AD-A095 401 RAND CORP SANTA MONICA CA F/G 9/2
SECURITY AND PRIVACY IN THE 80S,(U)
MAY 80 W H WARE
UNCLASSIFIED RAND/P-6492 NL

1 OF 1

END
DATE
FILMED
3-81
DTIC

LEVEL II

AD A095401

SECURITY AND PRIVACY IN THE 80s

Willis H. Ware

FEB 24 1981

May 1980

RAND/P-6492

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

P-6492

DDC FILE COPY

81 2 18 014

SECURITY AND PRIVACY IN THE 80s [1]

I'm pleased to have this chance to chat with you about my perceptions of where the future lies. Let's first briefly review to see where things stand on privacy and security. Security, as you remember, publicly surfaced for the first time in 1967; except for a few defense installations, progress was very slow into the 70s. Then there were a few fires, a few bombings, and a few sprinkler systems deluged computers; the commercial world began to worry. Realization developed that computer systems are central to the well-being of institutions, and suddenly the lock-and-key, fire, and personnel specialists became the core of computer security. The commercial world did move responsively to secure installations, to remove observation windows, to control entrance to computing centers, to control movement of tapes and discs, to screen personnel, and so on. In the large, computer security in the early 70s was mostly the physical protection aspect, with a light touch of personnel and administrative attention.

We came through the 70s with gradual progress, but little attention to access-controlling software--with one exception. A few places did pursue research in software at a modest level of effort through federal funding. Security software is the tough part of computer security and commercial vendors are now having to face the issue. There is a so-called "DOD Comp[illegible] Security Initiative" for trusted computer systems--the new phr se for systems with security

[1] Presented at Honeywell's Sixth National Computer Security and Privacy Symposium, Pointe Resort, Phoenix, Arizona, April 15, 1980.

Accession For
GRA&I
By
Distri
Avail
Spe

safeguards. It is expected to produce prototypical, kernelized operating systems for two classes of machines, neither of which regrettably are Honeywell ones.

The federal government has a tough job ahead and it ought to be highlighted. It is a task for which the best minds of the country have very little experience, few insights, and only rudimentary tools. The operating-system-software kernel must be certified to establish that it is what it is claimed to be. We must establish that the software does what it is supposed to do and hopefully also, that it does not do what it is not supposed to do. Thus, one is expected to prove the positive as well as prove the negative--a difficult job as one knows intuitively.

From the point of view of the federal government, it is a particularly agonizing situation because access-controlling software when produced is likely to be used to protect official state secrets; immediately one must ask "Does such software itself have to be classified and protected as classified information?" If the answer is yes, it is a very uncomfortable scene because civil government is now left without an essential capability. Obviously one would hope, and even desire, that software would not have to be classified; but at this juncture, we simply do not know. A similar agonizing situation exists for commercial vendors as well, and hopefully it will be perceived by them.

Suppose a vendor markets a software product that happens to have loopholes that permit penetration. While Gimbels has always advertised that "it should not tell Macys," suppose Macys finds out how to penetrate Gimbels' computers. Where does the vendor stand with

respect to liability, with respect to marketability and creditability? What is his position? My intuition tells me that even in the commercial world, access-controlling software somehow will have to have parameters that are unique to the installation and are, so to speak, secret to it. Moreover, software will have to be such that the parameters which are private to the installation cannot be penetrated by probing backward through it. It is not an easy job and I would hope that Honeywell and other vendors attend to it with care.

Now, what about privacy? You recall that it surfaced in the early 70s. You know that the original study effort at the federal level was the so-called HEW Committee, which produced a report in 1973, which became the intellectual foundation for the Privacy Act of 1974, which in turn created the Privacy Protection Study Commission, which in turn created its own set of reports. Since the latter work, the action has been sluggish, but the Administration now has its act together. A few bills are languishing in Congress but I would guess that things will stay largely static because privacy is not a vividly important issue to most people. In particular, privacy has trouble competing with issues such as oil, energy, and foreign policy.

It is regrettable that little action is likely to occur on the privacy front soon because present careful attention to privacy, in my view, is an essential ingredient to laying the foundation for a better and a safer future. Nonetheless we are not attending it; so we may have to recover the situation from behind, which is always tougher. In both privacy and security, we have come a long way but there is yet a long way to go.

Let me now suggest some things that might come up in the years ahead; in part they are extrapolations of the past but at the same

time they have somewhat different directions. It is easiest for me to speak to the new thoughts by example; let me pick the FBI's National Crime Information Center because it is one that I happen to have been thinking about recently.

The NCIC as it exists today reflects system-architectural decisions and technical choices of about fifteen years ago. The present network is what a communicator would call a star network, with the computer center at Washington and all participating states having appropriate links to it. For stolen items, which is what it was originally created for, the scheme works well; but when the FBI proposed to add what are called computerized criminal histories (CCHs), things disintegrated swiftly. It happens that criminal histories are subject to diverse state laws. In particular, states have quite different public records acts or freedom of information acts, and several have privacy acts which differ from one another. There also may be other legal restrictions on the use of criminal histories such as with whom they may be shared.

