Information Policies for Electronic Service Delivery

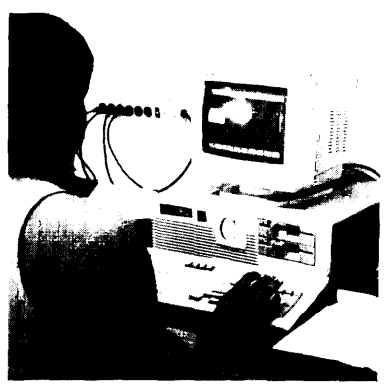
7

SUMMARY

Most Federal information policies either predate the electronic era or reflect, at best, the period when expensive mainframe computers dominated agency automation and telecommunications meant "plain old telephone service." The policymaking process has lagged technological advances and new applications by several or more years. Electronic service delivery provides a framework for balancing the reality of decentralized, dispersed, user-oriented agency automation with the need for some measure of centralized, yet flexible, policy direction and oversight.

The transition to electronic delivery of many Federal services will require the review and updating of most Federal information policies. Congress can play a central policymaking role in assuring that electronic delivery develops in ways that maintain or enhance: equity of access to Federal services; open government; confidentiality and integrity of service delivery; and fair and effective competitive procurement.

Perhaps the greatest challenge will be assuring equitable access to Federal services in an electronic environment. This will require both the kinds of management, planning, partnering, and budgeting actions discussed in chapter 6 and the various policy actions discussed here. To have meaningful electronic access, citizens need to know what services exist and how to obtain them, and they must be able to make the electronic connections necessary to receive the services at an affordable price. The Office of Management and Budget's (OMB) recently revised Circular



FRED B. WOOD

A-1 30 on "Management of Federal Information Resources" provides new guidance on many policies relevant to equitable access, such as directories, pricing, and use of depository libraries.] Congress could review the revised A-130 and determine which provisions warrant statutory treatment or fine-tuning to reinforce and clarify legislative intent.

Electronic delivery should provide many opportunities to improve citizen access not only to agency-specific mission-oriented services, but to the processes of government (e.g., hearings and rulemakings). The long-standing congressional commitment to open government is reflected in several statutes, such as the Freedom of Information Act, Federal Records Act, Government in the Sunshine Act, and Federal Advisory Committee Act. Congress could review and update open government statutes to clarify their applicability to electronic services and activities, and emphasize the appropriate use of information technology. Congress could require that governmental process information—for example, information on hearing schedules or opportunities for public comment or input—for both the executive and legislative branches be provided via electronic as well as conventional means.

Widespread electronic delivery of services that involve personal or financial information will create new privacy and security risks and accentuate the need for stronger safeguards. Congress could review and update the Privacy Act, Computer Security Act, and related statutes to help ensure the confidentiality and integrity of electronic delivery. Congress also could direct OMB and the National Institute of Standards and Technology (NIST) to conduct a privacy/security review of electronic delivery initiatives. Congress could extend the scope of the Privacy Act to include private sector systems used in electronic delivery, and establish a permanent, independent Privacy Protection Commission or Board to help assure protection of personal information used in electronic delivery.

Electronic delivery also will intensify the need to clarify Federal policy on contracting for information technologies and services. Congress could review the revised OMB Circular A- 130, any proposed revisions to OMB Circular A-76 on "Performance of Commercial Activities," and Federal procurement statutes to help assure an appropriate balancing of the sometimes competing considerations related to electronic delivery: public accountability; equity of access; government efficiency; public/private sector cooperation; and equity of competition (a "level playing field"). Absent improvements in procurement practices, major contracting for electronic service delivery could further strain a Federal procurement process that is already overly complicated, lengthy, rigid, expensive, and inefficient.

Congress could review and update information policies individually, in groups, or as part of a comprehensive package. The reauthorization of the Paperwork Reduction Act[2] (PRA) could be used as a vehicle, as could new legislation such as a "Federal Information Management Act" or "Electronic Service Delivery Act" that might supplement or supersede the PRA. Congress could encourage or require that OMB and individual agencies explicitly address these policy areas early in the demonstration and pre-operational stages of electronic delivery projects, and when considering information technology as a part of agency reorganization. Implementation of electronic delivery would, in many cases, require revision of public

---

[1] See Office of Management and Budget, Circular A- 130 Revised, "Management of Federal Information Resources," *Federal Register*, vol. 58, No, 126, July 2, 1993, pp. 36068-36086,

[2] The Paperwork Reduction Act of 1980, Public Law 96-511, was amended once by the Paperwork Reduction Reauthorization Act of 1986, Public Law 99-500. The reauthorization was for 3 years. Subsequent efforts to reauthorize and further amend the Act have not, as yet, reached fruition, but are continuing in the 103d Congress. See S. 681, the Paperwork Reduction Reauthorization Act of 1993, Mar. 31, 1993; S. 560, the Paperwork Reduction Act of 1993, Mar. 10, 1993; and H.R. 2995, the Paperwork Reduction Act of 1993, Aug. 6, 1993.

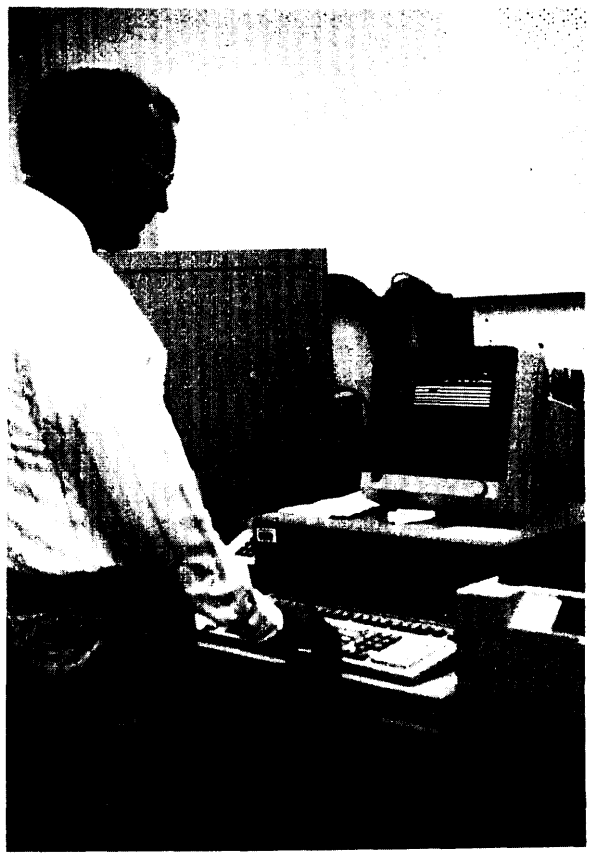
laws that establish and define the services being delivered.[3]

Congress could consider policy revisions in the context of proposals from the administration's technology policy, performance review, and information infrastructure initiatives. The administration's technology policy asserts that, to make government work better through information technology, "[m]any of the government's policies in such areas as privacy, information security, records management, information dissemination, and procurement will be updated to take into account the rapid pace of technological change."[4]

PROTECTING PRIVACY AND SECURITY

The Federal Privacy Act is intended to protect personal information maintained by the government from inappropriate or unauthorized disclosure and uses The original Privacy Act was passed in the early days of agency automation, before microcomputers or widespread electronic networking. Congress has modestly updated the Act to address applications such as computer matching (the electronic comparison of lists of persons receiving different benefit programs to help detect fraud, waste, and abuse).[6]

The pressure to match computer lists of government aid recipients against computerized tax, social security, medical, veterans, and other files seems relentless. The social security number has become a de facto national identifier, although this



FRED B. WOOD

The use of optical disks makes gigabytes of driver's license information available in seconds to State of Washington officials. The technology permits improved service to the citizens of Washington State, but also increases the need for protection of the privacy and security of personal information stored in State data banks.

[3]For a broad overview, see Charles R, McClure, Rolf T. Wigand, John Carlo Bertot, Mary McKenna, William E. Moen, Joe Ryan, and Stacy B. Veeder, Syracuse University School of information Studies, "Federal Information Policy and Management for Electronic Services Delivery," contractor report prepared for the Office of Technology Assessment, Dec. 21, 1992,

[4]President William J. Clinton and Vice President Albert Gore, Jr., "Technology for America's Economic Growth: A New Direction To Build Economic Strength," Feb. 22, 1993. Also see Vice President Al Gore, *Creating u Government That Works Better and Costs Less: Report of the National Performance Review* (Washington, DC: US. Government Printing Office, Sept. 7, 1993). One of the National Performance Review's crosscutting task forces focused on re-engineering the Federal Government through information technology. See National Performance Review Accompanying Report, *Reengineering Through Information Technology* (Washington, DC: U.S. Government Printing Office, September 1993), and the closely related Information Infrastructure Task Force, "The National Information Infrastructure: Agenda for Action," National Telecommunications and Information Administration, Washington, DC, Sept. 15, 1993. Also, improving the delivery of Federal services is within the scope of the proposed National Commission on Executive Organizational Reform. See S. 101, the Executive Organization Reform Act of 1993, introduced Jan. 21, 1993, and reported out by the Senate Committee on Governmental Affairs on Aug. 5, 1993. Recently enacted legislation will require Federal agencies to establish clear goals against which performance of agency activities-including service delivery-can be measured. See the Government Performance and Results Act of 1993, Public Law 103-62.

