

CIVILIZING CYBERSPACE:

Priority Policy Issues in a
National Information Infrastructure

Lance J. Hoffman

School of Engineering and Applied Science
Institute for Computer and Telecommunications Systems Policy
The George Washington University
Washington, D.C. 20052

Work Supported in part by Grant NCR 91-13216
from the National Science Foundation
Division of Networking and Communications Research
to The George Washington University

PREFACE.....	iv
EXECUTIVE SUMMARY.....	vi
1 INTRODUCTION	1
2 TECHNOLOGICAL CONTEXT.....	6
I. TODAY'S NETWORKS	7
II. TOMORROW'S NETWORKS	8
3 KEY POLICY.....	10
I. GOVERNANCE	10
II. REDEFINING COMMON CARRIAGE	13
A. Possible levels of regulation	14
B. Risks to the public good under each scenario	15
III. PRIVACY	16
A. Universal computer networks will greatly reduce the costs and technical obstacles to efficient, large-scale privacy invasion.....	16
B. Strict privacy policies are needed to encourage use of these networks	17
C. Aspects of privacy encroachment are intrusion, appropriation, and surveillance	17
D. Legal and statutory protection of privacy is weak	21
E. Regulatory authority is unclear	23
F. Privacy practices need to be harmonized internationally.....	24
IV. SECURITY	25
A. Aspects of security are anonymity, accountability, liability, and integrity.....	26
B. Encryption policy	27
V. INTELLECTUAL PROPERTY	32
A. Cultural norms on networks do not now favor intellectual property protection.....	32
B. Technological measures to protect intellectual property usually fail.....	32
C. Payment for initial distribution of intellectual property can be assured with existing mechanisms; technical methods to control re-use are by no means guaranteed.....	33
D. New paradigms of intellectual ownership or management need to be devised to fit the electronic marketplace.....	34
E. Intellectual property rights currently available for traditional media must be ensured for	

	electronic media as well; doing this is not trivial.....	36
4 PROPOSALS		37
I. GOVERNANCE		37
A.	Development of the national information infrastructure should be market-driven, with support from limited, appropriate government policies.....	37
B.	Government funding should be deployed efficiently to stimulate private-sector development.....	38
C.	Government and industry should construct a credible planning group now.....	38
D.	Government should immediately initiate coordination between PSS and the computer networking community.....	39
A.	Federal policies should ensure universal access and non-discrimination of content.....	40
B.	Federal policies should restrict carriers' liability.....	40
C.	Federal policies should restrict re-use of personal information.....	40
D.	Tariff regulations should be minimized or eliminated for network service providers.....	40
III. PRIVACY		42
A.	Service providers should voluntarily adopt a fair information practices code.....	42
B.	The government should set up an information practices commission.....	42
C.	The government could legislate minimum national standards for privacy.....	43
D.	The government could establish user royalties and a National Information Market (NIM).....	44
IV. SECURITY		46
A.	The ECPA should be extended to electronic networks	46
B.	Tradeoffs to cope with cryptographic advances must be openly discussed.....	46
C.	Development of security policies that are uniform throughout the network should be discouraged.....	48
D.	Accountability must be balanced with anonymity....	48
E.	International coordination is needed.....	49
V. INTELLECTUAL PROPERTY		50
A.	Network cultural norms should more fully recognize the public benefits of protecting intellectual property.....	50
B.	Intellectual property rights should be enforced in the national information infrastructure by suitable legislation and use of supporting technical mechanisms.....	50
GLOSSARY		51
BIBLIOGRAPHY		54
APPENDICES	A: D. Linda Garcia, "A National Communications and Information Policy: Reconciling the Issues B: Willis Ware, "Security Considerations for Data Networks" C: Marvin Sirbu, "Technology Trends" D: Kenneth C. Laudon, "Privacy Beyond 2000" E: Mark Rotenberg, letter to Kenneth C. Laudon	

F: FBI Digital Telephony proposed legislation
G: Information Infrastructure Task Force, "The
National Information Infrastructure: Agenda for
Action"
H: Steve Kent, "Intellectual Property: Future
Work"

CIVILIZING CYBERSPACE

Preface

There is a window of time available now in which to act to develop policy guidelines consistent among various national and international networks before delays result in inadequate privacy and security, cancellation or rejection of some otherwise fine networks, or costly retrofits.

