Chapter 12

Regulatory and Other Issues

Contents

Page

TABLE

Table No. *Page*

Chapter 12
Regulatory and Other Issues

Regulatory Boundaries

As computer-based information systems evolve, they challenge traditional concepts of boundaries—physical or social—that are reflected in the law and regulatory policy. The integration of computer and communication technologies form systems that cross boundaries between nations, States, and organizations. The issue of transborder data flow discussed below exemplifies the kinds of international problems created by such integration. Others include the following:

- *Interstate con flict.*" When States have conflicting laws involving information or information processing, for example, property tax laws that cover computer data bases, an integrated data system that exists in a number of different States can raise difficult questions of legal jurisdiction.

  Furthermore, some States may become data havens because they have weaker laws. * Computer networks also allow State-regulated services such as banking to be offered across State borders, thus challenging traditional attitudes toward single State banking. Telephone bill payer accounts, for example, can be used across State boundaries.
- *Federalism.* " Linking Federal data systems with local systems complicates jurisdictional problems even further. The Federal Bureau of Investigation's National Crime Information Center (NCIC) is an example where the traditional autonomy of local and State criminal justice organizations has complicated the Federalism issue (see the OTA assessment of NCIC/CCH, in progress). Similar problems could also arise by linking together Federal and State systems that contain data concerning such matters as taxation, welfare, education, medical care, and drug abuse.
- *Antitrust:* The economics of large integrated data systems, coupled with the potential for increased convenience to the customer, may push service providers to use shared facilities for banking, transportation scheduling, reservation systems, and so on. The Department of Justice and other regulators will be interested in whether such shared facilities create monopolistic barriers to new entrants or are mechanisms for control of the market, or whether they encourage competition by reducing the cost of access for smaller firms.

Information technology is changing form so fast that it is tending to outstrip the working definitions of devices and services that serve as the basis for law and regulation. These definitional problems relate both to the technology itself, and to the products and services that depend on it.

- *Computers or communication:* The best known example is the continuing attempt by the Federal Communications Commission to establish what services and what technologies are already "communications, thus regulated, and what are "computer" services and technologies, thus not regulatable. Their second inquiry on these questions, which began in 1976, only recently resulted in an opinion' that is now under

*A system operator could maintain the computer and data base in a State with a lenient legal environment, and access it by a terminal in a State with stricter laws

'Second Computer Inquiry Docket No. 20828, final decision adopted Apr. 7, 1980, FCC 80-189, and reported as 77 FCC 2d 384 (1980). See also the Memorandum opinion and Order, adopted Oct. 28, 1980, FCC 80-628.

court challenge. Even if the definition is accepted, there is no reason to believe that the problem has been permanently resolved. The general trend toward deregulation of all technology and services, however, may render the question less critical.

- *Branch banking:* Many States have laws that either prohibit or tightly regulate branch banks. An issue that has been debated considerably is whether the automated extensions of banking (e.g. automatic teller machines (ATMs) or pay-by-phone services) constitute "branches" in the usual meaning of the law. Since ATMs and telephone service can be dispersed widely as well as cross borders, significant issues centering on antitrust and interstate banking rest on the way in which a branch is defined (see the OTA assessment of electronic funds transfers, in progress).
- *The status of electronic mail:* Electronic data transmission has opened a major policy question about the definition of mail. As with the computer/communication issue above, this definition is significant because it places a class of services under one or another set of regulations. Unlike many other countries that have combined postal and telecommunication services under one national agency, the United States has pursued completely different approaches to regulating each service category. Electronic mail, in its various forms, provides a new service with features of both manual delivery and telecommunication, and may pose new and difficult regulatory questions (see the OTA assessment of the role of the Postal Service in electronic mail, in progress).
- *Bank information services:* Some very large banks have developed elaborate data processing hardware and software to support their operations. They have found that the sale of these products and information services to other smaller banks can be a profitable enterprise. In their view, it is a natural extension of their banking services. The service bureau industry, which sells access to computers and programs, does not agree. It contends that banks are using their enormous capital resources to enter an entirely new, unrelated field, and should not be allowed to do so under laws that strictly regulate the proper activities of banks.[2] The outcome may hinge on whether these new information services constitute banking in a sense compatible with law.

