D Appendix D: Summary of Issues and Options from the 1994 OTA Report

Part of the motivation for the OTA report *Information Security and Privacy in Network Environments* was the recognition that we are in transition to a society that is becoming critically dependent on electronic information and network connectivity. This is exemplified by the explosive growth of the Internet and sources of online information and entertainment.[1]

The need for congressional attention to safeguarding information has been reinforced in the months since the report was issued in September 1994. The use of information networks for business has continued to expand, and ventures to bring electronic commerce and "electronic cash" into homes and offices are materializing rapidly.[2] Government agencies have continued to expand both the scale and scope of their network connectivities. Information technologies and networks are featured even more prominently in plans to make government more efficient, effective, and responsive.[3]

Concerns for the security and privacy of networked information remain. In its 1994 report, OTA found that the fast-changing and competitive marketplace that produced the Internet and a strong networking and software industry in the

---

[1] For example, the number of Internet users has been more than doubling each year; some 30 million people worldwide can exchange messages over the Internet. "Browsing" and "chatting" online at home and in the office is increasingly popular—see, e.g., Molly O'Neill, "The Lure and Addiction of Life On Line," *The New York Times*, Mar. 8, 1995, pp. C1, C6.

[2] See, e.g., Randy Barrett, "Hauling In the Network—Behind the World's Digital Cash Curve," *Washington Technology*, Oct. 27, 1994, p. 18; Neil Munro, "Branch Banks Go Way of the Drive-In," *Washington Technology*, Feb. 23, 1995, pp. 1,48; Amy Cortese et al., "Cashing In on Cyberspace: A Rush of Software Development to Create an Electronic Marketplace," *Business Week*, Feb. 27, 1995, pp. 78-86; Bob Metcalfe, "Internet Digital Cash—Don't Leave Your Home Page Without It," *InfoWorld*, Mar. 13, 1995, p. 55; "Netscape Signs Up 19 Users for Its System of Internet Security," *The Wall Street Journal*, Mar. 20, 1995, p. B3; and Saul Hansell, "VISA Will Put a Microchip in New Cards—Product Is Designed for Small Purchases," *The New York Times*, Mar. 21, 1995, p. D3.

[3] See, e.g., Neil Munro, "Feds May Get New Infotech Executive," *Washington Technology*, Feb. 23, 1995, pp. 1, 49; Charles A Bowsher, Comptroller General of the United States, "Government Reform: Using Reengineering and Technology to Improve Government Performance," GAO/T-OCG-95-2, testimony before the Committee on Governmental Affairs, U.S. Senate, Feb. 2, 1995; and Elena Varon, "Reinventing Is Old Hat for New Chairman," *Federal Computer Week*, Feb. 20, 1995, pp. 22, 27.

United States has not consistently produced products equipped with affordable, user-friendly safeguards. Many individual products and techniques are available to adequately safeguard specific information networks, if the user knows what to purchase and can afford and correctly use the product. Nevertheless, better and more affordable products are needed. In particular, OTA found a need for products that *integrate* security features with other functions for use in electronic commerce, electronic mail, or other applications.

OTA found that more study is needed to fully understand vendors' responsibilities with respect to software and hardware product quality and liability. OTA also found that more study is also needed on the effects of export controls on the domestic and global markets for information safeguards, and on the ability of safeguard developers and vendors to produce more affordable, integrated products. OTA concluded that broader efforts to safeguard networked information will be frustrated unless cryptography-policy issues are resolved.

OTA found that the single most important step toward implementing proper safeguards for networked information in a federal agency or other organization is for top management to define the organization's overall objectives, define an organizational security policy to reflect those objectives, and implement that policy. Only top management can consolidate the consensus and apply the resources necessary to effectively protect networked information. For the federal government, this requires guidance from the Office of Management and Budget (OMB) (e.g., in OMB Circular A-130), commitment from top agency management, and oversight by Congress. The 1994 OTA report found that in practice, there have historically been both insufficient incentives for compliance, as well as insufficient sanctions for noncompliance, with the spirit of the Computer Security Act.