[5]Privacy Act of 1974, Public Law 93-579,

[6] Computer Matching and Privacy Protection Act of 1988, Publ ic Law 100-503; Computer Matching and Privacy Protections Amendments of 1990, Public Law 100-503.

use is technically prohibited by law.[7] And extensive computer matching can lead to a "virtual" national data bank, even if computer records are not physically centralized in one location.[8] Widespread use of 1-800 and 1-900 telephone numbers, combined with caller ID, has created new avenues for unintentional disclosure of personal information. By combining information from computerized credit, census, marketing, change-of-address, and mailing-list files, private companies can construct de facto personal profiles on individuals that are amazingly accurate.[9]

Privacy advocates believe that stronger privacy safeguards are needed to deal with current computer applications, and with new electronic service delivery applications. Electronic delivery of services that involve personal information will create new privacy risks and require stronger protections. Widespread electronic benefits transfer could mean that eligibility and payments information moves over a variety of electronic networks involving banks, retailers, clearinghouses, and the like, in addition to the government agencies already involved.[10] "Smart" cards could include a wide range of personal information. Use of kiosks or electronic filing to determine eligibility for Federal benefits could cut red tape and costs, but would create new opportunities for third-party abuse of personal information.

Computer networking, electronic kiosks, or interactive television, if used to request government services or information, create the potential to monitor citizen preferences. Profiles of citizens' interests compiled from information provided to a kiosk could be valuable for marketing purposes, for example, just as retail purchasing patterns are used to generate commercial mailing lists. Electronic delivery could increase opportunities for commercial "information brokers" to obtain personal information through legal and illegal means.11 It also could further weaken the ability of individuals to control the use of personal information, and could violate principles of fair information practice. [12]

Fortunately, electronic technology could also be used to protect privacy. Electronic delivery could, for example, allow individuals to access personal information maintained in government record systems, check its accuracy, request corrections, and monitor their records to make sure the corrections are made. Electronic mail or electronic data interchange could provide the opportunity for individuals to give informed consent prior to secondary use of personal information. Today, few people know how to exercise their legal rights to request copies of personal information stored in government or private sector record systems. Few even know where such personal information is stored or what uses are being made of the information. Existing or new technological applications rarely focus on protection of personal privacy. Intentionally or not, government and commercial

---

[7] The U.S. Court of Appeals for the Fourth Circuit recently voided the Commonwealth of Virginia's requirement that voters' social security numbers (SSNs) be recorded and made publicly available, noting concern over the potential use of SSNs for unauthorized access to personal information. See *Marc A. Greidinger v. Bobby Ray Davis, et al.,* USCA-4, *No. 92-1571,* Mar. *22, 1993.*

[8] *See* U.S. Congress, Office of Technology Assessment, *Electronic Record Systems and Individual Privacy,* OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986); and U.S. Congress, Office of Technology Assessment, *Privacy Rights in Computerized Medical Information,* forthcoming, 1993.

[9] See also u s. Congress, House, Committee on Government Operations, Subcommittee on Government Information, Justice, and Agriculture, *Give Consumers a Choice,* H.Rep. 102-1067, 102d Cong., 2d Sess. (Washington, DC: U.S. Government Printing Office, December 1992).

[10] See ch. 4 and U.S. Congress, Office of Technology Assessment, *Electronic Delivery of Public Assistance Benefits: Technology Options and Policy Issues,* OTA-BP-CIT-47 (Washington, DC: U.S. Government Printing Office, April 1988).

[11] See U.S. Congress, House, Committee on the Judiciary, Subcommittee on Constitutional and Civil Rights, *Sale of Criminal History Records, Hearing,* 102d Cong., 2d Sess. (Washington, DC: U.S. Government Printing Office, July 30, 1992), that discusses how private companies can obtain credit, social security, employment, driver's license, criminal history, and other personal information on most U.S. citizens-sometimes using illegal methods.

[12] See U.S. Congress, Office of *Technology* Assessment, *Individual Privacy,* op. *cit.,* footnote *.

interests usually take precedence over the privacy rights of individuals.

Public opinion surveys continue to indicate that Americans place high value on privacy of personal information, and have little confidence in the privacy of computerized records.[13] To prevent further erosion of individual privacy, new privacy rules would be needed to define appropriate use of personal information associated with electronic service delivery. Key principles could include the right of individuals to:

- know about electronic delivery systems that include personal information and how these systems and information will be used;
- have the opportunity to give prior informed consent regarding all uses and disclosures of personal information in electronic delivery systems;
- have access to and review personal information in such systems;
- correct erroneous information; and
- seek redress before an ombudsman or citizen advocate in the event of any alleged abuse, misuse, or uncorrected error.

To the extent that electronic delivery involves public-private partnerships, the Federal Privacy Act may need to be extended to cover related private sector activities. When electronic delivery involves State or local government participation, then applicable State privacy laws also may need to be amended and strengthened. The magnitude of the potential privacy threat may be great enough to warrant consideration of stronger privacy oversight than exists today. Privacy advocates have long argued for establishment of an independent Federal Privacy Protection Commission or the equivalent.[14] The Computer Matching and Privacy Protection Act did require each Federal agency to set up a so-called Data Protection Board to review and monitor agency computer matching projects, but these Boards are comprised of current agency officials just wearing another hat, and are not truly independent. Congress could strengthen these Boards and provide them with more independence and separate staff, along the lines of the agency inspectors' general offices.

OMB's Office of Information and Regulatory Affairs provides privacy oversight that is independent of the line agencies, but it is still subject to the value judgments and policies of the administration in power. The same is true for the Office of Information and Privacy in the U.S. Department of Justice. As an alternative, a Federal Privacy Protection Commission could serve as:

---

13 *Ibid, and* Office of Technology Assessment, *Privacy Rights,* op. cit., footnote 8. Several earlier OTA studies also highlighted the importance of privacy issues, See U.S. Congress, Office of Technology Assessment, *Computer-Based National Information Systems: Technology and Public Policy Issues,* OTA-CIT-146 (Springfield, VA: National Technical Information Service, September 1981); U.S. Congress, Office of Technology Assessment, *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity,* OTA-BP-CIT-12 (Springfield, VA: National Technical Information Service, March 1982); U.S. Congress, Office of Technology Assessment, *Implications of Electronic Mail and Message Systems for the U.S. Postal Service,* OTA-CIT-183 (Springfield, VA: National Technical Information Service, August 1982); and U.S. Congress, Office of Technology Assessment, *Alternatives for u National Computerized Criminal History System,* OTA-CIT-161 (Springfield, VA: National Technical Information Service, October 1982). Also see discussion of privacy issues in U.S. Congress, Office of Technology Assessment, *Automated Record Checks of Firearm Purchasers: Issues and Options,* OTA-TCT-497 (Washington, DC: U.S. Government Printing Office, July 1991); and U.S. Congress, Office of Technology Assessment, 7-he *FBI Fingerprint Identification Automation Program: issues and Options,* OTA-BP-TCT-84 (Washington, DC: U.S. Government Printing Office, November 199 1). Numerous public and private groups involved in the development of a national information infrastructure have identified privacy as a priority concern. H.R. 1757, the National Information Infrastructure Act of 1993, approved by the House on July 26, 1993, identifies privacy and security of networked transmissions as one of several priorities. Also see Information Infrastructure Task Force, op. cit., footnote 4.

14 Canada, Australia, and several Western European nations have privacy commissions or boards. Proposals for a U.S. privacy or data protection board date to 1974, when Senator Sam Ervin proposed a Federal Privacy Board to complement the Privacy Act of 1974, Legislation to establish a privacy board or commission has been introduced in the last six U.S. Congresses. See H.R. 3743, the Privacy Protection Act of 1984, Aug. 2, 1983; H.R. 296, the Consumer Privacy Protection Ac(. Jan, 3, 1985; H R, 1721, the Data Protection Act of 1985, Mar, 26, 1985; H.R. 638, the Data Protection Act of 1987, Jan, 21, 1987; H.R. 1549, the Individual Privacy Projection Act of 1987, Mar, 11, 1987; H.R. 126, the Individual Privacy Protection Act of 1989, Jan. 3, 1989; H.R. 3669, the Data Protection Act of 1989, Nov. 15, 1989; H.R. 280, the individual Privacy Protection Act of 1991, Jan. 3, 1991; H.R. 685, the Data Protection Act of 1991, Jan. 29, 1991; and H.R. 135, the Individual Privacy Protection Act of 1993, Jan. 3, 1993.

1. a focal point for citizen input and views on privacy matters (using electronic technology where appropriate, such as 1-800 numbers, electronic mail, and computer networking);
2. an ombudsman for citizens with privacy concerns;
3. an overseer of agency (and, prospectively, private sector) compliance with existing laws and regulations;
4. an investigator of alleged violations; and
5. an advocate for new or stronger laws when needed.

Congress could establish a Privacy Protection Commission or Board as an independent agency of the executive branch, or as a component of any Federal Information Management or Electronic Service Delivery agency that might be created. Since privacy and security are closely linked, Congress could include security within the mission of any Commission or Board—for example, a Federal Privacy and Security Protection Board.

Whether under the current or new institutional arrangements, Congress and the administration could require:

1. explicit early consideration of privacy threats and protection by each agency planning electronic delivery;
2. afresh round of up-to-date training for agency privacy specialists;
3. advance public notice of any privacy implications to clients of electronic delivery programs; and
4. agency workshops, forums, and communication with privacy advocates on the topic of electronic delivery and individual privacy.