To move ahead in developing appropriate policy guidelines, the National Science Foundation funded The George Washington University to conduct an invitational workshop to address the policy questions, to consider the adequacy of existing policy mechanisms, and to identify a number of legal issues which keep cropping up as networks expand.

A small select group of leaders gathered for four days in January 1993 at Amelia Island Plantation near Jacksonville, Florida to discuss these issues. The heterogenous group of invitees included computer network developers and managers, computer security experts, civil libertarians, hardware and software developers, legal experts, policy analysts, and others. All discussions were off-the-record. Because the development in the field is so quick, especially with the Administration's National Information Infrastructure Initiative, much has changed in the brief time since the workshop. Therefore, some of the issues discussed here have already been resolved. However, most of the work remains an important contribution. The boxed quotes that are scattered throughout the text are taken either from what was said at the workshop, or from conversations between the speaker and the author.

Four invited focus presentations drove the identification and prioritization of hard problems; these presentations, or later revisions, are included as appendices to this report, as are some other documents which I thought appropriate. The participants were split into smaller working groups for some of their time together, but worked together as a large group for much of the time, emerging with a short list of the most important and pressing short-term and long-term problems.

This project could not have been possible without the help provided by the National Science Foundation Division of Networking and Communications Research, and Dan Van Belleghem in particular. The advisory committee was also of great help. It consisted of L. Dain Gary, Computer Emergency Response Team, Software Engineering Institute; Rich Pethia, Computer Emergency Response Team, Software Engineering Institute; Steve Walker, Trusted Information Systems, Inc.; Willis Ware, The Rand

Corporation; Fred Weingarten, Computing Research Association; and Alan Westin, Columbia University.

Thanks are in order to a number of others, as well. Joyce Cavatoni helped with logistics of getting the attendees to the workshop. The bulk of turning a transcript of the last day's deliberations into a readable report was done by Kristin Knauth. Hae Chan Park also assisted in this process. A special thank you is due to Marianne Berkovich, who took disparate notes, early drafts, and other material and wove them all into a coherent final product.

Lance J. Hoffman

Washington, D. C.
September 1994

**CIVILIZING CYBERSPACE:
Executive Summary**

In the next 15 years, rapid technology development will drive the merging of voice and data communications and, to some extent, of common carriers and enhanced service providers. A new technological environment will emerge that combines public and private elements in a highly competitive marketplace. Although technological development is moving rapidly, the United States is just starting to address hard policy questions about governance, accountability, privacy, security, and intellectual property in a national information infrastructure. Because U.S. policies will have international ramifications, they also need to be coordinated globally. This report offers tentative directions, and suggests further steps to address these issues.

GOVERNANCE: Currently, fragmentation of authority for communications policy is a major impediment to speedy and inclusive resolution of the issues and jeopardizes the public interest. Agencies charged with communications regulations have interpreted their mandates narrowly and frequently have failed to coordinate policies. Although the Clinton administration has taken steps towards funding the "information superhighways," governance for the NII has not been adequately addressed. Proceeding without clear policy-making and regulatory structures could lead to waste of public funds and unnecessary conflicts with industry. The workshop participants agreed that the government should move quickly to facilitate cooperation between the two major players driving network development, public-switched networks and the computer networking community. They felt that the technological and structural evolution of the information superhighway system should be primarily market-driven, but Federal policies should be developed to balance public and private interests, foster competition, and help ensure universal and affordable access to the network. An information practices commission, with a specified lifespan of two years or less, should be set up to study the full range of national information infrastructure issues and make recommendations to the

government. A privacy commission could be set up separately or incorporated into the broader information practices commission.

REDEFINING COMMON CARRIAGE: As technological advances blur the distinction between the common carriers and enhanced service providers (ESPs), no analogous integration is occurring in terms of regulation. Either of two opposing scenarios could emerge: common carriers could assume the functions provided by ESPs, leading to near-universal regulation of networks; or competition could burgeon, inducing deregulation. Since both pure scenarios present threats to the public good, policymakers need to create a new legal definition of common carriage to ensure equitable and affordable access to networks while protecting users' privacy and minimizing carriers' liability and regulation.