During the course of the OTA assessment (1993-94), there was widespread controversy concerning the Clinton Administration's escrowed-encryption initiative. The significance of this initiative, in concert with other federal cryptography policies, resulted in an increased focus in the report on the processes that the government uses to regulate cryptography and to develop federal information processing standards (FIPS) based on cryptography.

The 1994 report focused on policy issues in three areas: 1) cryptography policy, including federal information processing standards and export controls; 2) guidance on safeguarding unclassified information in federal agencies; and 3) legal issues and information security, including electronic commerce, privacy, and intellectual property. The following sections present the issues and options from that report.

NATIONAL CRYPTOGRAPHY POLICY[4]

The 1994 OTA report concluded that Congress has vital strategic roles in cryptography policy and, more generally, in safeguarding information and protecting personal privacy in a networked society. Because cryptography has become a technology of broad application, decisions about cryptography policy have increasingly broad effects on society. Federal standards (e.g., the federal information processing standards, or the FIPS) and export controls have substantial significance for the development and use of these technologies.

Congressional Review and Open Processes

In 1993, having recognized the importance of cryptography and the policies that govern the development, dissemination, and use of the technology, Congress asked the National Research Council (NRC) to conduct a major study that would support a broad review of cryptography and

[4] See *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC; U.S. Government Printing Office, September 1994), pp. 8-18.

its deployment.[5] An important outcome of this review of national cryptography policy would be the development of more open processes to determine how cryptography will be deployed throughout society. Cryptography deployment includes development of the public-key infrastructures and certification authorities that will support electronic delivery of government services, copyright management, and digital commerce.

The results of the NRC study are expected to be available in 1996. But, given the speed with which the Clinton Administration is acting to deploy escrowed encryption within the government, OTA concluded that information to support a congressional policy review of cryptography is out of phase with implementation. Therefore, OTA noted that:

OPTION: Congress could consider placing a hold on further deployment of key-escrow encryption, pending a congressional policy review.

More open processes would build trust and confidence in government operations and leadership. More openness would allow diverse stakeholders to understand how their views and concerns were being balanced with those of others, in establishing an equitable deployment of these technologies, even when some of the specifics of the technology remain classified. (See also the policy section below on safeguarding information in federal agencies.) More open processes would also allow for public consensus-building, providing better information for use in congressional oversight of agency activities. Toward these ends, OTA noted that:

OPTION: Congress could address the extent to which the current working relationship between NIST and NSA will be a satisfactory part of this open process, or the extent to which the current arrangements should be reevaluated and revised.

Another important outcome of a broad policy review would be a clarification of national information-policy principles in the face of technological change:

OPTION: Congress could state its policy as to when the impacts of a technology (like cryptography) are so powerful and pervasive that legislation is needed to provide sufficient public visibility and accountability for government actions.

During the assessment, OTA found that many of the persistent concerns surrounding the Escrowed Encryption Standard, and the Clinton Administration's escrowed-encryption initiative generally, focused on whether key-escrow encryption will become mandatory for government agencies or the private sector, if nonescrowed encryption will be banned, and/or if these actions could be taken without legislation. Other concerns still focus on whether or not alternative forms of encryption would be available that would allow private individuals and organizations the *option* of depositing keys (or not) with one or more third-party trustees—at *their* discretion. The National Research Council study should be valuable in helping Congress to understand the broad range of technical and institutional alternatives available for various types of trusteeships for cryptographic keys, "digital powers of attorney," and the like. However, if implementation of the EES and related technologies continues at the current pace, OTA noted that key-escrow encryption may already be embedded in information systems before Congress can act on the NRC report.

Export Controls on Cryptography

As part of a broad national cryptography policy, OTA noted that Congress may wish to periodically examine export controls on cryptography, to ensure that these continue to reflect an appropriate balance between the needs of signals intelligence and law enforcement and the needs of the public and business communities. This examination would take into account changes in foreign capabilities and foreign availability of cryptographic technologies.

