

rate systems are tied together to improve efficiency. The communication network forms one weak point in the system from the standpoint of eavesdropping and tampering.

Now, for some directions toward a solution.

Assume that not everyone is as honest and as trustworthy as ourselves—but is just as diabolically clever.

Appreciate that we will be dealing increasingly with complex and, hence, difficult-to-understand-all-the-details types of systems in the future.

The people who best understand the operation of each system will be computer designers who build the system in the first place.

The best time for applying fundamental safeguards is during initial system design. "Patchups" at a later date may be relatively less effective compared to good initial design that includes an awareness of the existence and importance of the problem.

We cannot expect and should not expect legislative action alone to substitute for good design. Even ignoring the lag of the legislative/judicial procedure, the detailed subject matter verges on or beyond the limits of legislative effectiveness.

As you know, laws and laws alone have been pathetically ineffectual in stopping the growth of widespread electronic eavesdropping and wiretapping. At most, the courts have succeeded in preventing police from using the same techniques available to the private detective or the criminal—or even a casual reader of an electronics technician's magazine.

While laws in themselves may not solve the problem, new legislation could be helpful in two ways: (a) laws outlawing certain practices will be of minor help in increasing the price of the act and making its commission less flagrant; (b) laws can be written so that potentially weak systems cannot be built unless adequate safeguards are incorporated throughout for the protection of the information stored.

This last direction is to me viscerally unsatisfying as it carries with it a built-in loss of freedom. The creation of another governmental agency peering over one's shoulder contains the possible dangers of bureaucratic delay and arbitrary conclusions based upon inadequate understanding of complex problems.

Historically, Government regulatory agencies start as highly effective bodies but lose momentum as the original personnel leave and their replacements come from the industry being regulated. Where else are you going to get competent people who know the business? The competence needed in a regulatory agency of this type is a too rare commodity.

If the computer industry is to avoid external regulation, then it behooves everyone who is involved with time-shared systems handling potentially sensitive information to start working, or a least thinking, about the problem of privacy. The computer industry should take the initiative and the responsibility of building in the needed safeguards itself before "Big Brother" is forced to do it himself and we may not be too happy with the way he might want to do it.

Safeguards, whether they be screens around moving machinery or circuit breakers, cost money. Every design engineer is reluctant to add anything that costs money and buys little visible protection. But it is time to start regarding such added costs as necessary costs—a price