[2] "Citibank: A Rising Giant in Computer Services," *Business Week,* Aug. 4, 1980, pp. 54-56.

Computer Crime

The changing nature of crime in our information society creates problems in detecting and prosecuting crimes against information systems.[3]

- New types of abuses occur for which there are no appropriate laws.
- Traditional definitions, for instance of theft, may be inapplicable when information is the object of the criminal activity.
- Procuring evidence in information crimes can complicate or stop prosecution.

It may be that these problems will be temporary, and that the legal system will shortly be able to accommodate itself to these types of crimes. It has been suggested,

[3] Susan H. Nycum, *The Criminal Law Aspects of Computer Abuse: Federal Criminal Code* and *The Criminal Law Aspects of Computer Abuse: State Penal Laws*, Stanford Research Institute, 1976.

however, that the inherent nature of information and computer crimes mandates new laws.

Congress has recently considered two bills that address computer crime. The Senate bill would make it a Federal crime to use computers as tools for criminal assault or as its object. * The House** addressed the problem of protecting the providers of in-house information services, in particular cable and broadcast entertainment companies such as Home Box Office, from what is called “pirating. “***[4] The information industry feels that unless governmental sanctions are used to protect its products and services, there will be little incentive to provide them. The radio hobbyists, who are among the major “pirates,” counter that to date practically no technological safeguards are used by off-the-air pay TV and cable TV, and that reasonable use of more secure technology would safeguard these signals without having to legislate a new class of criminals into existence,

Although neither bill was passed by the 96th Congress, the problems that motivated them remain. It is likely that similar legislation will be introduced in the 97th Congress. Computer crime laws have already been passed by 10 States, and at least another 5 have bills pending’ (see table 8).

With the support of the Federal Government, researchers are exploring the nature of computer crime, the methods used and the types and motives of criminals.’ Even without new laws it is of particular importance to inform the staffs of Federal and local law enforcement and criminal justice agencies about the impact of this new type of criminal activity on their work.[7]

Table 8.—States Passing or Considering Computer Crime Legislation

	Passed
Arizona	October 1978
California	January 1980
Colorado	July 1979
Florida	August 1978
Hawaii	(a)
Illinois	September 1979
Massachusetts	(a)
Michigan	March 1980
Missouri	(a)
New Mexico	April 1979
North Carolina	June 1980
Pennsylvania	(a)
Rhode Island	(a)
Utah	May 1979

[a] Legislation Pending

SOURCE Computer Business Equipment Manufacturers Association, *State Legislation Status Report* 1980

To date, studies of computer crime and computer abuse have emphasized the acts of an individual or group of individuals against an organization. Some observers have noted, however, that the computer can also be used by organizations to take advantage of customers or clients. [a] Customers of organizations using electronic billing, funds transfer, or calculating aids (e.g., supermarket scanners) may simply be defrauded. Furthermore, computer systems are used for making many decisions that affect people’s lives, from political apportionment to setting pollution standards and assessing the effectiveness and hazards of a new drug. Therefore, there will likely be some temptation for various interests to misuse the systems they run, for their own purposes.

*S. 240.

**1]. R, 7747 (11. R. 6 192).

*** pirating is stealing the signal and decoding it, and is easy to do with current technology.

‘“The Piracy Danger to Subscription TV, ” *Business Week*, Sept. 29, 1980, pp. 44.

‘Computer and Business Equipment Manufacturing Association, “First State Legislation Status Report, ” Washington, D. C., 1980.

‘Dorm B. Parker, *(’rime by Computer,* Charles Scribners Series, New York, 1976.