Congress also could enact or update privacy statutes in specific programmatic areas where electronic delivery is likely, such as welfare, education, and health care.[15]

The 1980s were marked by growing public and congressional concern about the security of computer and communication systems.[16] Congress enacted the Computer Security Act in 1987 to improve security oversight and safeguards for Federal computer systems.[17] Paperwork Reduction Act amendments strengthened computer security management. The Electronic Communications Privacy Act of 1986 tightened legal protections against unauthorized interception of telecommunications and electronic mail.[18] The Computer Security Act assigns NIST the lead role for the technical aspects of computer security in Federal civilian agencies (the National Security Agency (NSA) has a comparable role for defense agencies). The PRA assigns OMB and the General Services Administration oversight responsibility for Federal civilian agency computer security, including technical and management actions, training, and audits to enhance security. The PRA also requires that computer security be addressed in agency information technology plans.[19]

Widespread electronic service delivery will increase the security risks. Valuable personal, financial, and government data will flow over a complex web of telecommunication networks technically accessible via an ever-growing number of computers, kiosks, and other terminals at-

---

15 For an up-to-date general discussion, see Office of Technology Assessment, *Privacy Rights in Computerized Medical Information*, forthcoming, 1993.

16 See U.S. Congress, Office of Technology Assessment, *Electronic Surveillance and Civil Liberties*, OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, October 1985); *Federal Government Information Technology: Management, Security, and Congressional Oversight*, OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986); *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987); *Critical Connections: Communication for the Future*, OTA-CIT-407 (Washington, DC: U.S. Government Printing Office, January 1990).

17 Computer Security Act of 1987, Public Law 100-235.

18 Electronic Communications Privacy Act of 1986, Public Law 99-508.

19 As specified in amendments included in the Paperwork Reduction Reauthorization Act of 1986, Public Law 99-500.

tached to the networks. Stand-alone units—such as kiosks located in malls—will represent new targets of opportunity for vandalism and robbery, along with automated teller machines (ATMs) and point-of-sale (POS) terminals. Electronic benefit transfers will be vulnerable to sophisticated white-collar computer crime, just as electronic funds transfer (EFT) is today. The information flow in an electronic world is, in general, more vulnerable to deliberate or accidental alteration and interception. The risks are further compounded because erroneous information can be rapidly disseminated over electronic networks and become accessible to large numbers of persons and organizations. Security in a networked environment poses very real and substantial challenges.[20]

It may be possible to keep computer security problems at an acceptable level, as is the case with commercial EFT and ATM and POS terminals. But this will require that Federal agencies and others participating in electronic delivery of Federal services give as much attention to security as do banks and financial institutions, especially where money or personal information are involved,

Congress and the administration could review the applicability of the Computer Security Act, Electronic Communications Privacy Act, and Computer Fraud and Abuse Act to electronic service delivery, and make whatever changes are needed to help ensure secure electronic delivery.[21] This might include extending some legal protections and security requirements from Federal agencies and users to all organizations that participate in electronic delivery, Also, electronic delivery inevitably will be affected by the ongoing debates over: 1) the roles of NIST and NSA in oversight of computer and communication systems in Federal civilian agencies; 2) selection of encryption technologies;[22] and 3) tensions between privacy, personal or organizational security, national security, and law enforcement interests.[23] Legal disputes over the applicability of privacy and security statutes to electronic mail only foreshadow the debates likely to ensue with growth of electronic delivery.[24]

A security risk analysis should be an integral part of electronic delivery planning. The analysis should examine the technical, physical, human, and organizational threats and protections to electronic services. Electronic delivery will only be as secure as its weakest link; if security is lax at end-user terminals, for example, tight security at the sending agency will be meaningless. OMB Circular A-130 could be further revised to focus attention on the security of electronic delivery systems.[25] In the 1993 Information Resources Management (IRM) planning bulletin, OMB asks agencies to report on improvements in systems security, security awareness and training programs for personnel, and agency-wide security upgrades resulting from internal or external audits

20 A new Office of Technology Assessment study will focus on privacy and security in a networked computer environment. Also see U.S. Congress, Office of Technology Assessment, *Accessibility and Integrity of Networked Information Collections*, BP-TCT-109 (Washington, DC: U.S. Office of Technology Assessment, July 1993),

21 The U.S. Department of Justice, for example, is considering possible revisions to the Computer Fraud Act, including forfeiture of computers used in criminal activities, criminal ization of intentionally planting computer viruses, and stiffer penalties for computer crimes that invade personal privacy or threaten national security,

22 The debate over the proposed key escrow chip, known as the "clipper chip," for encryption has heightened concerns among civilliberty and privacy advocates, and some in private industry, about potential government abuse. Law enforcement and national security agencies seek to maintain their technical ability to intercept even encrypted systems when necessary to carry out their agency missions.

23 For historical background, see Office of Technology Assessment, *Electronic Surveillance*, op. cit., footnote 16; Office of Technology Assessment, *Electronic Record Systems and Individual Privacy*, op. cit., footnote 8; and Office of Technology Assessment, *Defending Secrets, Sharing Data*, op. cit., footnote 16. By presidential order, an interagency task force is reviewing the current Federal system for classifying, safeguarding, and declassifying information, See Information Security Oversight Office, U.S, General Services Administration, "Hearing: Changes to the Security Classification System," *Federal Register, vol. 58, No, 96,* May *20,* 1993, p, *29480.*

24 See for example, the *controversy* surrounding *U.S.* Secret *Service* efforts to monitor electronic mail and bulletin boards used by computer hackers.

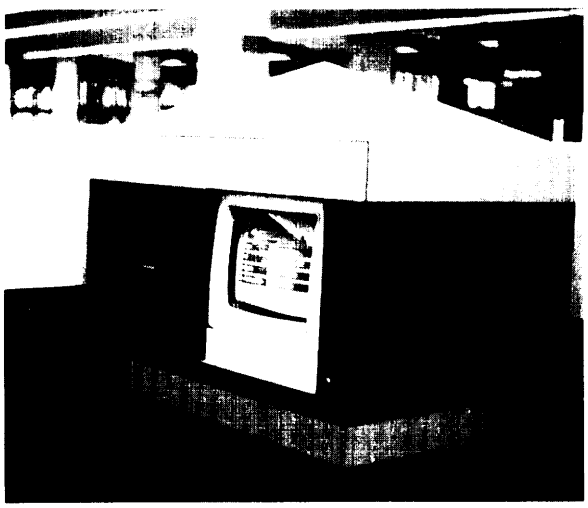
25 Office of Management and Budget, Circular No. A-130 Revised, op. cit., footnote 1.

or reviews.[26] OMB could, in the future, direct agency attention to the linkages between agency security activities and electronic service delivery initiatives, and require more complete monitoring and reporting of security breaches.

OPEN GOVERNMENT

The longstanding congressional commitment to open government is reflected in the Freedom of Information Act (FOIA), Government in the Sunshine Act, and Federal Advisory Committee Act.[27] The intent of these statutes is to ensure that the processes and substance of the Federal Government are open and accessible to the American people. Electronic technology can substantially improve public access and reduce the cost of access, under the general rubric of electronic service delivery. But there is no guarantee that this will happen. The governmentwide access statutes do not explicitly address electronic applications, thus

PHOTOS: FRED B. WOOD



Top left: *Island Epicenter touchscreen kiosk located in the Mercer Island Public Library, Washington State.*

Top right: *Mercer Island Public Library, a place for community access to electronic information services.*

Bottom left: *Microcomputers available for public use in the Mercer Island Public Library, Washington State.*

26 Office of Management and Budget, "Information Resources Management (IRM) Plans Bulletin," OMB Bulletin No. 93-12, Apr. 28, 1993.

27 Freedom of Information Act of 1966, Public Law 89-487; Government in the Sunshine Act of 1974, Public Law 94-409; Federal Advisory Committee Act of 1972, Public Law 92-463.

leaving agencies considerable discretion, Congress could review and revise each of these statutes to reflect advances in technology.

The pros and cons of updating FOIA have been debated for several years. Opponents emphasize that FOIA applies to Federal information regardless of format, and that judicial and administrative interpretations are clearly moving in this direction—thereby lessening the need to amend the Act. Opponents also are concerned that opening FOIA up to amendment might lead to unintended, regressive provisions. Proponents believe that the law leaves too much discretion to executive agencies, leads to unnecessary disagreements over what should be accepted as basic principles (e.g., over the FOIA status of agency electronic mail), and results in many lost opportunities to use technology to improve access to information.

OTA's prior work concluded that new electronic applications were likely to overtake FOIA.[28] The transition to electronic service delivery will surely exacerbate problems and increase lost opportunities if FOIA is not updated. Kiosks and home or office computer terminals offer great potential for remote electronic access to FOIA material kept in Federal agencies, as do off-line digital formats like compact optical disks. Electronic technology offers the potential to greatly reduce the costs of FOIA access for both citizens and Federal agencies. Copying paper documents is costly and cumbersome by comparison. Agencies need to design their automation programs to both facilitate FOIA access and tightly control access to private, proprietary, national security, and other exempted information.

Various researchers and advocacy groups alike have reaffirmed the applicability of FOIA to electronic information. Most support the following principles, and their enactment into law if necessary to assure agency compliance:[29]

- Federal agencies should provide information in any format in which it exists;
- information maintained in electronic format is fully covered by FOIA;
- when providing information in electronic formats, Federal agencies should include any manuals or software necessary for the retrieval and use of the information; and
- when responding to FOIA requests for electronic formats, Federal agencies should use the format requested if it already exists or can be generated with reasonable effort using existing software and equipment.