PRIVACY: Universal networks will greatly reduce the costs and technical obstacles to efficient, large-scale privacy encroachment, whether by commercial interests, law enforcement, or criminals. Legal and statutory protection of privacy currently is very weak; there is little clear regulatory authority for enforcing privacy rights. Federal policies are needed to give individuals greater control over the personal information that flows through national data networks. These laws then need to be harmonized among states and countries. The workshop participants considered a new "fair information practices" code to be adopted by both transport providers and enhanced service providers. It would protect individuals' transaction data from misuse and might give individual consumers options ranging from partial to complete restriction of use to royalty-based use.

SECURITY: Network monitoring for security purposes may compromise personal privacy, so the Electronic Communications Privacy Act should be extended to allow administrative monitoring of data networks. Due to cryptographic advances, existing technological mechanisms that enable law enforcement and intelligence agencies to gather intelligence electronically could lose their effectiveness in an increasing number of situations. Technical solutions to achieve a satisfactory tradeoff between personal/corporate privacy and law enforcement/national security needs should (and probably will) be developed in a competitive market. Uniform security policies throughout an information superhighway system, however, will be inappropriate. Therefore, new law enforcement methods and tradeoffs between personal privacy and law enforcement should be analyzed now in public discussions in a spirit of mutual good faith among competing interests. Accountability must be balanced against legitimate needs for anonymity. Technical means must be put in place to restrict the amount of damage that a user with a legitimate need for anonymity might inflict on a network. Liability for security breaches is especially problematic in two cases: when personal privacy is compromised, and across international boundaries.

INTELLECTUAL PROPERTY: Intellectual property rights should be respected in networks to make networks attractive to commercial providers and users. Only distribution of the first copy of copyrighted material can be controlled technologically; there are

to date no well-developed technical means available to control re-use of intellectual property. Current models of licensing are inadequate for electronic environments. Intellectual property protection in the national information infrastructure should be encouraged as a cultural norm through education.

1 INTRODUCTION: A Window of Opportunity

Policy decisions governing communication and information technologies determine not only the availability and distribution of products and services, but also ... the nature of society itself.

At the threshold of the 21st century, the global marketplace of ideas and commerce is evolving swiftly into a digital one. By 2010, ubiquitous digital networks transmitting a fusion of voice, data, and video will serve as the nation's primary channels for commerce, education, politics, entertainment, and personal communications.

In the United States, a national information infrastructure is rapidly emerging. The Clinton Administration has made development of an "information superhighway system" -- a web of high-speed telecommunications networks that are accessible and affordable to all Americans -- a top priority of its High-Performance Computing and Communications Program.

As America moves into this new era of technological interconnection, meaningful discussion about the emerging infrastructure cannot be framed in solely technological terms. Societal policies devised for an age of physical media and voice communications will not always translate easily to an electronic future. Maintaining freedom of expression and association and other democratic values will depend on initiating appropriate policies today to shape and govern the nation's communications infrastructure.

At a workshop convened at Amelia Island, Florida, on January 26-28, 1993, an interdisciplinary group of 24 experts gathered to discuss these issues. Their mission was to examine important policy issues related to computer networks today and, whenever possible, to produce directions for possible policy and/or technological solutions.

The participants chosen were knowledgeable leaders from the science and technology research communities, the legal community, scholarly institutions, public interest groups, and the federal government (see Table 1). The National Science Foundation Division of Networking and Communications Research funded the symposium.