[5] For information about the NRC study, contact Herb Lin at the National Research Council (crypto@nas.edu).

Information from an executive branch study of the encryption market and export controls that was promised by Vice President Gore should provide some near-term information.[6] At this writing, the Commerce Department and the National Security Agency (NSA) are assessing the economic impact of U.S. export controls on the U.S. computer software industry; as part of this study, NSA is determining the foreign availability of encryption products.[7] The study is scheduled to be delivered to National Security Council (NSC) deputies by July 1, 1995. It is anticipated that there will be both unclassified and classified portions of the study; there may be some public release of the unclassified material.[8]

OTA noted that the scope and methodology of the export-control studies that Congress might wish to use in the future may differ from those used in the executive branch study. Therefore:

OPTION: Congress might wish to assess the validity and effectiveness of the Clinton Administration's studies of export controls on cryptography by conducting oversight hearings, by undertaking a staff analysis, or by requesting a study from the Congressional Budget Office.

Congressional Responses to Escrowed-Encryption Initiatives

OTA also recognized that Congress also has a more near-term role to play in determining the extent to which—and how—the Escrowed Encryption Standard (EES) and other escrowed-encryption systems will be deployed in the United States. These actions can be taken within a long-term, strategic framework. Congressional oversight of the effectiveness of policy measures and controls can allow Congress to revisit these issues as needed, or as the consequences of previous decisions become more apparent.

The Escrowed Encryption Standard (Clipper) was issued as a voluntary FIPS; use of the EES by the private sector is also voluntary. The Clinton Administration has stated that it has no plans to make escrowed encryption mandatory, or to ban other forms of encryption. But, absent legislation, these intentions are not binding for future administrations and also leave open the question of what will happen if the EES and related technologies do not prove acceptable to the private sector. Moreover, the executive branch may soon be using the EES and/or related escrowed-encryption technologies to safeguard—among other things—large volumes of private information about individuals (e.g., taxpayer data and health care information).

For these reasons, OTA concluded that the EES and other key-escrowing initiatives are by no means only an executive branch concern. The EES and any subsequent escrowed-encryption standards (e.g., for data communications in computer networks, or for file encryption) also warrant congressional attention because of the public funds that will be spent in deploying them. Moreover, negative public perceptions of the EES and the processes by which encryption standards are developed and deployed may erode public confidence and trust in government and, consequently, the effectiveness of federal leadership in promoting responsible safeguard use.

In responding to current escrowed-encryption initiatives like the EES, and in determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies, OTA noted that:

OPTION: Congress could address the appropriate locations of the key-escrow agents, particularly for federal agencies, before additional investments are made in staff and facilities for them. Public acceptance of key-escrow encryption might be improved—but not assured—by an escrowing system that used separation of powers to reduce perceptions of the potential for misuse.

---

[6] Vice President Al Gore, letter to Representative Maria Cantwell, July 20, 1994. See OTA, op. cit., footnote 4, pp. 11-13.

[7] Maurice Cook, Bureau of Export Administration, Economic Analysis Division, personal communication, Mar. 7, 1995.

[8] Bill Clements, National Security Council, personal communication, Mar. 21, 1995.

With respect to current escrowed-encryption initiatives like the EES, as well as any subsequent key-escrow encryption initiatives (e.g., for data communications or file encryption), and in determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies, OTA noted that:

OPTION: Congress could address the issue of criminal penalties for misuse and unauthorized disclosure of escrowed key components.

OPTION: Congress could consider allowing damages to be awarded for individuals or organizations who were harmed by misuse or unauthorized disclosure of escrowed key components.

SAFEGUARDING INFORMATION IN FEDERAL AGENCIES[9]

Congress has an even more direct role in establishing the policy guidance within which federal agencies safeguard information, and in oversight of agency and OMB measures to implement information security and privacy requirements. The Office of Management and Budget is responsible for developing and implementing government-wide policies for information resource management; for overseeing the development and promoting the use of government information-management principles, standards, and guidelines; and for evaluating the adequacy and efficiency of agency information-management practices. During the assessment, OTA found that information-security managers in federal agencies must compete for resources and support to properly implement needed safeguards. For their efforts to succeed, both OMB and top agency management must fully support investments in cost-effective safeguards. Given the expected increase in interagency sharing of data, interagency coordination of privacy and security policies is also necessary to ensure uniformly adequate protection.