To complement an updated FOIA, or as an alternative, Congress could replicate the statutory approach used in the "community right-to-know" provisions of the Superfund Amendments and Reauthorization Act of 1986. Title III mandated public access to toxic waste information, known as the "Toxic Release Inventory," in several formats— including electronic.[30] The basic premise is that electronic technology can improve public access to information collected or developed by Federal agencies—if agencies plan for and include these capabilities in their electronic delivery and automation programs, Congress could develop a

---

[28] See U.S. *Congress,* Office of Technology Assessment, *Informing the Nation: Federal Information Dissemination in an Electronic Age,* OTA-CIT-396 **(Washington, DC: U S. Government Printing Office, October** 1988), and *Helping America Compete: The Role of Federal Scientific and Technical Information,* OTA-CIT-454 (Washington, DC: U.S. Government Printing Office, July 1990). See also Jamie A. Grodsky, "The Freedom of Information Act in the Electronic Age: The Statute Is Not User Friendly, " *Jurimetrics,* vol. 31, No. 1, **fall 1990, pp.** 17-51.

[29] See, for example, Henry H. Perritt, Jr., "Federal Electronic Information Policy," *Temple Law Review, vol. 63, No. 2, 1990,* pp. *202–2S0;* **and** American Bar Association, Section of Administrative Law and Regulatory Practice, Report to the House of Delegates, "Public Access to Government Electronic Information Under the Freedom of Information Act," February 1990 Legislation to clarify the applicability of FOIA to electronic formats has been introduced in the prior two Congresses See H. I?. 2773, the Freedom of Information Public Improvements Act **of** 1989, June 28, 1989; H.R. 1423, the Freedom of Information Public Access Improvement Act of 1991, Mar. 13, 1991; and S. 1940, the Electronic **Freedom of Information Improvement Act of 1991,** Nov. **7, 1991.**

[30] **For** background, see Susan G Hadden and W James Hadden, Jr . "Government Electronic Services and the Environment," contractor report prepared for the Office of Technology Assessment, November 1992.

standard “community or public right to know” provision that could be added to agency or program-specific statutes as they come up for reauthorization.

The Government in the Sunshine and Federal Advisory Committee Acts are in some ways even more outdated than FOIA, because there is not yet a body of judicial and administrative interpretations that clearly establish their applicability to electronic formats and activities, The Sunshine Act requires, for example, that agencies provide adequate public notice of meetings and administrative or regulatory proceedings. The Advisory Committee Act requires that working papers, reports, and other documents be accessible to the public at or before the meeting for which they were prepared. Citizens could use electronic technology to remotely access agendas, schedules, and documents prepared in support of agency rulemaking proceedings or advisory committee meetings. Citizens could provide input electronically via computer conferences and networks, or participate in agency or advisory committee videoconferences.

Congress could revise these and related statutes to clarify the role of electronic technology, and the rights of citizens to use these technologies to participate in governance. Electronic technology also could help citizens provide feedback on what is perceived as right or wrong with government programs and services, including alleged fraud, waste, and abuse. Congressional and executive oversight bodies, including inspectors’ general offices, could accept "whistleblower” input via computer bulletin boards and electronic mail, as well as 1-800 telephone numbers. Advocates believe that the “service” of helping the public know about and access government activities is really an obligation and, indeed, a requirement of democracy.

Electronic access could, on the other hand, raise new legal and constitutional issues about the limits of such citizen participation. The first amendment of the U.S. Constitution affirms the rights of citizens to free speech and to petition the government for redress of grievances. “Electronic” speech and petitioning, for example via computer bulletin boards, should be no different in principle than using mail, telephone calls, or face-to-face meetings. But some local governments and private vendors have been faced with difficult decisions about restricting the content of bulletin boards or computer conferences when electronic speech becomes abusive, obscene, or associated with criminal activity (e.g., drug sales or child pornography). Private vendors can and do enforce reasonable restrictions. Operators of taxpayer-supported bulletin boards, on the other hand, may be more reluctant to infringe on first amendment protections.

Only one of the many government bulletin boards reviewed by OTA has experienced significant problems—the City of Santa Monica, CA, “Public Electronic Network” (PEN). PEN is free to all residents via public terminals in libraries. Some of the computer conferences have included electronic discussion found to be offensive (although not illegal) by various participants and city officials. Inappropriate electronic behavior can be minimized, if not prevented, through education on electronic etiquette, adherence to reasonable rules of electronic exchange, and sanctions for flagrant abuse (e.g., revocation of passwords and limitations on use).

ACCESS TO CONGRESSIONAL INFORMATION

Congress could look for further opportunities to use information technology to improve citizen access to congressional activities. Fair] y extensive pilot testing suggests, for example, that videoconferencing can be cost effective for congressional hearings when witnesses have access to videoconferencing facilities and would otherwise have to

travel to Washington, DC, either at their own or congressional expense.[31] The House of Representatives' leadership has established a task force to move videoconferencing from experimental to operational status; several House committee rooms now are wired for videoconferencing.[32] Videoconferencing also has proven useful for electronic town meetings between Members of Congress in Washington, DC, and citizens back home.

Electronic dissemination of legislative information also has been studied and debated for several years.[33] Local governments have demonstrated that schedules and agendas of city council meetings, and related staff reports, can be provided via simple, low-cost dial-up computer bulletin boards.[34] Several private commercial companies and not-for-profit organizations already disseminate some congressional information via on-line services, computer networks, and compact optical disks. Participants in OTA-sponsored computer conferences expressed considerable interest in electronic access to Congress.[35]

Congress could set up a family of computer bulletin boards that would provide schedules for committee hearings and floor debates, bill status, and witness lists. These could be accessible via both dial-up and networked computers using a wide range of public and private systems. House and Senate computer systems also could be used by interested Members and staff to participate in computer conferences with citizens around the Nation, and to exchange comments on current issues with constituents and others via dial-up remote computer access. Several congressional offices are experimenting with computer net working and bulletin boards.

Videoconferencing and computer bulletin boards for Congress should be technically straightforward and relatively inexpensive to implement. But several specific questions would need attention, including:

1. staffing and training needs;
2. procedures and responsibilities for scheduling videoconferences, and creating and updating the databases;
3. cost sharing and cost recovery;
4. rules to assure open, equitable access; and
5. public/private sector roles and partnerships (including the involvement of the Senate Computer Center, House Information Systems Office, Government Printing Office, and various commercial telecommunication, value-added, and information service providers).[36]

Electronic connections to the public will require changes in the ways individual members of Congress and their staffs, and Congress as an institution, manage and respond to constituent information. This might not require more resources and staff, however. It might even cut costs, given the very large amount of staff time and money already spent on handling constituent mail, telephone calls, and meetings.

---

31 See Stephen Frantzich, "Electronic Service Delivery and Congress, " contractor report prepared for the Office of Technology Assessment, January 1993. Also see Fred B. Wood, Vary T. Coates, Robert L. Chartrand, and Richard F. Ericson, "Videoconferencing Via Satellite: Opening Congress (o the People," The George Washington University Program of Policy Studies in Science and Technology, April 1979.

32 Including th House Committees on Agriculture; Armed Services; Energy and Commerce; Education and Labor; Foreign Affairs; and Science, Space, and Technology.

33 See Frantzich, op. cit., footnote 31; OTA, *Informing the Nation*, op. cit., footnote 28.

34 See, for example, the Pasadena, CA, "Public Access Library System," and the Oakland, CA, "Community Access Project," discussed in OTA, "California Trip Report," Nov. 10, 1992,

35 See Frank Odasz, Big Sky Telegraph, "Computer Conference on Electronic Delivery to Rural/S ma]] Town America," contractor report prepared for the Office of Technology Assessment, Jan, 8, 1993; T.M. Grundner, National Public Telecomputing Network, "The OTA/NPTN Teleforum Project: An Experiment With a Multi-City Electronic Town Hall," contractor report prepared for the Office of Technology Assessment, January 1993.

36 See relevant discussion in later sections of the chapter on "Pricing and Public Access" and "Contracting Out/Procurement"; also see Frantzich, op. cit., footnote 31; OTA, *Informing the Nation*, op. cit, footnote 28; and OTA, *He/ping America Compete*, op. cit.. footnote 28.

Congress, or the Senate and House individually, could establish a legislative branch task force on congressional computer bulletin boards or, more broadly, on congressional electronic service delivery. Given their jurisdiction over congressional computer and telecommunications systems, the Senate Committee on Rules and Administration and House Committee on House Administration could hold hearings, separately or jointly with the Senate Committee on Governmental Affairs and House Committee on Government Operations. These topics might also be addressed by the Joint Committee on the Operations of Congress.

Congress gradually is building the information infrastructure on Capitol Hill that would support electronic service delivery.[37] Ultimately, in addition to scheduling and status information, congressional reports and documents also could be made available electronically. These could include committee reports and hearings, as well as public documents issued by the congressional support agencies—the Congressional Research Service (CRS), Congressional Budget Office (CBO), General Accounting Office (GAO), and Government Printing Office (GPO),[38] in addition to the Office of Technology Assessment (OTA). Several of these congressional agencies (e.g., GPO, GAO, OTA) already are experimenting with electronic dissemination. GPO now has a statutory mandate to provide on-line public access to the *Congressional Record;*[39] this could logically extend to other congressional documents. Taken together, electronic service delivery applications could further open Congress to the people, help Congress better manage its own information, strengthen the role of Congress as the "people's branch of government," and, in the process, set an example for the executive branch and the Nation.