Thus, states are not enthusiastic about the idea of depositing their criminal histories in one place at Washington because state law may be inadvertently violated--an uncomfortable position. Moreover, there is a federal-state interface issue as well; states are concerned lest the "feds" have everything. Generally speaking, the states have become very reluctant and many have withdrawn from participating. Cost is important too, but the fundamental issues are beneath. In an effort to move forward, the FBI has offered to run a message switch and connect such states as have traffic to exchange. Any technical

person knows how easy it is to monitor traffic, and copy whatever might be of interest. Thus, states are still squeamish of such an arrangement.

Meanwhile in Congress the debate that one hears is in terms of mainframes, of communication controllers, or in terms of message switches; such technical points are not the issue at all. The debate in Congress has been a surrogate for the real issues which are basically information-use ones. To me, the central question of the NCIC/CCH is: "What uses do we as the United States society accept or permit for criminally related histories? Who do we wish to have them? How much may any one have? For what uses may they be used?" It is an information-use issue, but we have not held such a debate. Until we do, and Congress is probably the place where it must be done, Congressional attention will continue to focus on inappropriate substitute issues.

I submit, as an item for the future, that there is a latent privacy issue but different from classical privacy. The latter has been an information-use one too, but focused on the individual and his position vis-a-vis a recordkeeping organization. I now suggest that there is a corresponding privacy issue for society at large--for all individuals collectively--but in the context of some body of information. It is a matter that we as a country will have to learn to deal with but we have not yet; the NCIC/CCH is a clear example of the issue.

There are two instances that have come to mind in which we have attended the matter properly but did not know at the time that we were. So far as I can discern, census data can be used for just about

everything and anything provided no individual can be identified. So long as data is satisfactorily aggregated, census data is freely available to anybody that wishes it and can afford it. The position seems to be the result of first, a legal stipulation that census data is confidential plus, second, a plethora of administrative decisions by the Bureau of Census. There is a more recent and somewhat sharper case, vis-a-vis tax information; the Tax Reform Act of 1976 is quite explicit. The Act says very pointedly that such information is confidential and will be used only for tax administration. It may be shared with states, but only under carefully prescribed circumstances and then only to tax authorities in the state. The IRS oversees the states and makes sure that conditions are met. Tax information is also available for specified other things. While Congress has delineated usage for tax information, there are other bodies of information needing attention--criminal justice for one. In the two examples noted, it was neither thought of nor phrased as a societal privacy issue; we can be grateful for our good fortune.

How about something new in security? Let's continue with the NCIC/CCH criminal history example. What one clearly would like is to architect the system so that any state can communicate with any other state as their mutual rules will permit, but at the same time minimize--or hopefully completely prevent--the risk that any one state or the federal FBI could accumulate an inappropriate amount of criminal history. Let me suggest one response to such a a design goal.

Imagine that we construct a network in the spirit of the ARPAnet; all the states would be netted together and the federal government

would be a member like anybody else. In particular, it would have no special privileges. There are several ways the query matter could be handled but, for the sake of argument, let's imagine that there is an "ask the network" feature. A state-originated query automatically would fan out across the network to all participants and any who can respond would speak up. It is not an impossible job, and there are research efforts to that direction already; it is within the state of the art to do. In such a system configuration, it would be easy to arrange for one or, if you like, two, or if you prefer, all states to monitor traffic requests by the FBI and to monitor one another. With such collective oversight, it would take massive collusion for any one entrant on the network to surreptitiously acquire and accumulate an inappropriate amount of data. It would take equally extensive collusion for someone to behave improperly and remain undetected.

The issue in the example is really an access-control one, but at a more global level than commonly discussed. Usually we talk about access control in the context of a computer system--it may have several processors in it--but a computer system that is typically in one place or within a confined geographical place with many users hooked to it. Importantly, notice that the user community in the usual circumstance is typically under the same jurisdiction, or responsive to the same line of authority. The point that I want to make is that we have not yet considered security safeguards in the context of a distributed network arrangement, especially one in which the participants are in separate legal jurisdictions as the fifty states are. In my example, each member becomes obligated to watch everybody else and become part of the operational security controls as

a condition of being in the network. In another sense, we are really addressing a system-wide audit trail feature.

The operative observation is that issues of the kind raised by nationwide network systems, especially when run by a federal agency, can be facilitated by appropriate network architectures and procedures. I would intuit that issues of such kind will find their way into computer security matters in the 80s because it provides a new opportunity to accommodate very awkward problems.

Since it has become a matter of floor discussion today, I want to comment on Senate bill S-240; I want to provide a different point of view than has been expressed. First let's stipulate several things. There is absolutely no question but that our computer-based record systems are vulnerable--no question whatsoever. Likewise there is absolutely no question that computers have been exploited in many ways for criminal purposes. They have also become interesting targets for criminal acts; that's clear too. It is also evident that computers introduce many new dimensions with respect to prosecuting a case. In this regard, I think it is important we all recognize that the Parker-Nycum work at Stanford has been extremely valuable in focussing attention on the whole issue of computer abuse, in keeping it alive through a long gestation period, and in raising everyone's consciousness about it. Their work has been an enormous service to the country.

