INFORMATION POLICY--THOUGHTS FOR THE 80s

Willis H. Ware

August 1982

P-6798

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

INFORMATION POLICY--THOUGHTS FOR THE 80s*

The dominant concern for privacy in the 1970s was directed to recordkeeping systems, ones that maintain information about people for the purpose of making decisions or judgments about them, or for conducting a business transaction with them. The subject is well discussed by this time, has had the attention of two federal-level bodies, has been the subject of several reports and many books, has attracted some amount of research effort, and is generally well understood. While the legislative response may not be as complete as some would want, nonetheless a good foundation exists, but there are significant new dimensions ahead. Let's not speak further in that direction except to note the one major area of recordkeeping untouched by a comprehensive examination by a federal study group is that of law enforcement and criminal justice.

In my view an important new dimension of privacy will emerge in the 1980s as computer technology is used for systems that provide new services which happen to involve personal information other than directly in a recordkeeping sense. Let's develop the topic by example; consider electronic mail or electronic message systems such as the Postal Service is now offering in the so-called ECOM. Incidentally, ECOM is a subclass of first-class mail according to the Domestic Mail Classification Schedule.

An electronic mail system is, by intent, a mechanism to transmit some message from a sender to an addressee or, possibly, multiple

---

*Presented at the NTIA Conference on "Future Directions in Information Policy," U.S. Department of Commerce, Washington, D.C., May 24, 1982.

addressees; and to do so error-free. Hence, one item of personal information in the system is the sender-addressee pair which in principle can be exploited to establish relationships among individuals or groups of individuals. The content of the message itself may very well contain information about people such as their activities, financial transactions, business dealings, legal difficulties, or what have you. Except in a minor way, none of the personal information in an EMS is for recordkeeping purposes.

One aspect of recordkeeping will be billing for services rendered. Moreover, enough information must be stored for reasonable periods to enable misdirected or lost messages to be traced and properly delivered, or to provide audit trails for a variety of management purposes. However, the bulk of personal information is simply in the system for the purpose of being moved from one place to the other, i.e., from sender to addressee.

Thus an interesting aspect of such systems will be that moderately small amounts of personal information are retained within the system for reasonably short periods of time, perhaps weeks or a few months, as a collateral consequence of the function the system performs. Presumably there won't be any long-time archiving. I have come to call such temporary aggregations of personal information "data puddles," simply because they are around for a short while but then dry up and vanish.

In the present legislative situation, mail in the custody of the U.S. Postal Service is governed by various Statutes which stipulate a protective umbrella that must be provided for first-class mail. The Postal Service has imposed the consequences of present Statutes on any

contractor that handled it by stipulating appropriate physical protective measures. Vendors could comply because physical protection is well understood.

In an electronic era, once an electronic message moves from the custody of the Postal Service to that of a telecommunications carrier, it escapes from the purview of the postal Statutes and instead is governed by the Communications Act of 1934. The latter provides a different level of protection and deals quite differently with surreptitious acquisition of information.

I won't argue the technical point in detail, but let me simply note that it is no problem to secretly intercept either microwave or satellite transmissions, both of which are used by most telecommunication carriers. I offer only as evidence what one has read in the media of such intercepts by foreign intelligence services. The necessary antennas are becoming available as a consequence of direct home-reception of satellite-transmitted television, and the ubiquitous personal computer provides ample computing power to sort through the traffic and find desired items.

Thus we have a three-way situation: systems which contain information about people for other than recordkeeping purposes; a mixed, if not confused, and perhaps incomplete legal umbrella of protection; and the very real threat of covert interception of electronic transmissions--altogether, a very awkward and complex public information policy issue.

Offhand one might suggest that the postal Statutes could be extended to cover electronic mail while in the custody of telecommunication carriers but there are two technical problems. Under some

circumstances digital message traffic, such as electronic mail, is combined with normal voice conversations and carried over the same circuit. While techniques exist for protecting digital traffic, techniques for mixed digital and analog voice traffic are another matter. In addition, telecommunication carriers need operational flexibility to reassign traffic to circuits and channels as the total load shifts and changes, or as failures occur to disrupt circuits. For these and other reasons it would be very awkward, if not impossible, for the common carriers of the country to respond to a legislative mandate to selectively protect electronic mail traffic while in transit through their facilities.

To illustrate, the Tax Reform Act of 1976 stipulates that all tax information shall be considered confidential and protected as such. Therefore, such information while in the custody of tax authorities will be protected as required, but the IRS (among others) transmits tax information by circuits provided by a common carrier. Clearly the IRS is in no position to extend the 1976 Tax Reform Act to the common carriers. In a strict interpretation at least, the Act will unavoidably be violated for some amount of tax data unless IRS provides its own protection for the data. Setting aside whatever technical difficulties exist, how could common carriers possibly respond to the demands of such diverse legislation as the postal Statutes, various tax legislation, and who knows what else?

