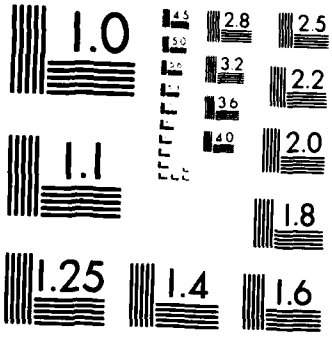
AD-A152 559 INFORMATION AND COMMUNICATIONS PROTECTION(U) RAND CORP 1/1
SANTA MONICA CA W H WARE NOV 84 RAND/P-7033

UNCLASSIFIED F/G 17/2 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963 A

AD-A152 559

INFORMATION AND COMMUNICATIONS PROTECTION

Willis H. Ware

November 1984

DTIC FILE COPY

APR 1 7 1985

E

P-7033

...has been approved
...release and sale; its
...distribution is unlimited.

85 4 ... U

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, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138

Testimony of

Willis H. Ware

INFORMATION AND COMMUNICATIONS PROTECTION

Before the Subcommittee on Courts, Civil Liberties and the Administration of Justice, Committee on the Judiciary, United States House of Representatives

January 24, 1984

Special
A-1

QUALITY INSPECTED 1 DDC

INTRODUCTION

My name is Willis H. Ware. I am a member of the Corporate Research Staff of The Rand Corporation, but the views I state today are solely my own; they in no way reflect a position of The Rand Corporation or of its research clients. Furthermore, my views do not come from a specific research project, but rather reflect more than a decade of my attention to a set of issues of which communications security is one. I am an electrical engineer by training, but have specialized in the field of computer technology for over thirty years.

My credentials for addressing the issue include the following. In 1967, I was the first to bring the broad issue of computer security to the attention of the technical field by organizing a special session on the subject at a Joint Computer Conference in the spring of that year. Subsequently, I chaired a Defense Science Board (Department of Defense) committee to look at the issue of computer security which had never been examined comprehensively anywhere in government. The report was a definitive treatment of the subject, and to this day remains an excellent primer. Computer security, of course, involves communications security.

Because of my work in computer security, I was asked in the early 1970s to join a special advisory group to the Secretary of HEW, and I subsequently became its chairman. Its report, *Records, Computers and the Rights of Citizens,* was the first comprehensive treatment of the matter at the federal level. It provided the intellectual foundation for the Federal Privacy Act of 1974, which among other things created the Privacy Protection Study Commission of which I was a member and vice chairman.

Finally, as a practitioner of computer technology for some three decades, I must for professional reasons stay conversant with modern communications technology, and be aware of the concomitant security and privacy threats. I have participated in a variety of relevant workshops, committees, and task groups. Among them have been several for the Office of Technology Assessment.

In addition to my participation in the activities noted above, I have also spoken and written widely on the subject. In particular, I presented a paper, *Policy Aspects of Privacy and Access*, to a National Science Foundation symposium.*

STATEMENT

Congressman Kastenmeier, it is a pleasure to testify before your committee this morning on a subject of importance to the nation. To make sure that we are on common ground, let me observe first that there are two dominant electronic technologies for information handling, namely computer technology and communications technology. In today's usage the two blend in almost every application. One finds computers in modern-day communications systems; conversely, one finds communications in contemporary computer systems. I would note particularly that contemporary communications systems are, in the large, computer-managed and computer-controlled. For our purposes this morning we can think of communications technology as the collection of technical mechanisms for electronically transporting information from place to place; in

---

*Published by Crane, Russak & Company as a special double issue of its journal *The Information Society*, Vol. 2, Numbers 3/4, 1984.

contrast, computer technology is used primarily to manipulate information in very general ways. It is important to pay careful attention to the meaning of words in our discussion because the two technologies have caused new interpretations of familiar concepts and phrases.

We are talking here today about **electronic** means for transporting information from place to place. We must insert the word **electronic** because there are other mechanisms for information transport, for example the postal carriage of printed materials.

A wide scope of technology is used in modern communications networks. The carriers who operate them employ traditional twisted-pair copper-wire circuits, microwave links, coaxial cable circuits, perhaps wave guide links, fiber optics increasingly, and communication satellites. In the future, perhaps even laser beams might be exploited for such things as short-hop circuits, say, across a river or between buildings of an industrial complex. In each instance the fundamental point of the technology is to convey electromagnetic energy from place to place; it in turn will be the vehicle for transporting information. I might observe parenthetically that the choice of technology in any particular instance is essentially an engineering consideration and balancing of such factors as cost of the installed link, its information capacity, the volume of information to be moved, and the long-time economics of revenue and cost recovery.

Technical opportunity for intercepting the electromagnetic energy--and therefore the information which it carries--is not the same for each technology. For example, microwave and satellite circuits are more exposed in the sense that the energy is in transit through the atmosphere or space, and can therefore be intercepted from afar. Conversely, one has to get close to twisted-pair copper-wire circuits in order to capture its energy.

For the purposes of providing legal protection though, one must consider that any communications mechanism is interceptable in principle. I use the term "interceptable" as a generalization of wiretap.

Thus, there will flow a wide variety of information on circuits composed of a mix of such technology, all networked together by and among carriers. In the past the communications traffic, especially in the classical telephone networks, has been limited predominantly to voice conversations, but in today's world there is an ever increasing volume of data flow; so to speak, computer conversations. There will also be facsimile transmission of images from place to place; there will be video signals such as television, either for commercial distribution or for private use such as in teleconferencing; and on many circuits, particularly those having large transmission capacity, there will be a mix of such information types.