ARCHIVING ELECTRONIC RECORDS

Another important aspect of access is the ability of the public to retrieve historical records and information developed by or for the government. Access to decisionmaking documents is especially important. These materials typically offer one of the few avenues for researchers, historians, and concerned citizens to more fully understand the "whys" and "hews" of Federal actions. The Federal Records Act and related statutes set out requirements for archiving agency documents. Once again, however, these statutes predate the modern electronic era. The Act was amended in 1976 to cover "machine-readable materials," but has not been updated to address the complex challenges and opportunities presented by personal computers, electronic mail, compact optical disks, and computer networking .40

The National Archives and Records Administration (NARA) oversees agency archiving and the operation of various Federal archival centers and activities. NARA is aware of the opportunities and problems presented by electronic technology, and has taken some noteworthy initiatives-establishing a Center for Electronic Records, sponsoring interagency conferences and agreements, and developing manuals and other guidance for agencies on how to archive electronic materials. NARA is working with selected mission agencies in developing procedures for appropriate archiving via optical disk, electronic mail, and computer networking—including Internet. NARA provides

---

[37] Congress is installing a local area fiber optic network that will serve the House, Senate, and congressional support agencies, with gateways to private-sector computer and telecommunication networks.

[38] See the Government Printing Office Electronic Information Access Enhancement Act of 1993, Public Law 103-40.

[39] Ibid.

[40] The term "machine readable materials" was added by the Federal Records Management Amendments of 1976, Sec. 4 (Oct. 21, 1976, 90 Stat. 2723-2727). 44 USC 33 now defines "records" to include "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them."

guidance to agencies on both (a) retaining electronic materials so that they are accessible, readable, etc., whenever the agency needs them (in months or years); and (b) preserving electronic records for future generations under NARA's legal and physical custody.

Some scholars and historians believe that NARA's efforts are still too little, too late. hey feel that the Federal Government is in danger of losing its history because it is failing to capture the rapidly increasing portion of Federal records and decision documents that are created, stored, and sometimes destroyed electronically.[41] Scientists share a related concern that large volumes of scientific data, for example from earth-observing satellites, are stored on obsolete and deteriorating electronic media (i.e., magnetic tapes).[42] Fortunately, newer technologies like optical disks provide viable options for long-term archiving of Federal records and data. NARA has been cautious in its adoption of new technologies due, in part, to concern over rapid technical change and lack of hardware and software standards needed to assure future access. Archival technologies should conform to international technical standards to assure long-term accessibility.

Congress could review and update the Federal Records Act and the role of NARA to ensure that modern information technology is applied and that archiving needs and records management are explicitly addressed in the development of electronic delivery systems.[43] Current NARA guidance calls for an integrated approach.[44] But agency compliance is spotty at best; stronger enforcement appears necessary. NARA cannot be expected to do this alone; cooperation from OMB and the General Services Administration (GSA), among others, is essential.[45] It would help if Congress included NARA in any review of executive branch agencies responsible for governmentwide management, policy, and oversight of electronic service delivery-broadly defined.

DIRECTORIES OF ELECTRONIC SERVICES

If citizens are going to use and benefit from electronic service delivery, they need to first know what services are available and where. OTA research reaffirms the need for directories or, in this case, "electronic road maps" to help citizens identify and locate relevant services. Congress has long recognized this need in mandating a variety of directory services, ranging from the catalog of domestic assistance programs and a Federal information center (run by GSA), to a catalog of Federal research in progress and bibliographic index of technical reports (maintained by the National Technical Information Service (NTIS)), to the catalog of government publications (prepared by GPO). Numerous agencies operate clearinghouses and 1-800 telephone numbers that help direct citizens to a wide variety of services—from grant and loan programs; to education and training; to dissemination of reports and databases.

The mission agencies are adapting to electronic technology by setting up computer bulletin boards, placing directory information on both computer networks and compact optical disks, and participating in interagency efforts to develop

---

[41] See for example, National Academy of Public Administration, *The Effects (#Electronic Recordkeeping on the Historical Record of the U.! Government* (Washington, DC: National Archives and Records Administration, January 1989). NARA gave increased attention to electronic recordkeeping in the 1990s, and has further intensified its electronic initiatives during 1993—but still lags the technology pace being set by many mission agencies and private companies.

[42] See OTA, *Helping Americu Compete*, op. cit. ! footnote 28»

[43] For general discussion, see, for example, Henry H. Perritt, Jr., "Electronic Records Management and Archives," *University of Pittsburgh Law Review, vol.* 53,1992, pp 963–1024; Administrative Conference of the United States, Recommendation 90-5, "Federal Agency Electronic Records Management and Archives," *Federal Register*, vol. *55, No. 250, Dec. 28, 1990*, pp. *5327&53271.*

[44] See for examples, NARA regulations i„36 *CFR* 1 *234,* 10(d) "[the agenc, head shall establish] procedures for addressing records management requirements before approving new electronic records systems or enhancements to existing systems"; and 36 *CFR 1234.22(a)* "Electronic records systems that maintain the official file copy of text documents on electronic media shall provide for the disposition of documents including, when necessary, the requirements for transferring permanent records to NARA."

[45] OMB could check agency compliance when reviewing agency 5-year IRM plans; GSA could do likewise when reviewing agency requests for delegation of procurement authority.

PHOTOS: FRED B. WOOD

Top: One of several dozen microcomputers available to students at the Little Big Horn College.

Bottom: *Little Big Horn College, Crow Indian Reservation, Montana.*

governmentwide directories (e.g., regarding global climate change data or geographic information systems). Many agencies are creating and operating electronic directories entirely inhouse (although frequently with at least some private sector contracting support), while others form partnerships with private sector commercial or not-for-profit organizations, In some cases, private firms develop and market electronic directories on their own initiative if sufficient demand exists.

The complexity of agency activities, combined with the changed economics of information technology, clearly favors decentralized approaches to electronic directories. But this, in turn, increases the need for common standards to ensure both technical interoperability and consistent formatting among directories. Otherwise chaos would result. The trend toward decentralized directories also complicates the roles of agencies responsible for government wide directories that have operated primarily in a centralized mode. For several years, Congress, OMB, agencies, and interested parties have debated the need and options for a governmentwide directory, with considerable disagreement on how to proceed, what technologies to use, and who should be in charge (e.g., OMB, GPO, NTIS, or GSA).[46] This has occurred despite the fact that the Paperwork Reduction Act of 1980 mandated the implementation of a governmentwide Federal Information Locator System (FILS), and that the Paperwork Reduction Reauthorization Amendments of 1986 reaffirmed congressional desire that FILS be fully implemented.[47]

OTA's current and prior research[48] has reaffirmed the need for a publicly accessible locator to Federal services (including information). OTA

---

46 See Charles R. McClure, Ann Bishop, Philip Doty, and Pierrette Bergeron, *Federal Information Inventory-Locator Systems: From Burden to Benefit* (Syracuse, NY: Syracuse University School of Information Studies, 1990).

47 As implemented by OMB during the 1980s, FILS primarily was used to check on agency information collection activities, not to facilitate public access to agency information. For an historical overview, see Gary D. Bass and David Plocher, "Finding Government Information: The Federal Information Locator System (FILS)," *Government Information Quarterly*, vol. 8, No. 1, 1991, pp. 11-32.

48 See OTA, *Helping America Compete*, op. cit., footnote 28, and *Informing the Nation*, op. cit., footnote 28. Also see Fred B. Wood, "Title 44 and Federal Information Dissemination-A Technology and Policy Challenge for Congress: A Viewpoint," *Government Publications* Review, vol. 17, 1990, pp. 1-5.

has concluded that an effective solution would include the following elements:

1. an interagency task force would develop standards for agency-specific and governmentwide directories to Federal services;[49]
2. the task force could be coordinated by NIST or GSA, or perhaps by an existing interagency committee,[50] but would need high-level support from the White House, including OMB and the Office of Science and Technology Policy (OSTP);
3. the task force would need active participation from agency innovators;
4. the task force would recommend consistent formats and compatible software for agency directories;
5. directories would be accessible on a dial-up and networked basis (including wide-area and Internet[51]) and could be downloaded for use in off-line electronic formats, such as compact optical disks, multimedia kiosks, and the like;
6. every Federal executive agency would develop and maintain an electronic directory to its own services (including information services);
7. individual agencies would have discretion in implementing their own directories, so long as the directories meet governmentwide standards;
8. GPO and NTIS would continue to index and catalog government reports and documents, with NTIS concentrating on material of a more technical nature;
9. GPO and NTIS would offer gateway and wide-area directory services[52] (i.e., a "virtual" directory), as well as off-line electronic formats—individual agencies and the private sector could do the same; and
10. agency electronic directories would be accessible via commercial and not-for-profit networks and gateways, and could be downloaded for use in commercial and not-for-profit off-line electronic products.

This approach appears consistent with—but goes beyond—the recently revised OMB Circular A-1 30 and the recently enacted "GPO Electronic Information Access Improvement Act."[53] To implement this scenario, legislative and/or executive action would be needed to: 1) assign primary responsibility for directory development to an interagency task force; 2) direct the development of a two-tier directory system—governmentwide

---

49 The Interagency Committee on Data Management for Global Change and the interagency CENDI committee (Commerce, Energy, NASA, Defense Information) have been working on directory standards for several years.