Table 1: The George Washington University/National Science Foundation Workshop on Priority Policy Issues in a National Information Infrastructure

PARTICIPANTS

Jerry Berman
Electronic Frontier Foundation

Scott Charney
Department of Justice

Paul Clark
Trusted Information Systems

Stephen Crocker
Trusted Information Systems

Dorothy Denning
Georgetown University Computer Science Department

David Flaherty Woodrow
Wilson Center

D. Linda Garcia
Office of Technology Assessment

Dain Gary
Carnegie-Mellon University Software Engineering Institute

Mike Godwin
Electronic Frontier Foundation

Janlori Goldman
American Civil Liberties Union

Lance J. Hoffman
The George Washington University

Brian Kahin
Harvard University Kennedy School of Government

Stephen Kent
BBN Communications

Robert Kraut
Bell Communications Research

Kenneth Laudon
New York University Stern School of Business

Arthur Oldehoeft
Iowa State University Computer Science Department

Ronald Plesser
Piper and Marbury

Charla M. Rath
Federal Communications Commission

Ed Roback
National Institute of Standards and Technology

Michael Roberts
EDUCOM

Marc Rotenberg
Computer Professionals for Social Responsibility

Marvin Sirbu
Carnegie-Mellon University Engineering & Public Policy Department

Willis Ware
Rand Corporation

Alan Westin
Columbia University Political Science Department

The workshop adopted no "official" positions. Indeed, much work remains to be done to formulate appropriate solutions to the issues. But the suggestions that follow promote informed discussion. Some of these suggestions correlate almost exactly with those of the Clinton Administration in its September 1993 proposal for a national information infrastructure.

Workshop participants and the administration agree, for example, that the government's role in shaping the network is critical at this juncture, that government's role should be limited to supporting and protecting a market-driven information infrastructure, and that a high-level inquiry should be convened without delay to address the issues.

In many respects the symposium went beyond the Administration's plan to provide a more detailed analysis of the issues. Participants soon identified five major problems engendered by the emergence of national and international information networks:

- 1 Governance: Delineating the roles of the players (federal government, private companies, users, other organizations) in creating, regulating, and using the network
- 2 Defining the network: Creating a legal definition for universal networks that codifies their regulatory structure, accessibility, and accountability
- 3 Privacy: Balancing personal privacy against the legitimate needs of business, government, and organizations
- 4 Security: Protecting universal networks from disruption of service and from unauthorized disclosure, destruction, or modification of the programs and data available on the networks

5 Intellectual property: Defining and protecting intellectual property rights in an electronic milieu

Although all of these concerns pertain to the voice and data networks that exist today, the arrival of much higher-speed, universally accessible, national networks will amplify tremendously their importance and complexity. The vast scale of the emerging information infrastructure will swell commensurately the risks to privacy, security, and intellectual property.

Finding solutions to these problems will require a detailed, thoughtful balancing of conflicting interests. For example, security standards that allow a system to meet the needs of business and government could limit the extent to which the same system can be used for research and other collaborative efforts. Security features may add costs, slow transmission speeds, increase network traffic, and generally dispirit the cooperative and uncircumscribed spirit which promotes scientific advances. Users may disagree significantly on the levels of security required and the sacrifices that should be made to achieve it.

Resolving the tradeoffs will not be easy. The stakes are rising, especially as the strategic value of information increases in all aspects of American life. Constituencies with vested interests in the NII are numerous and sundry: academic institutions, from kindergarten to post-graduate; the telecommunications industry; state enterprises dedicated to economic development, research, and education; industrial research and development laboratories; corporations, large and small; and federal research agencies. Advanced networks extend into the majority of American homes now and ultimately will reach them all. These decisions will thus affect virtually every citizen.

Furthermore, setting communications policy in the United States is particularly difficult. Since responsibility for telecommunications policy is highly fragmented within the federal government, no single agency is responsible for the big picture. Hence, there has been little communication, let alone coordination, among these players. Most agencies have based their decisions on narrow definitions of the issues, largely failing to recognize the wide-ranging implications of network communications policies.

Jurisdiction between state and federal governments with respect to communications policy is similarly ambiguous. The Federal Communications Commission (FCC) regulates the interstate aspects of telecommunications, and intrastate aspects to the extent that they significantly affect interstate policy. States hold responsibility for everything else. But trying to apportion a national (or international) network theoretically into interstate and intrastate pieces is something like trying to cut spaghetti on a plate into distinct sections.

In the future all these issues of jurisdiction, security, interoperability, intellectual property rights, and privacy will extend to the international arena. We live in a global economy, and there is no doubt that the information superhighway system soon will reach around the globe. Over 70 countries have full TCP/IP Internet connectivity, and about 150 have at least email services.