‘Department of Justice, *Computer (’n”me: Criminal Justice Resource Manual,* 1979.

“Rob Kling, “Computer Abuse and Computer Crime as organizational Activities, ” *Computers and Law Journal,* spring 1980, pp. 403-427.

Transborder Data F1ow

During the past several years, international attention has been focused on a collection of issues referred to as transborder data flow. These diverse issues have a common origin in the increased communication of data across national boundaries.[9] In the developed world, they have crystallized around the proliferation of national privacy laws that usually specify the treatment of personal data in domestic systems, and also set standards for the transfer of such data across national boundaries. [10] Several potential problems have emerged that would act to constrain the international flow of information.

- Different and conflicting laws could make the operation of distributed computer systems by large multinational corporations difficult if not impossible.
- Third-party organizations providing computer services across national borders could be inhibited from competing with similar firms operating within countries.
- The extension of privacy protection to the concept of legal persons such **as cor**porations could vastly expand the types of information controlled, by restrictions placed on transmission over national boundaries.

Some efforts are underway to reconcile these various constraints. The Ministers of the Council of Europe have approved model legislation that would provide guidelines for national privacy laws.[11] However, the United States is not a member of the Council, and even more significantly, the U.S. approach to privacy law does not fit the Council model. Thus, from the U.S. perspective the Council approach does not provide a solution.

The Organization for Economic Cooperation and Development has developed a voluntary agreement for its member states that would be more flexible.[12] The initial enthusiasm for a third approach—an international treaty on information flow—appears to have been dampened by the difficulties in getting even a general voluntary agreement.

In general, the U.S. position on this issue has been to favor the free flow of information across borders, and to view the European privacy efforts as principally a disguise for protectionist control of international commercial data processing. Some Europeans maintain that their actions derive principally from their deep concerns about privacy, pointing to historical abuse by totalitarian nations of government and private record systems.

Another aspect of the transborder data flow issue is the concern by the Third World countries that control over information and information flow is a form of international power exerted by the Western nations. This attitude was manifested both in negotiations at the World Administrative Radio Conference[14] and in proposals in the United Nations Educational, Scientific, and Cultural Organization (UNESCO) for a “New Information Order. ”

[9] R. Turn (cd.), *Transborder Da ta Flou's.* report of the American Federation of Information Processing Societies, Panel on Transborder Data Flow, 1979.

[10] “Department of Commerce, *Selected Foreign National Data Protection Laws and Bills*, Office of Telecommunication, special publication 78-19, 1978.

[11] Council of Ministers of the Council of Europe, “Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, ” approved September 1980.

[12] Council of the Organization for Economic Cooperation and Development, *Recom mend tion of the Council Concern - ing Guidelines Gov'erning the Protection of Privacy and Transborder F1ouI.s of Personal Data*, adopted Sept. 23, 1980.

[13] Department of State, Bureau of Oceans and International Environment and Scientific Affairs, *Selected Papers on International Policy Implications of Compu ters and Adoanced Telecom munications Systems*, January 1979.

[14] See U.S. Congress, Office of Technology Assessment, *Assessment of Radio FrequencyUse and Management Impacts From the World Administrative Radio {'conference of 1979*, in progress.

The concerns that have been expressed are not just focused on computer systems. They also cover such topics as international news-gathering, access to satellite communication, the spilling of broadcasts over borders, and the exchange of scientific data. However, the fundamental attitudes and goals of the various nations as expressed in their negotiations over international information policy will undoubtedly shape the laws and regulations under which international data systems will be operated in the future.

Information Gap

Some observers have suggested that the advent of information technology will widen the gulf between the haves and the have-nots in society. This view is based on relative differences in what might be called “information literacy, ” the ability to use information technology to cope with everyday life.