Effectiveness of OMB Guidance

The Paperwork Reduction Act of 1995 was signed by President Clinton on May 22, 1995. Both the House (H.R. 830) and Senate (S. 244) versions of the bill reaffirmed OMB's authorities under the Computer Security Act for safeguarding unclassified information. The conference bill[10] containing these provisions passed in both Houses on April 6, 1995 (see chapter 4 of this background paper for discussion).

Appendix III ("Security of Federal Automated Information Systems") of the 1985 version of OMB Circular A-130 set forth OMB's government-wide policy guidance for information security. *At this writing, a new, proposed revision of Appendix III has just been issued.* The proposed revision is intended to lead to improved federal information-security practices and to make fulfillment of Computer Security Act and Privacy Act requirements more effective generally, as well as with respect to data sharing and secondary uses.

The new, proposed revision of Appendix III ("Security of Federal Automated Information") will be key to assessing the prospect for improved federal information security practices. The proposed revision was presented for comment at the end of March 1995. According to OMB, the proposed new government-wide guidance:

> . . . is intended to guide agencies in securing information as they increasingly rely on an open and interconnected National Information Infrastructure. It stresses management controls such as individual responsibility, awareness and training, and accountability, rather than technical controls. . . The proposal would also better integrate security into program and mission goals, reduce the need for centralized reporting of paper security plans, emphasize the management of risk rather

---

[9] See OTA, op. cit., footnote 4, pp. 18-20.

[10] See U.S. Congress, House of Representatives, "Paperwork Reduction Act of 1995—Conference Report to Accompany S.244," H.Rpt. 104-99, Apr. 3, 1995. These provisions are found in 44U.S.C. section 3504.

than its measurement, and revise government-wide security responsibilities to be consistent with the Computer Security Act.[11]

See chapter 4 of this background paper for discussion of the proposed revision to Appendix III. The issues and options presented below are in the context of the 1994 report and the 1985 Appendix III. However, OTA expects that congressional oversight and analysis as indicated below will remain useful for understanding OMB's new guidance and assessing its potential effectiveness.

Because the revised Appendix III had not been issued by the time *Information Security and Privacy in Network Environments* was completed in 1994, the OTA report was unable to assess the revision's potential for improving information security in federal agencies, for holding agency managers accountable for security, or for ensuring uniform protection in light of data sharing and secondary uses. OTA noted that, after the revised Appendix III of OMB Circular A-130 is issued:

OPTION: Congress could assess the effectiveness of the OMB's revised guidelines, including improvements in implementing the Computer Security Act's provisions regarding agency security plans and training, in order to determine whether additional statutory requirements or oversight measures are needed.

This might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the General Accounting Office (GAO). However, the effects of OMB's revised guidance may not be apparent for some time after the revised Appendix III is issued.

Therefore, a few years may pass before GAO is able to report government-wide findings that would be the basis for determining the need for further revision or legislation. In the interim:

OPTION: Congress could gain additional insight through hearings to gauge the reaction of agencies, as well as privacy and security experts from outside government, to OMB's revised guidelines.

Oversight of this sort might be especially valuable for agencies, such as the Internal Revenue Service, that are developing major new information systems. In the course of its oversight and when considering the direction of any new legislation, OTA noted that:

OPTION: Congress could ensure that agencies include explicit provisions for safeguarding information assets in any information-technology planning documents.

OPTION: Congress could ensure that agencies budget sufficient resources to safeguard information assets, whether as a percentage of information-technology modernization and/or operating budgets, or otherwise.

OPTION: Congress could ensure that the Department of Commerce assigns sufficient resources to the National Institute of Standards and Technology (NIST) to support its Computer Security Act responsibilities, as well as NIST's other activities related to safeguarding information and protecting privacy in networks.