50 Such as a computer networking committee of the Federal Coordinate ng Committee on Science, Engineering, and Technology; or CENDI, an interagency coordinating committee on scientific and technical information.

51 T. include use of Wide Area Information Server (WAIS) and Gopher software that permits easy electronic access to information and databases at dispersed geographic locations,

52 See Charles R, McClure, William E. Moen, and Joe Ryan, "Design for an Internet-Based Government-Wi& Information Locator System," *Electronic Networking, vol. 2, No. 4,* winter 1992, pp. 6-37; U.S. Government Printing Office, *GPO/2 (Xl 1: Vision for a New Millennium* (Washington, DC: U.S. Government Printing Office, 1992); National Technical Information Service, U.S. Department of Commerce, *NTIS Business Plan* (Washington, DC: NTIS, July 1992). Also see the Government Printing Office Electronic Information Access improvement Act of 1993, Public Law 103-40, that mandates GPO to, among other things, develop an electronic directory to Federal on-line informat ion; and the American Technology Preeminence Act of 1991, Public Law 102-245, that mandates NTIS to study the feasibility of an on-line electronic directory. These Acts clarify the authority of GPO and NTIS to disseminate information in electronic formats, Public Law 102-245 also requires Federal agencies to submit to NTIA in a timely manner all unclassified scientific, technical, and engineering information that results from federally funded research and development, Earlier NTIS and GPO electronic initiatives were delayed in part by debates over privatization of NTIS and the appropriate role of GPO in electronic information dissemination. See OTA, *Informing the Nation,* op. cit., footnote 28; OTA, *Helping America Compete,* op. cit., footnote 28; Wood, "Title 44 and Federal Information Dissemination," op. cit., footnote 48; Fred B. Wood, "Proposals for Privatization of the National Technical Information Service: A Viewpoint," *Government Publications Review, vol. IS, 1988,* pp. 403-409; and Fred B. Wood, "Office of Technology Assessment Perspectives on Current U.S. Federal Information Issues," *Government Publications Review, vol. 17, 1990,* pp. 281-300.

53 Public Law 103-40. Also see Information Infrastructure Task Force, op. cit., footnote 4.

ED WOOD

Microwave and satellite dishes at the University of Alaska at Anchorage.

"gateway" or "virtual" directories, and agency-specific directories; 3) reaffirm that the governmentwide and agency directories will be broadly available in on-line and off-line electronic formats, and that governmentwide directories will complement and not supplant or preempt line agency initiatives; 4) ask the task force to set up a technical support group to develop the necessary directory standards; 5) include representatives of the Depository Library Program, Consumer Information Center, Federal Information Centers, agency clearinghouses, community information and referral centers, and NARA, among others, in the task force work; and 6) establish a framework for oversight and accountability, including at least general milestones for implementation. To assure success, the task force needs to approach this assignment with creativity and flexibility, include users in planning and implementation (see chs. 5 and 6), and build on the rapidly advancing state-of-the-art in directory technology.[54]

PRICING AND PUBLIC ACCESS

The shift to electronic service delivery raises a fundamental issue about the pricing of such services. Some Federal, State, and local government agencies view electronic delivery as an opportunity to recover costs or actually generate net revenues. This would be accomplished by charging users for, in effect, the privilege or convenience of receiving services electronically rather than having to telephone, write, or show up in person at an agency office. The California kiosk system, for example, might charge users extra to renew drivers' licenses at remote locations, presumably since users are saving time (and money) by not having to wait in line at a State office. State and local government use of 1-900 telephone numbers is increasing rapidly as a means to recover costs and pay for system development in financially strapped jurisdictions.[55] Some local governments charge users enough for local land-use information to cover not only the cost of providing information, but the cost of developing the automated system as well.[56] While real estate companies and

[54] This includes, for example, WinWAIS (WAIS using Windows software) available as freeware from the National Clearinghouse for Network Information Discovery and Retrieval; InterNIC (Internet Information Center) for new user orientation and directory services, among others [some individual agencies are establishing their own NICs, e.g., AgriNIC]; and emerging standards for information search and retrieval using low-cost or free software (for more on the Z39.50 standard, contact the U.S. Geological Survey),

[55] 900 charges can approach private sector commercial levels. The Los Angeles County Planning Department, for example, charges 75 cents per minute ($45/hour) for remote computer access to planning commission directives, zoning information, and development proposals. See Brian Miller, "900 Numbers Speed Service," *Government Technology,* January 1993, pp. 8-9.

[56] See Public Technology, Inc., and the Videotex Industry Association, *Local Government Opportunities in Videotex: A Guide to Communicating and Gaining Review Through Electronic Services* (Washington, DC: Public Technology, Inc., 1991); and Patricia T. Fletcher, Stuart I. Bretschneider, and Donald A. Marchand, *Managing Information Technology: Transforming County Governments in the 1990s* (Syracuse, NY: Syracuse University School of Information Studies, August 1992).

developers may be able to afford these charges, local citizen and consumer groups on tight budgets may be placed at a disadvantage.

Charging for electronic delivery creates a potential barrier to access and could create new or aggravate existing inequities. public policy could be based in part on whether electronic delivery is viewed as a luxury or frill or specialized application, or, on the other hand, as a likely major mode of delivery for a growing range of government services. To the extent the Federal Government is shifting to electronic delivery, as appears to be the case, then Congress and the President need to pay careful attention that this shift improves—not impairs-equity of access, Pilot projects suggest that electronic delivery can benefit the economically and educationally disadvantaged, but if the price is too high (or the training inadequate or equipment unavailable) these benefits will not be realized. Also, man y Federal programs strive to reach as many eligible citizens as possible, presumably because of the substantial benefit not only to the recipients, but to society-at-large (e.g., from health, nutrition, training, and education services). From this perspective, it makes little sense to erect price (or other) barriers to electronic delivery for the very persons the programs are intended to benefit.

But electronic delivery does cost money, and various forms of cost- sharing may be reasonable for specific programs and recipients. At present, for example, most users of Federal agency electronic bulletin boards must pay long-distance telecommunication charges themselves, but agencies frequently assess minimal access charges or none at all. This controls the Federal cost and may tend to minimize frivolous use, but it also may discourage legitimate use for those who cannot afford long-distance charges or do not have (or cannot afford) a telephone and computer. The exact cost structure and pricing formula may need to be determined on a case-by-case basis, within an overall framework established by Congress.

To set policy, Congress could use a modified version of the pricing framework developed for Federal information dissemination, As debated over the last several years and embodied in the recently revised OMB Circular A-130, Federal agency pricing may not exceed the marginal cost of dissemination and may be reduced or waived entirely at the discretion of the agency heads' The exact definition of "marginal cost" is still somewhat ambiguous, as is a determination of whether "free" really means zero cost to the user (who may still have to pay for equipment and telecommunications). Congress could direct agency heads, when setting prices, to give priority to assuring equity of access and fulfillment of statutory agency and program goals and that, in any event, the prices should not exceed the marginal cost of electronic service delivery.[58] Congress could specify that pricing should not be used to recover the cost of system design and development, or of the services being delivered, only—at most—the

---

[57] See Office of Management and Budget, Circular A- 130, "Management of Federal Information Resources," Dec. 24, 1985, 50 *Federal Register* 5273052751; OMB, proposed revision of Circular A- 130, 83 *Federal Register* 18296–18306; and final revision, op. cit., footnote 1. Congress may need to clarify that OMB Circular A-25 on "User Charges" does not authorize or require full cost recovery for Federal services intended to benefit the general public, To the contrary, OMB Circular A-130 takes precedence, See Office of Management and Budget, OMB Circular A-25 Revised, "User Charges," *Federal Register,* vol. *58, No, 134,* July 15, 1993, pp. 38 142–38 146. Also see OTA, *Informing the Nation,* op. cit., footnote 28; OTA, *Helping America Compete,* op. cit., footnote 28; Interagency Working Group on Government Electronic Information, "Public Access to Government Electronic Information: A Policy Framework," Aug. 10, 1992, working draft; and U.S. Congress, House, Committee on Government Operations, Subcommittee on Government Information, Justice, and Agriculture, *Creative Ways of Using and Disseminating Federal Information, Hearings,* June 19, 1991, and June 4, 1992. The marginal cost-pricing principle also is reflected in proposed **legislation,** such **as** H R, **629,** the **Improvement of Information** Access Act **of 1993,** Jan, 26, 1993, and S. 681, the Paperwork Reduction Reauthorization Act of 1993, Mar, 31, 1993.

[58] See OTA He/ping *America Compete,* op. cit., footnote 28, Federal agency pricing of information in electronic formats varies widely; the principle of marginal cost pricing appears to be inconsistently or erroneously applied, A 1993 GAO survey, for example, found that agency pricing of CD-ROMs varies from a few dollars per disk to over $1,000 per disk, See U.S. General Accounting Office, *Federal CD-ROM Titles: What Are Available and How They Are Priced,* GAO/IMTEC-93-3-34FS (Washington, DC: U.S. General Accounting Office, 1993).

cost of delivery. This presumes, however, that Federal agencies are adequately funded for technology innovation and system development for electronic delivery.

