September 1994

****
* OTA REPORT SUMMARY *
*
* INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS *
****

The technology used in daily life is changing. Information technologies are transforming the ways we create, gather, process, and share information; electronic transactions and records are becoming central to everything from commerce to health care. Computer networking is driving many of these changes. The explosive growth of the Internet the number of users more than doubles each year exemplifies this transition to a networked society. According to the Internet Society, as of July 1994 the Internet linked over 3 million host computers in more than 75 countries; some 20 to 30 million people worldwide can exchange messages over the Internet.

The use of information networks for business, in particular, is expanding enormously; government use of networks features prominently in plans to make government more efficient, effective, and responsive. But the transformation brought about by networking also raises new concerns for the security and privacy of networked information. If these concerns are not properly resolved, they threaten to limit networking's full potential, in terms of both participation and usefulness.

The OTA report Information Security and Privacy in Network Environments was requested by the Senate Committee on Governmental Affairs and the House Subcommittee on Telecommunications and Finance. The report focuses on safeguarding unclassified information in networks, not on the security or survivability of networks themselves, or on the reliability of network services to ensure information access. OTA's analysis examines 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.

Information safeguards, especially those based on cryptography, are becoming increasingly important. Appropriate safeguards (countermeasures) must account for and anticipate technical, institutional, and social changes that increasingly shift responsibility for safeguarding information to the end users. Broader efforts to safeguard networked information will be frustrated unless cryptography-policy issues are resolved.

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, formulate 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 (e.g., in OMB Circular A-130), commitment from top agency management, and oversight by Congress.

POLICY ISSUES

Cryptography Policy

Congress has a vital role in formulating national cryptography policy and in determining how we safeguard information and protect personal privacy in our networked society. Cryptography has become a fundamental technology with broad applications. Decisions about cryptography policy will affect the everyday lives of most Americans because cryptography will help ensure the confidentiality and integrity of health records and tax returns. It will help speed the way to electronic commerce, and it will help us manage copyrighted material in electronic form.

Despite two decades of growth in nongovernmental research and development, the federal government still has the most expertise in cryptography. The nongovernmental market for cryptography products has grown in the last 20 years or so, but is still developing. Thus, export controls and the federal information processing standards (FIPS) developed by the Commerce Department's National Institute of Standards and Technology (NIST) have substantial impact on the development and use of information safeguards based on cryptography. In its activities as a developer, user, and regulator of safeguard technologies, the federal government faces a fundamental tension between two important policy objectives: 1) fostering the development and widespread use of cost-effective information safeguards, and 2) controlling the proliferation of safeguard technologies that can impair U.S. signals-intelligence and law-enforcement capabilities. This tension is evident in concerns about the proliferation of cryptography that could impair U.S. signals intelligence and law enforcement, and in the resulting struggle to control cryptography through use of federal standards and export controls.

Previously, control of the availability and use of cryptography was presented as a national-security issue focused outward, with the intention of maintaining a U.S. technological lead over other countries. Now, with an increasing policy focus on domestic crime and terrorism, the

availability and use of cryptography has also come into prominence as a domestic-security, law-enforcement issue. Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives intended to preserve U.S. law-enforcement and signals-intelligence capabilities.

Policy debate over cryptography used to be as arcane as the technology itself. However, as the communications technologies used in daily life have changed, concern over the implications of privacy and security policies dominated by national security objectives has grown dramatically, particularly in business and academic communities that produce or use information safeguards, but among the general public as well. This concern is reflected in the ongoing debates over key-escrow encryption and the government's Escrowed Encryption Standard (EES).

The Clinton Administration announced the "escrowed-encryption" initiative (often referred to as "Clipper" or the "Clipper chip") in April 1993. The EES uses a classified algorithm developed by the National Security Agency (NSA). The Department of Commerce issued the EES as a federal information processing standard for encrypting unclassified information in February 1994. The escrowed-encryption initiative in general and the EES in particular have been met with intense public criticism and concern: the EES has not yet been embraced within government and is largely unpopular outside of government. The controversy and unpopularity stem in large part from privacy concerns and the fact that users' cryptographic keys will be held by government-designated "escrow agents" (currently, within the Departments of Commerce and Treasury). Other concerns regarding the EES and its implementation include the role of NSA in the escrowed-encryption initiative and in NIST's standards development, the use of a classified algorithm in the standard, the requirement that the standard be implemented in hardware (not software), the possibility of key-escrow encryption being made mandatory in the future, and the general secrecy and closed processes surrounding the Clinton Administration's escrowed-encryption initiative.