If the Postal Service or anyone else is to offer an electronic mail service with end-to-end protection equivalent to that of the sealed envelope, then the only solution I see would be for the offeror to provide its own protection before entrusting such traffic to the common carriers. But the complexity is just beginning.

Whatever the Postal Service decides to do and whatever legislation is created to govern its behavior, it may well be that there will be private offerors of electronic message systems. What then? One could take the view of caveat emptor. Users of privately offered services would understand that no protection would be afforded and knowingly accept any risk of unintended disclosure. Unfortunately the threat against electronic forms of information is subtle and very different from that against physical objects. The matter is poorly understood by institutions and managers; moreover it is not well understood in magnitude by anyone. Let me offer a reason though why the country might want to require protection for private offerings.

An enormous volume of business, industrial, and commercial information flows over presently unprotected communication circuits. While none of it could properly be classified as national defense or foreign policy and therefore not subject to existing law and executive orders, sufficiently large amounts of it can give very deep insights to U.S. corporate activity, activities in regard to commodity affairs, and much else. There has arisen a new category of information that is related to the general welfare of the country but not governed by law nor executive order. So to speak, it is the industrial espionage game but played among countries. As the situation exists today there is a feast of information available from satellite interceptions that is there for the taking.

Under a document known as "Presidential Directive 24," concern has already been expressed about protecting the communications vital to the

United States but other than that concerned with national defense or foreign policy. The government will obviously want to be a user of electronic message, mail and facsimile systems. If those offered by its own Postal Service or by private concerns are unprotected, how does one resolve the obvious conflict with PD 24? It seems foolish to suggest that the government must provide all of its own electronic message and mail systems. On the other hand, can the government pass any form of legislation that will require end-to-end protection of privately offered electronic mail service? If the government manages to impose such a requirement only on the USPS, then in effect the government could be at the mercy of a monopolistic position.

The situation is a can of worms of first magnitude. It obviously involves a variety of very tricky public policy issues with major technological components. The way through is by no means clear, policy or not; but this is only one example.

As the blend of computer and communications technology makes possible a vast array of new services by public and possibly government offerors, in one way or another information about people will often be involved. New aspects of privacy and information security are bound to arise. Sometimes the issue will be information protection per se. Consider a private organization such as Chemical Abstracts Service; it delivers chemical information services to a wide variety of users. Its services though are value-added, notably indexing and abstracting. As an organization it has contracts with foreign consumers.

In an electronic future, it may well have the problem of assuring secure delivery of data traffic to identified overseas users. Perhaps

such recipients will then add other information value, but at minimum the integrity of the information must be protected and its value as an economic good, safeguarded.

It all suggests that any international data delivery service will require transnational flow of encrypted data--a subject whose present legal status is not at all clear. International electronic message services that offer end-to-end protection will also need similar transborder encrypted data flows. What international law, treaties, agreements and oversight monitoring arrangements will be necessary to deal with this issue?

Here are some more conjectures. What about the personal information that presently gets captured in automated supermarket checkout stands? What about the home computer that allows a law enforcement officer to keep records at home that he is not legally allowed to maintain at the office? What about the ease with which microprocessors can be interfaced with communication circuits and networked together to do who knows what? What about the marriage of cable services with data base vendors? What about all those data puddles that will abound in a wide variety of systems that are yet to be invented and developed? What about the office automation scene? What about all the information about individual behavior and habits that will be captured by automated energy control systems? What about the information captured by systems as a by-product of their use by people? A remotely accessed electronic data bank can know who uses it, when, and for what subject.

The 80s then will not be the traditional recordkeeping scene in which one can speak to this class of records or that--employment or

medical; or to this industry or that--insurance or credit. Rather, the new issues will transcend established jurisdictional, industrial, or legal boundaries. The new policy issues probably won't even fall into the established committee structure of Congress or the agency structure of government. Nor will they fall into the usual trade associations or bodies of industrial spokesmen. Information flows will threaten, pierce, and in some cases destroy a lot of established interfaces and boundaries. Nor can the new issues be handled at the municipal or state level because the effects are generally interstate or international. Nor can all effects be handled on a voluntary industrial basis. For example, law will be needed to create the legal protection of confidentiality and establish judicial mechanisms for appropriate authorized access to some categories of information.

I see no way for the federal government to avoid being involved in some aspects of the coming privacy issues. But the depth of the involvement can be limited to that which is essential if the private sector gets with it and responds adequately and properly. On the other hand, not all privacy issues will arise in the private sector, and in those cases the government will have to do it in its entirety--a prominent example is the electronic offerings of the U.S. Postal Service.

In general then, I would suggest that the new dimensions of privacy policy in the 80s are those concerned with computer-based systems and services that contain, capture, and handle information about people for other than recordkeeping purposes, supplemented by the secondary issue of protecting international transit of data as it flows to legitimate end-consumers in various political jurisdictions.

RAND/P-6798

INFORMATION POLICY--THOUGHTS FOR THE 80s

Willis H. Ware