Regarding NIST's computer-security budget, OTA did not determined the extent to which additional funding is needed, or the extent to which additional funding would improve the overall effectiveness of NIST's information-security activities. However, in staff discussions and workshops during the course of the assessment, OTA found that individuals from outside and within government repeatedly noted that NIST's security activities were not proactive and that NIST often lagged in providing useful and needed standards (the FIPS) and guidelines. Many individuals from the private sector felt that NIST's limited resources for security activities precluded NIST from doing work that would also be useful to industry. Additional resources, whether from overall increases in NIST's budget or otherwise, could enhance

[11] Office of Management and Budget, "Security of Federal Automated Information," Proposed Revision of OMB Circular No. A-130 Appendix III (transmittal memorandum), At this writing, the proposed revision of Appendix III was available from NIST via World Wide Web at http://csrc.ncsl.nist.gov/secplcy as <a130app3.txt>.

NIST's technical capabilities, enable it to be more proactive, and hence be more useful to federal agencies and to industry.

OTA found that NIST activities with respect to standards and guidelines related to cryptography are a special case, however. Increased funding alone will not be sufficient to ensure NIST's technological leadership or its fulfillment of the "balancing" role as envisioned by the Computer Security Act of 1987. With respect to cryptography, OTA concluded that national security constraints set forth in executive branch policy directives appear to be binding. These constraints have resulted, for example, in the closed processes by which the Escrowed Encryption Standard (Clipper) was developed and implemented. Increased funding could enable NIST to become a more equal partner to NSA, at least in deploying (if not developing) cryptographic standards. But, if NIST/NSA processes and outcomes are to reflect a different balance of national security and other public interests, or more openness, than has been evidenced over the past five years, OTA concluded that clear policy guidance and oversight (not just funding) will be needed.

LEGAL ISSUES AND INFORMATION SECURITY

The laws currently governing commercial transactions, data privacy, and intellectual property were largely developed for a time when telegraphs, typewriters, and mimeographs were the commonly used office technologies and business was conducted with paper documents sent by mail. Technologies and business practices have dramatically changed, but the law has been slower to adapt. Computers, electronic networks, and information systems are now used to routinely process, store, and transmit digital data in most commercial fields. OTA found that changes in communication and information technologies were particularly significant in three areas: electronic commerce, privacy and transborder data flow, and digital libraries.

Electronic Commerce

As businesses replace conventional paper documents with standardized computer forms, the need arises to secure the transactions and establish means to authenticate and provide *nonrepudiation services for electronic transactions*, that is, a means to establish authenticity and certify that the transaction was made. Absent a signed paper document on which any nonauthorized changes could be detected, a *digital signature* to prevent, avoid, or minimize the chance that the electronic document has been altered must be developed. In contrast to the courts' treatment of conventional, paper-based transactions and records, little guidance is offered as to whether a particular safeguard technique, procedure, or practice will provide the requisite assurance of enforceability in electronic form. This lack of guidance concerning security and enforceability is reflected in the diversity of security and authentication practices used by those involved in electronic commerce.

Legal standards for electronic commercial transactions and digital signatures have not been fully developed, and these issues have undergone little review in the courts. Therefore, OTA noted that immediate action by Congress might not be warranted.[12] However, OTA noted the need for congressional awareness of these issues:

OPTION: Congress could monitor the issue of legal standards for electronic transactions and digital signatures, so that these are considered in future policy decisions about information security.

Such attention would be especially timely, given the increasing focus of the national and international legal communities and the states on developing legal standards for electronic commerce, as well as guidelines and model legislation for digital signatures.

[12] Note this refers to *legal* standards for contracts, rules of evidence, and so forth, not to specific *technical* standards like the DSS.