Recognizing the importance of cryptography and the policies that govern the development, dissemination, and use of the technology, Congress has asked the National Research Council (NRC) to conduct a major study that would support a broad review of cryptography. (See footnote 1.) The OTA report presents several options for congressional consideration in the course of a strategic policy review. Because information to support a congressional review of cryptography is out of phase with the government's implementation of key-escrow encryption (the NRC report is expected to be completed in 1996), one option would be to place a hold on further deployment of key-escrow encryption, pending a congressional policy review.

An important outcome of a broad review of national cryptography policy would be the development of more open processes to determine how cryptography will be deployed throughout society in support of electronic delivery of government services, copyright management, and digital commerce. More open processes would build trust and confidence in government operations and leadership, as well as allow for public consensus-building, providing better information for use in congressional oversight of agency activities. As part of a broad national cryptography policy, Congress could also 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.

Congress also has a more near-term role to play in determining the extent to which and how the Escrowed Encryption Standard and other types of key-escrow encryption 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 OTA report presents immediate options for Congress in responding to current escrowed-encryption initiatives like the EES, as well as for determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies. These options include addressing the appropriate choice of escrow agents, as well as establishing criminal penalties for misuse and unauthorized disclosure of escrowed key components and allowing damages to be awarded to individuals or organizations who were harmed by misuse or unauthorized disclosure of escrowed key components.

****
* Safeguarding Information in Federal Agencies *
****

Congress has a direct role in establishing the policy guidance within which federal agencies safeguard information, and in oversight of agency and Office of Management and Budget (OMB) measures to implement information security and privacy requirements. OMB is responsible for: 1) developing and implementing government-wide policies for information resource management; 2) overseeing the development and promoting the use of government information-management principles, standards, and guidelines; and 3) evaluating the adequacy and efficiency of agency information-management practices. 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.

The forthcoming revision of Appendix III of OMB Circular A-130 is intended to improve federal information-security practices. To the extent that the revised Appendix III facilitates more uniform treatment across agencies, it can also make fulfillment of Computer Security Act and Privacy Act requirements more effective with respect to data sharing and secondary uses. The revised Appendix III had not been issued by the time this report was completed. Therefore, OTA was unable to assess the revision's potential for improving information security in federal agencies. The report offers options for Congress in determining the effectiveness and adequacy of OMB's guidelines and the need for additional legislative guidance. Topics to be addressed in the course of oversight and when considering the direction of any new legislation would include ensuring that: 1) agencies include explicit provisions for safeguarding information assets in any information-technology planning documents; 2) agencies budget sufficient resources to safeguard information assets, whether as a percentage of information-technology modernization and/or operating budgets, or otherwise; and 3) the Department of Commerce assigns sufficient resources to NIST to support its Computer Security Act responsibilities, as well as NIST's other activities related to safeguarding information and protecting privacy in networks.

Congress may also wish to address the working relationship of NIST and the National Security Agency in implementing the Computer Security Act of 1987 (P.L. 100-235). The act gives NIST (then the National Bureau of Standards) final authority for developing government-wide standards and guidelines for safeguarding unclassified, sensitive information, and for developing government-wide security training programs. Implementation of the Computer Security Act has been controversial, particularly regarding the roles of NIST and NSA in standards development; a 1989 memorandum of understanding between the two agencies appears to cede more authority to NSA than the act had granted or envisioned.

****
* Legal Issues and Information Security *
****

Laws evolve in the context of the cultural mores, business practices, and technologies of the time. 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 routinely to process, store, and transmit digital data in most commercial fields. Changes in communication and information technologies are 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 must be developed to prevent, avoid, or minimize the chance that the electronic document has been altered. 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 is reflected in the diversity of security and authentication practices used by those involved in electronic commerce. Although Congress may wish to monitor this issue, the time is not yet ripe for legislative action.

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, the market for computer-matched personal data has expanded rapidly, and a private-sector information industry has grown around the demand for such data.

Increased computerization and linkage of information maintained by the federal government is arguably not addressed by the Privacy Act, which approaches privacy issues on an agency-by-agency basis. 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 difference between the level of personal privacy protection in the United States and that of its trading partners, who in general protect privacy more rigorously, could inhibit the exchange of data with these countries. The OTA report offers a range of options for dealing with privacy issues in the public and private sectors, ranging from continuing to

allow federal agencies to manage privacy on an individual basis to establishing a Federal Privacy Commission.

****
* Protection of Intellectual Property in the *
* Administration of Digital Libraries *
****

The availability of protected intellectual property in networked information collections, such as digital libraries and other digital information banks, is placing a strain on the traditional methods of protection and payment for use of intellectual property. Technologies developed for securing information might also hold promise for monitoring the use of copyrighted information and for providing a means to collect royalties and compensate the copyright holders. The application of intellectual-property law to protect material in electronic form continues to be problematic, especially for mixed-media (multimedia) works; 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 also addressed these issues in 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).