The technology itself is potentially highly flexible. Information systems can be designed to make the use of devices and services far easier than before, for example by providing access to people with language problems and physical handicaps. Research and development (R&D) in such subjects as computer speech, speech understanding, and pictorial display will continue to improve the potential accessibility of information technology.

Whether these capabilities will be used by a system designer is a different question. Making a computer system accessible often imposes added costs for hardware or for more computation. Therefore a concern for efficiency or economy, or the system designer’s biases or ignorance, can result in an information system with unequal accessibility built into it. ”

Should such an information gap develop, it could affect the citizenry in areas such as:

- *Employment:* As automation penetrates the workplace—both manufacturing and white-collar—unemployment may result not so much from increased productivity as from the inability of existing employees to adapt to the new technology. If projections about an evolving information society and economy are correct (see ch. 5), information literacy could become an essential requirement for entering the labor market.
- *Relation with Government:* To the extent that information technology stands between the citizen and a governmental obligation or service, a potential barrier exists. Banks carried out extensive studies with regard to consumer acceptance before undertaking the design of ATM devices. Government agencies, on the other hand, because they do not have the same economic motivation, may not necessarily be very concerned about the acceptability of their systems. (Incentives to have such concern may need to be imposed by law, regulation, or executive policy.) Individuals who are technologically illiterate may be affected in several ways:
  —they may not exercise basic rights such as voting;
  —they may be at a serious disadvantage in legal proceedings, both criminal and civil; and
  –they may find access to such needed services as welfare, health care, and educational benefits, barred or severely impeded.

To the extent that information illiteracy is unevenly distributed among cultural or eco-

“>hlilton R. Wessel, *Freedom's Edge: The Computer Threat to Society* (Reading, Mass.: Addison-Wesley Publishing Co., 1974).

[16]T. Sterling, et al, “Humanizing Information Systems: A Report From Stanley House, ” *(’communications of the Association for Computing Machinery*, November 1974, pp. 609-612.

nomic groups, the consequences would fall disproportionately on the poor and disadvantaged, in general. The gulf between the haves and the have-nets in society might not only be increased but, due to such barriers as a more limited access to jobs, societal efforts to bridge that gulf would be frustrated.

Computer Software Protection

As discussed in chapter 3 and later in chapter 13, the cost of computer software has become a pacesetting factor in development of new computer applications. Increasingly, computer hardware is being designed to fit the software. With the investment so high, the value of software research and development is even greater and the need for proprietary protection felt even more strongly. At the same time, however, there is a strong need for innovation in software R&D, the sharing of ideas, and breakthroughs among researchers.

Copyright and patent protection are the traditional means for protecting the commercial value of information while providing for public disclosure. But the continuing uncertainty concerning copyright and patent protection for computer software leads many software researchers to use the trade secret approach to protect their time and dollar investment. Private firms doing software R&D generally protect software trade secrets through employee nondisclosure agreements, restricted access measures, and by otherwise keeping the work confidential. This of course makes the sharing of information in the software R&D community quite difficult.

The Copyright Act of 1976 specifies that computer programs are copyrightable as “literary works. ” But the extent of protection defined under the act and more recent court decisions[17] have left the situation ambiguous. Amendments to the act were introduced and enacted in the 96th Congress as the “Computer Software Copyright Act of 1980."[18] However, the issue of computer software protection appears sufficiently important and unsettled to warrant continued congressional attention. [19]

[17] *Data Cash Systems, Inc. v. JS&A Group, Inc.,* U. S. D. C., for Northern Illinois, Sept. 26, 1979.

‘“H. R. 6934, Mar. 26, 1980, enacted as an amendment to H.R. 6933, “Government Patent Policy Act of 1980, ” Public Law 96-517, Dec. 12, 1980, and based on a recommendation of the National Commission on New Technological Uses of Copyrighted Works, *Final Report,* Washington, D. C., 1979.

¹⁹See “Court Broadens Rules on Patenting Software, ” *Science,* vol. 211, Mar. 20, 1981, pp. 1325, ff.