For example, the American Bar Association's (ABA) Information Security Committee, Science and Technology Section, is drafting "Global Digital Signature Guidelines and model legislation. The ABA effort includes federal-agency representatives, as well as representatives from the private sector and other governments. With participation by the International Chamber of Commerce and the U.S. State Department, the United Nations Commission on International Trade Law has completed a Model Law on electronic data interchange (EDI).[13]

Utah has just enacted digital signature legislation. The Utah Digital Signature Act[14] is intended to provide a reliable means for signing computer-based documents and to provide legal recognition of digital signatures using "strong authentication techniques" based on asymmetric cryptography. To assure a minimum level of reliability in digital signatures, the Utah statute provides for the licensing and regulation of certification authorities by a "Digital Signature Agency" (e.g., the Division of Corporations and Commercial Code of the Utah Department of Commerce). The act, first drafted as a proposed model law, provides that the private key is the property of the subscriber who rightfully holds it (and who has a duty to keep it confidential); thus, tort or criminal actions are possible for theft or misuse. It is technology-independent; that is, it does not mandate use of a specific signature technique, although it envisions use of signatures based on standards similar to or including the ANSI X.9.30 or ITU X.509 standards.[15] (Also see discussion in chapter 4 of this background paper.)

Liability issues are also important to the development of electronic commerce and the underpinning institutional infrastructures, including (but not limited to) escrow agents for key-escrowed encryption systems and certificate authorities for public-key infrastructures. Widespread use of certificate-based, public-key infrastructures will require resolution and harmonization of liability requirements for trusted entities, whether these be federal certificate authorities, private certificate (or "certification") authorities, escrow agents, banks, clearinghouses, value-added networks, or other entities.[16]

Protection of Privacy in Data

Since the 1970s, the United States has concentrated its efforts to protect the privacy of personal data collected and archived by the federal government. Rapid development of networks and information processing by computer now makes it possible for large quantities of personal information to be acquired, exchanged, stored, and matched very quickly. As a result, a market for computer-matched personal data has expanded rapidly, and a private sector information industry has grown around the demand for such data.

OTA found that increased computerization and linkage of information maintained by the federal

---

[13] Information on ABA and United Nations activities provided by Michael Baum, Principal, Independent Monitoring, personal communication, Mar. 19, 1995. See also Michael S. Baum, *Federal Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures*, NIST-GCR-94-654, NTIS Doc. No. PB94-191-202 (Springfield, VA: National Technical Information Service, 1994).

[14] Utah Digital Signature Legislative Facilitation Committee, "Utah Digital Signature Legislation," Dec. 21, 1994. The Utah Digital Signature Act act was signed into law on Mar. 10, 1995, as section 46-3-101 et seq., Utah Code Annotated. (Prof. Lee Hollaar, University of Utah, personal communication, Mar. 22, 1995.)

[15] Utah Digital Signature Act, ibid. The model legislation was endorsed by the American Bar Association, Information Security Committee of the Science and Technology Section, EDI/Information Technology Division; Prof. Lee Hollaar, University of Utah; Salt Lake Legal Defenders Assoc.; Statewide Association of Public Attorneys; Utah Attorney General's Office; Utah Dept. of Corrections; Utah Information Technology Commission; Utah Judicial Council; and Utah State Tax Commission.

[16] See Michael Baum, op. cit., footnote 12 for discussion of liability exposure, legal considerations, tort and contract remedies, government consent to be liable, and recommendations and approaches to mitigate liability.

government is arguably not addressed by the Privacy Act, which approaches privacy issues on an agency-by-agency basis. To address these developments, OTA noted several alternatives:

OPTION: Congress could allow each agency to address privacy concerns individually, through its present system of review boards.

OPTION: Congress could require agencies to improve the existing data integrity boards, with a charter to make clearer policy decisions about sharing information and maintaining its integrity.

OPTION: Congress could amend the existing law to include provisions addressing the sharing and matching of data, or restructure the law overall to track the flow of information between institutions.

OPTION: Congress could provide for public access for individuals to information about themselves, and protocols for amendment and correction of personal information. It could also consider providing for online publication of the Federal Register *to improve public notice about information collection and practices.*

OTA noted that, in deciding between courses of actions, Congress could exercise its responsibility for oversight through hearings and/or investigations, gathering information from agency officials involved in privacy issues, as well as citizens, in order to gain a better understanding of what kinds of actions are required to implement better custodianship, a minimum standard of quality for privacy protection, and notice to individuals about use and handling of information.