Congress may need to review policies for those agencies that do not receive adequate funding for system development, such as NTIS. NTIS faces a dilemma—with no appropriated funds, it must charge more than marginal cost (narrowly defined) for some products and services in order to cover the costs of basic archiving activities and product and system development. Congress also might consider authorizing agencies to retain funds received from sale of products and services—so long as pricing and other policies are complied with. At present, agencies must return such funds to the US. Treasury, unless specifically exempted. Agency use of retained funds could be restricted to electronic delivery innovations or other specified purposes, such as subsidies to disadvantaged users.

Effective electronic delivery to economically or educationally disadvantaged users may require not only "free" delivery, but at least partial Federal subsidization of the requisite equipment and training. Federal agencies might offer, for example, to pay part of the cost of kiosk deployment or 1-800 telephone numbers for computer access in distressed areas as part of an intergovernmental partnership or public/private partnership-possibly with telephone, cable, computer networking, or value-added information companies. Or Federal agencies might provide electronic delivery infrastructure grants or vouchers to schools, libraries, and small businesses in disadvantaged areas; these should, of course, be closely coordinated with any agency information technology funds set aside for grassroots involvement, community communication centers, or local innovation.[59]

As part of an electronic service delivery "safety net," Congress also could initiate a review of the roles the Consumer Information Center (CIC) and Depository Library Program (DLP) might play in assuring equity of access. The CIC is operated for GSA by GPO's Superintendent of Documents (SupDocs), and provides copies of free or low priced agency pamphlets and publications to the general public. CIC's potential role in electronic delivery has received little attention to date. The DLP also is operated by SupDocs, and provides copies of selected agency reports to roughly 1,400 designated libraries throughout the United States, at least one in every State and congressional district. The cost of documents provided to depository libraries is covered by agency budgets and/or the DLP direct appropriation, but each library must pay the costs of storing, equipping, and staffing the government documents collection. The DLP serves all citizens, free of charge.

The DLP's role in electronic delivery has been studied and debated for several years. The recently revised OMB Circular A-130 requires Federal agencies to submit all required materials to the DLP, regardless of format, to the maximum extent feasible. Recently enacted legislation clarifies and strengthens GPO's general role in electronic delivery and information dissemination, which also should benefit the DLP. While some DLP policy and funding issues remain, the significant potential role for depository libraries (and libraries in general) in electronic delivery is now well established.[61]

Congress could, as part of any governmentwide electronic delivery initiative, mandate a careful review of all Federal or federally supported programs intended to help assure an access "safety net" for citizens who do not have adequate financial, institutional, or technical resources. The

---

59 See chs. 5 and 6.

60 See Public Law 103-40, op. cit. footnote 52.

61 See John Harris, Alan F. Westin, and Anne L. Finger, Reference Point Foundation, "Innovations for Federal Service: A Study of Innovative Technologies for Federal Government Services to Older Americans and Consumers," contractor report prepared for the Office of Technology Assessment, February 1993; OTA, *Helping America Compete*, op. cit., footnote 28; OTA, *Informing the Nation*, op. cit., footnote 28. Also see OMB, Circular A- 130, op. cit., footnote 1.

review could include not only CIC and DLP, but also the Federal Information Center program run by GSA, the network of U.S. Department of Agriculture (USDA) Extension Service offices, the numerous individual agency clearinghouses and libraries (those run directly by agency personnel and by agency contractors), and various agency, interagency, NTIS, and GPO electronic directory initiatives—all of which could have some role in an electronic service delivery "safety net."

CONTRACTING OUT/PROCUREMENT

As with other Federal activities, some electronically delivered services will be contracted out to the private sector, others will be implemented by the agencies themselves, and still others will proceed in partnerships among Federal agencies, their State/local counterparts, and/or the private sector. Privatizing government activities is a popular although controversial notion. At one extreme, privatization advocates look for opportunities to get the government out of the "business" of providing materials or services that could, in principle, be supplied by the private marketplace. Opponents argue, with some justification, that Congress established many Federal programs to meet important public policy goals that probably would not be met without government involvement and funding. When carefully considered, most privatization proposals to date have focused on contracting out or eliminating current government services. The "reinventing government" theme is drawing more attention to the role of contracting in systems integration and outsourcing of electronic delivery, but it also is spotlighting the growing concern about possible conflicts of interest and over-reliance on contracting.

The OMB Director has initiated a review of current Federal contracting policies and practices, including OMB Circular A-76 on "Performance of Commercial Activities," with particular attention to accountability y, cost effectiveness, and the inherent nature of governmental functions. Congress could evaluate the results of the administration's review, when complete, to determine if the proposed policies better balance the competing principles relevant to electronic delivery, such as:

- Public Responsibility-However implemented, the government in most cases must remain responsible for assuring that electronic delivery meets the goals set by Congress for each service and for electronic delivery generally.
- Equity of Access—An important policy goal is that electronic delivery improve public access to Federal services and broaden public awareness of such services, and that it reduce—not increase—the chasm between socioeconomic "haves" and "have-nots."
- Government Accountability—Some Federal services must be implemented by the government to assure accountability and integrity of the process, provide independent management and oversight, and preclude conflicts of interest.
- Government Efficiency—The public clamor to cut government expenditures and get more "bang" for the tax "buck" does not automatically translate into increased contracting. Contracting out can end up costing the government more money, and, if carried too far, can deny the government the expertise needed to effectively monitor contractors. The most efficient way for agencies to implement electronic delivery usually is outsourcing to commercial providers of computer and telecommunications equipment and networks. But the operation of the delivery system—at least the agency part of the system—may sometimes be done more efficiently by the agency. The determination of the best mode of service delivery must be made on a case-by-case basis.
- Government Competition—Contracting out also minimizes competition between the government and private sector, and can stimulate the private marketplace, At the Federal level, computer and telecommunications equipment is competitively procured. Federal civilian agencies likewise use commercial computer and telecommunication networks almost exclusively, rather than building their own. Agencies typically contract with commercial systems

integrators for the design, implementation, and sometimes operation of the major automated agency systems, Electronic service delivery might raise concerns about government competition with the private sector, to the extent that electronic delivery is similar to operating agency computer centers, clearinghouses, libraries, or information dissemination programs. Privatization of such activities has proven controversial. Some agencies contract out; others do not. The cost effectiveness of contracting these activities is difficult to verify. Agencies rarely conduct follow-up evaluations.

To set a contracting-out policy, the Federal Government could use a modified version of the public-private framework developed for Federal information dissemination.[62] The policy could direct agencies, when planning and implementing electronic delivery, to assure—as first priority—that public accountability, equity of access, and other statutory public policy goals are met. Within that context, the policy could require agencies to: 1) deploy electronic delivery in ways that are cost effective; 2) use commercial off-the-shelf equipment and networks to the extent possible; 3) carefully and creatively consider contracting or partnering roles for the private sector; and 4) assure, whenever the private sector is involved, a level competitive playing field and open access to both the delivery vehicles and the services themselves (to the extent provided or limited by law).

Open access has been a controversial issue with respect to Federal information services. Federal information cannot be copyrighted,[63] but some agencies have used licensing agreements for various purposes, such as: 1) generating revenue to cover the cost of dissemination; 2) limiting or controlling the resale or enhancement of Federal information by private companies; and /or 3) helping assure the quality of the information by enforcing restrictions on allowable reuse or redissemination of the information. Also, Federal technology transfer laws could erode the copyright prohibition if extended to allow agencies to enter into licensing agreements with private companies that restrict access to technical data and software developed by Federal employees.[64]

Consumer, library, and public advocacy groups are concerned about any restrictions on access. Agency proposals to permit copyrighting of federally funded bibliographic and other databases have proven inflammatory. The information industry asks that licensing agreements, when used, be available to any qualified and interested company and that the licensing fee not exceed the marginal cost of providing the information—in order to ensure a level competitive playing field. The practice or plans of some State and local governments to either go into business for themselves or contract with selected private companies to sell public information or other services at a "profit" would raise serious concerns at the Federal level (profit defined as charging more than the marginal cost or, possibly, whatever the market will bear).[65]

Electronic service delivery should, overall, be a net positive sum activity for both the Federal Government and the private sector. A carefully

62 See OMB, proposed and final revisions to Circular A-130, op. cit., footnote 57; OTA, *Helping America Compete*, op. cit., footnote 28.

63 For private information, which can be copyrighted, the intellectual property issues surrounding electronic formats are complex and controversial. For a discussion, see U.S. Congress, Office of Technology Assessment, *Finding A Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change, OTA-TCT-527* (Washington, DC: U.S. Government Printing Office, May 1992).

64 See OTA, *Helping America Compete*, op. cit., footnote 28.

65 A case in point is the Federal Maritime Commission's Automated Tariff Filing and Information System (ATFI). After considerable debate, Congress directed the FMC to collect fees for direct and indirect use of ATFI, in an attempt to generate revenues that would offset phasing down or out the unpopular boat tax. FMC responded with proposed rules that attempt to very tightly control all use of ATFI data, charge ATFI access fees that appear to be higher than marginal cost, and assert that ATFI data are the exclusive property of the FMC. The FMC proposals are strongly opposed by representatives of the information industry, libraries, and public interest and consumer advocates, and conflict with several policy principles in the recently revised and reissued OMB Circular A-130; see OMB, op. cit., footnote 1, Public advocacy groups have raised similar concerns about the Security and Exchange Commission's Electronic Data Gathering and Retrieval System (EDGAR) and the Department of Justice's legal information system (known as JURIS). In both the EDGAR and JURIS cases, the contracting out of information services has led to the imposition of limitations on use and/or high user fees that have had the effect of restricting public access.

crafted policy should simultaneously enhance equity of access to Federal services; improve the productivity and efficiency of Federal service delivery; and stimulate the private sector through direct procurements of off-the-shelf items, contracting out for technology systems and services, and creation of new value-added competitive marketplace opportunities.

