to society for the privilege of building a potentially dangerous system. When you buy a new system of this type, plan to spend extra for safeguards.

This is not a new concept. We have, for example, been practicing this in the design of sewerage systems and in electrical distribution systems for some time. But, historically, it usually has taken an epidemic to build a local sewerage disposal system. It took a series of disastrous fires to get our electrical codes and possibly the recent Northeast blackout to start work on a better power grid.

The national geographical extent of the new data systems, their impact, and the investment are so large that the price of the "retrofit" after calamities occur may be higher than we need pay with preplanning.

To be more specific, what safeguards do I envision? Of course, we do not know all the answers yet. But, clearly, there are steps that we should be considering, including:

Provision for minimal cryptographic-type protection to all communications lines that carry potentially embarrassing data—not superduper unbreakable cryptography, just some minimal, reversible, logical operations upon the data stream to make the eavesdropper's job so difficult that it isn't worth his time. The future holds the promise of such low-cost computer logic, so this may not be as expensive as it sounds.

Never store file data in the complete "clear." Perform some simple—but key controllable—operation on the data so that a simple access to storage will not dump stored data out into the clear.

Make random external audits of file operating programs a standard practice to insure that no programer has intentionally or inadvertently slipped in a "secret door" to permit a remote point access information to which he is not entitled by sending in a "password."

When the day comes when individual file systems are interconnected on a widespread basis, let us have studied the problem sufficiently so that we can create sensible, precise ground rules on cross-system interrogation access.

Provide mechanisms to detect abnormal informational requests. That is, if a particular file is receiving an excessive number of inquiries or there is an unusual number of cross-file inquiries coming from one source, flag the request to a human operator.

Build in provisions to verify and record the source of requests for information interrogations.

Audit information requests and inform authorities of suspected misuse of the system.

This list is open-ended, and it is hoped that more suggestions will be forthcoming. But this will take much work.

Clearly here is an example of the trade-off between dollars and the type of society we want. We will face such decisions more and more often in the future.

What a wonderful opportunity awaits us to exercise a new form of social responsibility so that the advent of the new computer-communications technology need not be feared as we approach 1984. Rather, we have in our power a force which, if properly tamed, can aid, not hinder, raising our personal right of privacy.