During the current 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. Two options for dealing with copyright for multimedia works would be to allow the courts to continue to define the law of copyright as it is applied in the world of electronic information, or to take specific legislative action to clarify and further define the copyright law. A third approach would allow producer and user communities to establish common guidelines for use of copyrighted, multimedia works. More generally, Congress could encourage private efforts to form rights-clearing and royalty-collection agencies for groups of copyright holders or allow private-sector development of network tracking and monitoring capabilities to support a fee-for-use basis for copyrighted works in electronic form.

1. The NRC study was included in the Defense Authorization Act for FY 1994 (Public Law 103-160).

****
INFORMATION SECURITY AND PRIVACY

There are three main aspects of information security: confidentiality, integrity, and availability. These protect against the unauthorized disclosure, modification, or destruction of information. The focus of this report is on the confidentiality and integrity of information in network environments. Confidentiality refers to the property that

information is made available or disclosed only to authorized parties. Integrity refers to the property that information is changed only in a specified and authorized manner.

Privacy refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information. Confidentiality and privacy are not mutually exclusive: safeguards that help ensure confidentiality of information can be used to protect personal privacy.

INFORMATION SAFEGUARDS

In this report, OTA often uses the term "safeguard" in order to avoid misunderstandings regarding use of the term "security," which some readers may interpret in terms of classified information, or as excluding measures to protect personal privacy. Cryptography is an important safeguard technology. Modern encryption techniques can be used to safeguard the confidentiality of the contents of an electronic message (or a stored file). Message authentication techniques and digital signatures based on cryptography can be used to ensure the integrity of the message (that it has been received exactly as it was sent), as well as the authenticity of its origin (that it comes from the stated source).

CRYPTOGRAPHY

Cryptography, a field of applied mathematics/computer science, is the technique of concealing the contents of a message by a code or a cipher. Cryptography provides confidentiality through encoding, in which an arbitrary table is used to translate the text or message into its coded form, or through encipherment, in which an encryption algorithm and key are used to transform the original plaintext into the encrypted ciphertext. The original text or message through the inverse operation of decryption.

Cryptographic algorithms--specific techniques for transforming the original input into a form that is unintelligible without special knowledge of some secret (closely held) information--are used to encrypt and decrypt messages, data, or other text. In modern cryptography, the secret information is the cryptographic key that "unlocks" the encrypted ciphertext and reveals the original plaintext. Key management underpins the security afforded by any cryptography-based safeguard. It includes generation of the encryption key or keys as well as their distribution, storage, and eventual destruction.

KEY-ESCROW ENCRYPTION

The Escrowed Encryption Standard, or EES, is intended for

use in encrypting voice, facsimile, and computer data communicated in a telephone system. It is currently intended for voluntary use by all federal departments and agencies and their contractors to protect unclassified information; other use by the private sector is voluntary. The EES encryption algorithm, called SKIPJACK, is implemented in tamper-proof electronic devices, or "chips." An early implementation of SKIPJACK was called "Clipper," hence the use of "Clipper chip" refers to the technology.

The EES specifies a type of key-escrow encryption intended to allow easy decryption by law enforcement when the equivalent of a wiretap has been authorized. This is accomplished through what is called key escrowing. Each EES chip is programmed with a chip-specific key. A copy of this key is then split into two parts; one part is held by each of two designated "escrow agents." The EES also specifies how the Law Enforcement Access Field (LEAF) that is transmitted along with encrypted messages is created.

When intercepted communications have been encrypted using the EES, law-enforcement agencies can obtain the two escrowed key components from the escrow agents. (A device identifier in the LEAF indicates which ones are needed.) The escrowed key components are then used to obtain the keys that will decrypt the intercepted communications sessions.
****

ORDERING INFORMATION

Congressional requests: Call OTA's Congressional and Public Affairs Office at 202-224-9241.

"Information Security and Privacy in Network Environments" is available from the U.S. Government Printing Office. Call GPO at 202-512-1800 or fax this order form to GPO at 202-512-2250. Alternatively, mail this form to Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.

Orders placed at GPO generally take four weeks for delivery. If you need fast delivery, the Superintendent of Documents offers Federal Express service for domestic telephone orders only. The cost is an additional $8.50 per order. Inquire for bulk quantities. If the order is called in before noon, Eastern Standard Time, the Superintendent of Documents will guarantee 48-hour delivery. There is no Federal Express delivery to Post Office boxes or APO/FPO addresses.

For information about other OTA publications, a free "Catalog of Publications" is available from OTA's Publication Distribution Office. Call 202-224-8996 or e-mail pubsrequest@ota.gov or write to: Office of Technology Assessment, U.S. Congress, Washington, D.C. 20510-8025. Attn: Publication Distribution.

□
□