Frequently, information in transit will be represented, so to speak, in its natural form. Voice signals will be represented in transit as electrical ones that wiggle, and the wiggles will be a mirror image of the motion of the air molecules that transmit sound from lips to ear. Similarly, video pictures will probably also be represented in the so-called analog form. Information from computers, however, naturally comes in digital form and it will be transmitted that way, although if one could "hear" such data transmissions, it can sound like a sequence of tones.

On the other hand, much information will be changed from whatever its natural form happens to be into digital form. Voice, for example, may be transformed into a stream of digits which outwardly could be mistaken for a data stream from a computer; it has been digitized. Voice which has been transmitted digitally is then reconstructed to its analog form prior to delivery at the listener's ear. Theory clearly establishes that the reconstructed voice signal contains all of the information in the original spoken word. Commonly a facsimile system transforms the original image by some scanning process into a digital stream and reconstructs it at the receiving end by an appropriate mechanism.

Such are the common carriers of the nation, but out on the ends of their networks are the locally franchised cable networks. They carry many kinds of information now, and in the future can be expected to carry the same broad scope of information as will the common carrier networks--voice, data, television, facsimile, etc.

The Congressional problem is to decide how wide a blanket of protection to throw and what kinds of information warrant protection. Certainly, voice will be included as it already is, but it must be clear that the protection must exist whether the voice is represented within the communications network in analog or digital form. There are increasing volumes of data flow among computer systems of the industrial base, among computer systems of the research establishment, among the computer systems of government, among the computer systems of defense, and on and on. Such transmissions can obviously be of interest to eavesdroppers because they can reveal much about individuals, about corporations, about government, and about sensitive defense matters.

Congress could patch the 1968 Wiretap Act to bring data transmissions under its purview, but I would ask: Why do it piecemeal? It will only bring us back to this table in five or so years to address concerns about other kinds of information transiting the nation's common carrier system.

Even the phrase **wiretap** is inadequate and outmoded. It connotes the wrong thing because much of today's communications traffic is not carried on wires so one needs to consider some broader phrase such as **communications tap** or **communications interception**.

Suppose one does adopt a very broad point of view in order to avoid the risk that new law will be outrun by technology, and suppose one agrees that we really want to afford some measure of legal protection against the unauthorized interception of electromagnetic energy. Then, how does one distinguish between such energy flowing between (for example) microwave antennas owned by the telephone company and electromagnetic energy propagating between two antennas that sustain, say, international communications between the United States and some other continent or between any other two antennas? From a broad technical purview each is a carrier of information which can be intercepted. Distinguishing among them could only be done in some artificial way--which might, however, be desirable or essential from the viewpoint of law.

The point I want to leave with you is that information protection as now addressed in the Communications Act of 1934 and information protection that ~~you~~ will address in any revision of the 1968 Wiretap Act are but two aspects of the same general problem. One would suppose, therefore, that there is an important interface between the two items of legislation, and that some coordination must take place as the respective laws are revised. We must harmonize the concept of protecting information against interception across all pertinent law.

One clear option is to redo the 1968 Act in such a way that it is the legal basis for protecting against unauthorized interception wherever it occurs. A revised 1968 Act could, for example, accommodate any protective mechanisms that a revised 1934 Act might require. Clearly, another option is a minimum patch of the 1968 Act just to catch new technological developments, such as digitized voice, and to catch new kinds of information at risk, such as data flow or facsimile. If Congress chooses the latter course, however, I would urge that we be sure to review the matter again in five years or so lest technology again outruns or endruns law.

Clearly, my choice would be to do the whole job now, once and for all, and to get it off our minds. I do not see any risk attached to providing broad legal protection for any kind of information that is in transit on a communications channel implemented in any technology, and where the information can be represented in either analog or digital form.

I would note parenthetically that the analogous problem also plagues the copyright issue. For example, a movie first comes to the marketplace on film stock. Later the same movie will be transferred from film onto video cassettes or will be electronically transmitted to the viewer along cable television networks or over communication satellite networks instead of visually as in a theater. To whatever extent we wish to provide protection for the information contained on the original film base, such protection ought to be independent of whether it appears on film, on video cassettes, in transit along a CATV network, or over a satellite link. The protection is for the information, not for its fixation or its manner of representation.

Finally, I want to speak briefly to the subject of encryption which in effect hides information. Technically, protecting information by encrypting it is easier to do in the digital world than in the analog world. It is regularly done, of course, in defense communications for digital traffic, but analog information, such as voice conversations, will have first been converted to digital form. There are some things that can be done directly to analog information to protect it, but in general such mechanisms are not as strong as those that can be afforded to digital traffic.

The problem of protecting information in common-carrier communications networks by encrypting it is partly technical, but it is dominantly economic. To protect the common-carrier networks of the country by encryption techniques would require a massive retrofit of the installed plant, and it would require an enormous infusion of capital. Such protective encryption mechanisms, of course, could be done selectively, but then who is to say where an "intercept tap" threat will emerge? Moreover, even if done selectively, it is not likely that it would provide end-to-end protection--from the handset of the speaker to the handset of the listener--so the net effect of encryption would be simply to force the potential tapper to get closer to the handset for his activities. Eavesdroppers who could not get close enough to an unprotected end-link will, of course, be ruled out of the game.

A user can himself provide encryption capabilities if he wishes, but in the present state of art the cost of doing so is roughly $5,000 at each end of the link. Thus the economic burden is out of reach for ordinary individuals.

For encryption the bottom line becomes:

- It is technically feasible--techniques do exist.
- It is extremely costly to do end-to-end.
- It would impact the common carriers enormously if mandated.
- It is out of reach for the ordinary individual.

It has been a pleasure to interact with you this morning. I hope that my views and my way of looking at the problem will be of value as you move forward on an issue which I consider to be of high import.

END

FILMED

5-85

DTIC