Absent improvements in procurement practices, major contracting for electronic service delivery could further strain an already overly complicated, lengthy, rigid, and—some would argue—unnecessarily expensive Federal procurement process. Federal technology managers frequently find themselves locked in by cumbersome procurement practices that leave little room to adapt to technology changes and result in guaranteed early obsolescence of Federal automation programs. Major agency automation initiatives have, in the past, typically taken several years to a decade or more to complete. Procurement strategies that may have worked reasonably well in the 1970s and 1980s are likely to result in automated systems for the 1990s that will be two or three generations of technology behind on the day they become operational. Computer and telecommunication companies general] y prefer that the government define its requirements in functional terms rather than attempting to specify detailed technical designs. This provides greater flexibility to the private sector in creatively responding with proposed technological solutions.

OTA concluded that Federal agencies need to: 1) take advantage of new breakthroughs in less expensive off-the-shelf commercial equipment, software, and services, and the accelerating trend toward interoperable and compatible technologies; 2) find new ways to integrate pilot and demonstration projects, requests for information (RFIs), and requests for proposals (RFPs) that will increase the flexibility and cut the time and cost of Federal information technology procurements; 3) seek creative opportunities for intra- and interagency procurement partnerships that take advantage of the economies of scale and scope made possible through electronic delivery; 4) mandate improvements in the system plans and designs on which the procurements ultimately are based, using evolutionary rather than static procurement strategies; and 5) use information technology to open up competition and cut procurement overhead and red tape.[66]

OTA's vision of Federal procurement practices takes full advantage of information technology *to:*[67]

1. cut the response time for contracting by using electronic bulletin boards and computer networking to announce contract solicitations, and to receive questions and comments; and electronic data interchange (EDI)—with electronic signatures—to receive bids and proposals;
2. cut the cost and paperwork by encouraging all-electronic contracting and electronic filing of contract documents (filing of private sector responses to contract solicitations and agency filing of contract records); and
3. reduce the complexity of contracting through fewer, simpler, streamlined procurement regulations available in a variety of electronic formats.

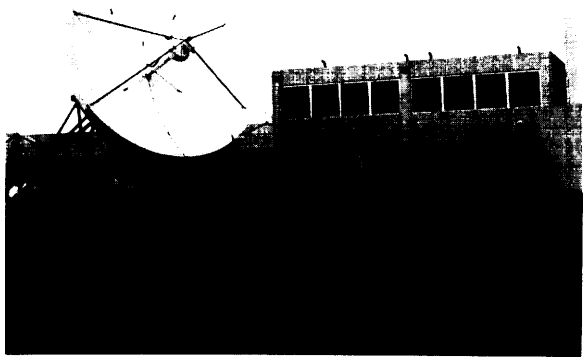
Congress could direct OMB and GSA to review and revise procurement procedures accordingly. Congress could hold periodic oversight hearings on information technology procurement, and, if

---

[66] Based on the results of OTA's own research and on reviews by the Department of Defense and various nongovernmental groups. See, for example, Thomas Giammo, *Managed Evolutionary Development GUIDEBOOK: Process Description and Application* (Arlington, VA: U.S. Patent and Trademark Office, February 1993); Steven Kelman, Jerry Mechling, and John Springett, *Information Technology and Government Procurement: Strategic Issues for the Information Age* (Cambridge, MA: John F. Kennedy School of Government, Harvard University, June 1992); Armed Forces Communications and Electronics Association, "Evolutionary Acquisition Draft Report," Mar. 12, 1993.

[67] The General Services Administration makes some price schedule information available via bulletin board; the Defense Commercial Communications Office places full requests-for-proposals on a bulletin board

PHOTOS: FRED B. WOOD



Top: The 54th Fighter Squadron at Elmendorf Air Force Base, Alaska, depends on telecommunications and computer systems for air traffic control and military intelligence.

Bottom: *One of several satellite earth stations at Elmendorf Air Force Base, Alaska.*

necessary, consider statutory changes and accompanying report language to provide further, stronger guidance (possibly including revisions to the Brooks Act,[68] Competition in Contracting Act,[69] Paperwork Reduction Act,[70] and other Federal procurement statutes).

The transition to electronic procurement, however, raises equity of access issues for smaller businesses and not-for-profit organizations that may not have the expertise, equipment, or resources needed for participation. In this sense, the small-business community faces challenges similar to many government service recipients. Equitable competitive opportunities for small businesses can be furthered by including them in broader grassroots and partnering initiatives designed to help assure equity of access to electronic delivery (see chs. 5 and 6).[71]

TECHNICAL STANDARDS

Electronic service delivery will intensify the need for interoperability among Federal agency computer systems, and compatibility of Federal systems with the commercial telecommunications and computer infrastructure. The economies of scale and scope offered by electronic delivery will be largely lost if Federal agencies (and, where appropriate, their State/local counterparts) cannot use the same kinds of networks and "platforms" (e.g., personal computers, kiosks, ATMs) for getting services to the people.

Common technical standards thus are an essential component of cost-effective electronic delivery, The Federal Government should, to the maximum extent possible, use equipment and systems that incorporate widely accepted private sec-

---

~ Brooks Act of 1%5, Public Law 89-306.

69 Competition in Contracting Act of 1984, Public Law 98-369.

70 Paperwork Reduction Act of 1980, Public Law %-51 1, and **Paperwork Reduction Reauthorization Act of 1986,** Public Law 99-500.

71 For further discussion of business use of information technology for marketing and contracting, see **U.S.** Congress, Office of Technology **Assessment,** *The Electronic Enterprise: Opportunities for American Business and Industry,* in progress. H.R. 2238, the **Federal Acquisition Improvement Act of 1993, introduced May 24, 1993, and** reported out by the House Committee on Government Operations on July 28, 1993, would, among other things, create electronic procurement networks for small purchases, encourage procurement of off-the-shelf products and services, and establish a program to test innovative procurement practices. To assure equitable Federal procurement, the small-business community needs to be a full partner in **these** initiatives. Also see Vice President Gore, op. cit., footnote 4.

tor technical standards, where they exist. Federal procurements of electronic delivery technologies and systems could mandate use of appropriate standards. The computer and telecommunication industries have, in recent years, increasingly recognized that common standards are in their own, as well as the government ‘s, interests. Many computer and telecommunication products and services are on the threshold of becoming mass consumption items, and common technical standards can help further develop the market (e.g., as with CD-ROM or electronic mail standards), Where private sector standards do not yet exist, the Federal Government could exert its influence through the existing public-private standards-setting processes .72

A logical first step at the Federal level (and by extension at the State/local levels) is a careful review of electronic service de] i very as a “system” to identify all relevant technical standards-current and prospective. Standards are needed for: computer networking (and internetworking); electronic mail; videoconferencing; electronic data interchange; smart and hybrid cards and terminals; kiosks; optical disk formats and software; and electronic document and publishing formats, among others.

Congress and the President could designate a lead executive agency, perhaps NIST, for an electronic delivery standards-setting effort. The standards identified then could be mapped into the existing public-private standards structure to determine where: 1) existing standards are satisfactory or need to be modified; 2) standards-setting is underway but should be accelerated; and 3) standards-setting needs to be initiated. NIST could convene forums on electronic delivery technologies, such as kiosks, so that manufacturers, software developers, and users (including Federal users) could collectively identify ways to fill gaps in current standards.

REVISING STATUTES ON SERVICE DELIVERY

Full implementation of electronic delivery would, in many cases, require revision of public laws that establish and define the services being delivered. Widespread electronic benefits transfer, for example, would need clarification of the rights and responsibilities of providers, intermediaries, and recipients of electronic food stamps, WIC food supplements, medical expense reimbursements, and the like. The use of kiosks or home computer terminals for obtaining Federal training services (e.g., from the Department of Labor) or agricultural research services (e g., from the USDA Extension Service) could result in changes in legal definitions of who provides the specified Federal services and how.

Statutory revisions needed to accommodate electronic delivery would be further complicated by pending or planned Federal agency reorganizations. The Secretaries of Agriculture, Education, Labor, and Housing and Urban Development, for example, all have indicated their intent to use information technology as one of the tools for reorganizing their departments. Detailed planning will take months, but any significant changes in the agency and programmatic structures most likely would—and should—affect the deployment of electronic service delivery. Information technology offers many potential opportunities to support agency reorganization and streamlining.

Fine-tuning or revising program and service delivery statutes would, in sum, require consideration of: 1) the current or revised governmentwide information and telecommunication policy statutes that apply to electronic delivery; 2) current or revised statutes and directives that apply to information technology management; 3) pending or planned agency reorganizations; and 4) pending or planned major programmatic changes that would affect the services delivered--electronically *or* otherwise. Making the statutory revisions

---

72 For a general overview of standards-setting processes and options for improvement, see U.S. Congress, Office of Technology Assessment, *Global Standards: Building Blocks for the Future*, OTA-TCT-512 (Washington, DC: U.S. Government Printing Office, March 1992).

necessary to accommodate electronic delivery could be difficult, given the complex set of laws, policies, plans, and directives that may be relevant. In order to expedite the process as much as possible, a policy analysis component could be included in electronic delivery pilot projects and pre-operational tests, as is being done with, for example, the EBT projects and tests sponsored by USDA (see ch. 4).