cautious about the pretense that we have something new on our hands that needs or will require wholly new inventions.

One issue of concern raised by SARK--and one can appreciate that it is a real one in Europe--is that of communication circuits passing through many countries. En route the communication circuits are of

*[*The Vulnerability of the Computerized Society*. A report by a Swedish Government Committee, Ministry of Defence, Sweden, December 1979. Translated by John Hogg, LiberTryck, Stockholm, Sweden, 1979. (ISBN91-38-05356-X)

course controlled by various countries, and therefore the country originating the data has a vulnerability. The Satellite Business Systems company has a neat answer to that. It will offer satellite communication paths from one rooftop to another rooftop; moreover, for a fee the traffic will be encrypted. Thus, such circuits are protected communications outside the purview of other countries, and moreover do not depend on the telephone or telegraph structure of a particular country. At the moment, SBS offers services only in the United States; but if international arrangements can be managed, there is extant technology to avoid one vulnerability that SARK raises.

A second one is also a peculiarly European issue; namely, data bases that are sensitive and might fall into the hands of a future enemy. European countries have had such a concern historically but encryption is a unique and available answer to the difficulty. Simply encrypt sensitive data bases, and if one is threatened or at risk of capture, it is a simple matter to destroy the key. In fact, it is much easier to do so than to destroy the physical data base itself. It is not a novel problem; there is at least one way to protect a sensitive data base if deemed necessary.

Another issue that SARK raises is the vulnerability of individual computing centers. We simply need to notice the technology of less expensive and smaller computers. One can proliferate them everywhere and hence offset the vulnerability of a centralized installation.

Turn now to the question of manipulation of some data system by a foreign country. The intent would be to create upsets, havoc, or perhaps orchestrate a takeover of some kind. I offer you the following thought which is easiest to discuss by example. The FBI operates a National Crime Information Center that maintains a national catalog of stolen goods and cars plus miscellaneous other things; the data are furnished from state level. The FBI has not been successful in getting so-called computerized criminal histories into the NCIC because states have resisted, partly on the grounds that they do not want the federal government to have so much information, but partly on the grounds that criminal histories are subject to different laws in different states.

There is a technical solution but it has been obscured in congressional debate because surrogate issues have dominated discussion. The idea is to network everybody together and to assign to each state an obligation to watch two or three others. Thus, there would be a collective awareness of what is going on in the network; it would take a massive collusion in such an arrangement for one party to misbehave and to aggregate more data than he is supposed to have or to surreptitiously seek unauthorized data. Presumably everybody would watch the FBI; and with fifty watchdogs peering over its shoulder, it is very unlikely that anything inappropriate would occur.

In this regard, I submit that there are technological possibilities at network levels for security safeguards that have not been examined. We tend to think of computer security and computer defense from the centralized system point of view and simply extrapolate the concepts to a network. We ought to look as well from the other view because there are kinds of safeguards that can be built into networks--I have just suggested one--that cannot be implemented in isolated stand-alone systems.

Thus, the risk suggested in some discussions that computer systems of a country are vulnerable to takeover or to manipulation does have at least one solution which modern technology can make feasible. We can create international networks that collectively can watch for evidence of wrongdoing. I would suggest again that we do not have a wholly new problem. If we will simply look around us and see what is already known about analogous situations, we can find insights for problems that are thought to be overwhelmingly difficult.

In another dimension, the SARK report stresses the difficulty of spare parts for computers, and it points out the dependence of Sweden on U.S. vendors for them. It is not a new issue either. Any country that buys weapons from elsewhere has the spare parts problem, and everyone knows what to do about it. Typically, one buys ten years' worth of spare parts along with the weapon. Sweden could avoid its vulnerability in this direction with money.

The United States as a country has just the same problem, but it is called the strategic materials problem. For example, if certain countries of Africa were to be seriously disrupted, our supply of cobalt, chromium, and manganese would decline sharply, but the United States attempts to deal with the matter by stockpiling such strategic materials. There already is a major dependence among countries of the world for the goods of commerce and for strategic materials, and countries have accommodated it. They either stockpile items considered to be strategic and critical, or perhaps alternate materials are developed, or trade agreements are forged, or treaties negotiated. Spare parts is not a new issue; neither is the vulnerability of a country to something which lies outside its borders.

One vulnerability in a network is the risk that a transaction will be bogus. It is a network-level vulnerability if somebody does something which is not a legal or legitimate transaction. How does one protect against it? I observe that there is technology that can deal with it; it is called public key cryptography. Without getting into technical details, it provides a technique for safely transmitting authenticated digital signals so that one can really be sure who-is-talking-to-whom at both ends. Moreover, one can transmit authenticating digital signals over the telephone network by simply using touchtone pads as an input mechanism. There is ample technology if one needs to avoid such a risk.

Why haven't we done things that are clearly within the technical art? Partly it is the inertia of organizational structures; partly it is the head-in-the-sand typically American attitude that "Oh, it can't happen to me." To illustrate, suppose the bankers of the world got concerned about the risk that somebody would disturb the international financial structure by manipulating data bases surreptitiously. One answer would be to net all the bankers of the world together in the same spirit as the FBI-NCIC example mentioned before. The whole banking world would be watching the whole banking world, and it would be unlikely that any unauthorized difficulty could arise. So to speak, there would be a collective community awareness of what is happening.

Can you imagine though what it would take to get the bankers of the world to get organized in such a way? It would be an almost insurmountable problem from the organizational, jurisdictional, and political point of view, but the technical issues are nearly trivial.

The bottom line to this discussion is straightforward. Computer technology is not a wholly new experience for the world nor are the aspects it emphasizes totally new. New dimensions of the computer's effect have to be identified, noticed, and dealt with but we do not start completely from scratch. We must not expend our time, our energy, and our intellectual capital--which is always in short supply--redoing what does not have to be done. To do so will cause unnecessary travail; it will divert our attention from the central issue; it will introduce surrogate issues that act to obscure the real ones. We must pay attention lest we dissipate too much energy addressing problems whose solution may be before us and even be familiar, but we simply have not related the computer version to existing experience and insights. Instead, we must concentrate on genuinely new dimensions which we can identify in many cases and deal with them appropriately.

A nontrivial problem in moving ahead on some of these matters is the Congress of the United States. I expect it to be true in the electronic fund matter; I know it will be true in the electronic mail matter. Unfortunately, Congress tends to become immersed in surrogate questions and to miss the real issues; the NCIC-FBI debate was a classic. The real issue in it was an information use one: Who may have access to what computerized criminal histories and for what purpose? It is the central theme, but the issues that the Congress debated were those of mainframes, system architectures, and implementation details that clearly obscured the pivotal issue. An analogous thing is going to come up in EFT. A proper argument about the role of the Federal Reserve Board will arise; but an equally important privacy concern about data-on-people in EFT networks may never get addressed. Who shall have access to such data, for what purposes, and what will its legal status be? The very same issue will arise regarding electronic mail service. The debate is likely to focus on the position of the United States Postal Service versus private industry. What service should each be allowed to offer? What competition shall be allowed? We may never discuss a pivotal issue of protecting both the content of electronic mail and the sender-addressee records from inappropriate access and use by third parties, especially exploitation by law enforcement and other investigative agencies.

My intent today has been to leave thoughts, ideas, and suggestions with you and to indicate where I stand in my thinking about such matters. I hope that you do have new insights into the many dimensions of vulnerability that will inexorably arise and are associated with extensive use of computers and communication technology. I hope you will keep them in mind as you think toward the future, as you perform in your professional responsibility, and as you participate in a democratic style of government.