In my view, the evidence and incidents to date do clearly add up to a case for more and better and comprehensive security controls; but I am not yet convinced that there is a case for new legislation. The fact that we need better security controls to offset the undesired

things which we all agree are taking place, does not automatically justify legislation. Even if we become convinced that legislation is warranted, it is not clear what kind we need. There are about a dozen states that have some kind of computer-crime bill. Many of them follow federal draft legislation, but at least one (Florida) shows considerable insight to the situation plus ingenuity on the part of the legislators. As I look back on history, I note that the earlier S-1766 bill of Senator Ribicoff is generally perceived as politically motivated; moreover, it was badly structured. Now we have the much improved version known as Senate bill S-240.

I don't want to take a position on the appropriateness of such legislation, but I will express my personal conviction that our homework at the federal level has not yet been done. We have not delineated how the computer makes crime different; we simply feel that it does. Clearly, scale factor is one aspect. If one commits crime with a computer rather than manually, whatever is done is almost certainly many-fold larger. Maybe that is important from the standpoint of law and prosecution, but we do not know; we have not examined the situation analyticaly.

We have not yet determined how to look at a computer in the light of criminal activities and in light of legislation to counter undesirable acts. Do we think about it as a better and larger file cabinet? If so, what's different about penetrating a computer system vis-a-vis prying open a file drawer? Do we think about it like a gun which obviously has significantly more power to inflict bodily harm? If that is the way to regard it, then what are the dimensions in which computers have an analogous property? Then let us target legislation

against them. Or do we think about a computer as just another mechanism for maintaining records? If that is the way we should think about it, is there any difference at all in regard to criminal activity? I submit that these are issues that have not been examined. For the most part they are issues to which an answer has been assumed: "Yes, the computer is different in some mysterious way and the unspecified difference is demanding of a legislative response."

I want to argue that it is important for the country to understand such things because from understanding will come the clues needed to guide new legislation. In my view the homework has yet to be done. For that reason, I would hope that Congress does not pass S-240. On the other hand, S-240 has had a very desirable effect; it has raised the awareness of the law enforcement community which is getting its act together--obviously a good response. Having catalyzed action though, let's now put the catalyst aside, stand back and ask: "What is it that we really need to support the law enforcement community in a new area of criminal activity?"

If Congress does not pass S-240, and it has been estimated that it has a fifty-fifty chance, then I will assert that an essential item of the 80s is to get our homework done. We must structure the problem intellectually; we must understand the dimensions of the new thing that is upon us. We must perceive the implications of such dimensions for criminal acts or, for that matter, for other undesirable social acts which may be civil rather than criminal.

As professionals in the data processing field, we each should know what's going on. I would urge that you get your personal homework done; I want to emphasize it very strongly. If S-240 passes,

you could inadvertently find yourself on the receiving end of a federal felony indictment with significant penalties--a long jail term and a large fine. Such consequences are hardly inconsequential for a minor action such as drawing Snoopy or printing a calendar. It is true that drafters of the bill have tried to sort such things out in its language; it is also true that the legal view would say: "leave such details to case law." Unfortunately, it is also true that broad sweeping legislation is subject to abuse, and I need not remind you of the terrifying misuse of information that has happened in the last ten years.

To me, it all adds to a case for caution. You, as professionals, must understand what Congress is proposing to do in legislation; you must appreciate how it will impact you dramatically, and impact your companies equally dramatically. I would make the same observation to professional societies as well. They are normally not oriented to legislation, but here is a case that comes very close to home. We all better be with it, or we will discover that there exists inappropriate legislation that is burdensome and annoying, will constrain us in ways that are undesirable, and importantly will create conflicting anomalies in the law.

I agree with the view that it would be nice to prosecute people for the things that they do; but I would also assert that we are getting convictions under present law, and getting the convictions seems more important to me than having a tidy legal situation at the cost of questionable law. As long as we are not losing the ball game completely, I would opt for playing a few more cautious innings until we understand fully just what the game is.

I have given you a second point of view; you have also heard the view that the evidence does justify legislation. You ought not to take either without your own thoughtful consideration. You ought to do your own homework, make up your own mind, and take your own actions as appropriate.

One final item--the whole issue of information ownership, and especially as related to computer programs. The country has not done well with it in the last decade. The matter is still before us and it still needs attention; let us anticipate for the best.

Hopefully I have given you something new to think about in privacy and something new in security. For privacy, it is the information usage question but from the point of view of society overall. For security, the new thought that I would leave with you is the possibility of architectures for distributed arrangements that provide additional safeguard mechanisms that are effective against an ever increasing spectrum of threats. For legislative matters, I would argue we urgently need some analysis so that we understand new dimensions of computer-oriented crime, know where we are going, and what we are trying to accomplish. If I have successfully exposited the general aspects on such issues, I would leave it to you as practitioners in the field to implement the details of the ideas; please do debug them for me. Thank you.

FILMED

3-8