Although the United States does not comprehensively regulate the creation and use of such data in the private sector, foreign governments (particularly the European Union) do impose controls. The Organization for Economic Cooperation and Development (OECD) adopted guidelines in 1980 to protect the privacy and transborder flows of personal data. The difference between the level of personal privacy protection in the United States and that of its trading partners, who in general more rigorously protect privacy, could inhibit the exchange of data with these countries. U.S. business has some serious concerns about the European Union (EU) proposal, as it relates to the data subject's consent and the transfer of data to non-EU countries. OTA noted that Congress had a choice when addressing the sufficiency of existing U.S. legal standards for privacy and security in a networked environment for the private sector:

OPTION: Congress could legislate to set standards similar to the OECD guidelines;

or,

OPTION: Congress could allow individual interests, such as the business community, to advise the international community on its own of its interests in data protection policy. However, because the EU's protection scheme could affect U.S. trade in services and could impact upon individuals, Congress may also wish to monitor and consider the requirements of foreign data protection rules as they shape U.S. security and privacy policy to assure that all interests are reflected.

OTA noted that a diversity of interests must be reflected in addressing the problem of maintaining privacy in computerized information—whether in the public or private sector. To deal with this, OTA noted that:

OPTION: Congress could establish a Federal Privacy Commission.

Proposals for such a commission or board were previously discussed by OTA in its 1986 report *Electronic Record Systems and Individual Privacy.* In that study, OTA cited the lack of a federal forum in which the conflicting values at stake in the development of federal electronic systems could be fully debated and resolved. As privacy questions will arise in the domestic arena, as well as internationally, a commission could deal with these as well.

Protection of Intellectual Property in the Administration of Digital Libraries

OTA found that the availability of protected intellectual property in *digital libraries* and other networked information collections is straining the traditional methods of protection and payment for use of intellectual property. Technologies (like digital signatures and encryption) developed for safeguarding information might also hold promise for monitoring the use of copyrighted informa-

tion and facilitating means for collecting royalties and compensating the copyright holders. The application of intellectual-property law to protect works maintained in digital libraries continues to be problematic; traditional copyright concepts such as *fair use* are not clearly defined as they apply to these works; and the means to monitor compliance with copyright law and to distribute royalties is not yet resolved.

OTA had addressed these legal and institutional issues in an earlier report, *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change*. The 1992 report included several options to deal with the use of works in electronic form.

During the 1994 assessment, OTA found that the widespread development of multimedia authoring tools—integrating film clips, images, music, sound, and other content—raises additional issues pertaining to copyright and royalties. With respect to copyright for multimedia works, OTA noted that:

OPTION: Congress could allow the courts to continue to define the law of copyright as it is applied in the world of electronic information;

or,

OPTION: Congress could take specific legislative action to clarify and further define the copyright law in the world of electronic information.

Instead of waiting for legal precedents to be established or developing new legislation, OTA noted that Congress might try a third approach that would allow producer and user communities to establish common guidelines for use of copyrighted, multimedia works:

OPTION: Congress could allow information providers and purchasers to enter into agreements that would establish community guidelines without having the force of law. In so doing, Congress could decide at some point in the future to review the success of such an approach.

More generally, with respect to private sector solutions for problems concerning rights and royalties for copyrighted works in electronic form, OTA noted that:

OPTION: Congress could encourage private efforts to form rights-clearing and royalty-collection agencies for groups of copyright owners.

Alternatively,

OPTION: Congress might allow private sector development of network tracking and monitoring capabilities to support a fee-for-use basis for copyrighted works in electronic form.

In the latter case, Congress might wish to review whether a fee-for-use basis for copyrighted works in electronic form is workable, from the standpoint of both copyright law and technological capabilities. OTA suggested that this might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the Copyright Office.