Current United States policies concerning privacy, security, and intellectual property rights are not well matched to the corresponding policies of the European Community or Asian nations.

Already, disputes within the United States about policy jurisdiction have hindered the American case in international standards debates. Also, international law enforcement cooperation (for example, in drug enforcement operations) is impeded by disparate standards of electronic protection of personal information.

Responsibility for telecommunications policymaking has shifted from the political arena to the marketplace in the last decade, compounding the difficulty of trying to impose unified policies.

Divestiture of the Bell Telephone System, the emergence of large users, and regulatory liberalization have all been factors in this shift to a market-driven, heterogeneous telecommunications environment.

No clear policymaking structure existed at the time of the workshop to resolve these issues, and the mechanisms for involving industry in decision making and for coordinating policies internationally were insufficient. The Administration is attempting to address these problems via its U.S. Advisory Council on the NII and intragovernmental task forces. The technology will not wait. There is a window of opportunity available now in which to act rapidly to develop policy guidelines consistent among the various national and international networks. Delay in considering these issues could result in dangerous breaches of security and privacy, large-scale violations of intellectual property rights, cancellation of some networks, or costly retrofits. If, as a society, we fail to grasp the moment, ... the opportunity to make deliberate choices about new communication technologies -- and about the nature of American society itself -- will be overtaken by rapid technological advances, hardening of stakeholder positions and the force of international developments.

2 TECHNOLOGICAL CONTENT

The national information infrastructure will be a communications environment of unprecedented technological complexity. Although its ultimate structure and management remain speculative, prevailing opinion in the scientific community is that it will encompass a broad range of information services transported by hundreds and perhaps thousands of competing commercial enterprises over diverse, autonomous user

networks. Voice and computer communications will merge -- a trend that is well underway today. The "interstate highway system of the information age" and will become the most powerful tool for disseminating and manipulating information that has ever existed. Rapid technological development of the NREN and other advanced networks is outpacing regulations and policies that were devised for yesterday's voice and data networks. Setting appropriate policies for the forthcoming era of universal interconnection requires a basic understanding of the technological and regulatory directions in which today's networks are evolving.

I. TODAY'S NETWORKS For policy makers, the key technological trend to understand is the rapid converging and interconnection of public and private networks. This trend is exemplified in the closest existing prototype for the emerging information infrastructure, the Internet, a worldwide super-network that connects thousands of academic and scientific research networks. The Internet encompasses both publicly regulated telephone networks ("common carriers") and unregulated information service providers. Yet this super-network -- which is the world's largest computer network -- has no central governance. Its tremendous growth in the last two decades has taken place in a context of near-anarchy, controlled only by a combination of standards-setting committees and a spirit of collegial collaboration in the pursuit of science. Its abiding success strikes even some of its most dedicated users as a happy aberration. The anarchy cannot continue, however, as the Internet continues to expand into the commercial and education sectors. Less technically sophisticated users demand more user-friendly tools and less chaotic governance, and since the user community is now less homogeneous, more disagreement over what is appropriate behavior on the net is inevitable. Increasingly, a need is becoming apparent for clear guidelines and accountability, and for someone to be in charge. In a typical "cell" of the Internet today, a university campus, with its thicket of local area networks and hosts, is connected to a router, a computer which serves as a gateway from the campus to the rest of the networking universe. Usually the router is connected by a leased line, provided by an "interexchange carrier," (a long distance company) to larger networks, such as the NSFNet, those owned by enhanced service providers (ESPs), and others. Some typical ESPs are Compuserve (owned by H&R Block), Prodigy (owned by IBM and Sears), and GENie (owned by General Electric). They can be used to pay bills, shop from home, deliver electronic mail, and participate in electronic special interest groups, among other functions. Some elements of this basic cell are strictly regulated while others are completely unregulated. In 1980, in a decision known as Computer Inquiry II, the Federal Communications Commission (FCC) drew a distinction between "basic service elements" (information transport services) and "enhanced services" (value-added information services such as voice messaging or financial services). This was the first time the FCC distinguished between the transport mechanism and the information that is transported over it. Under the ruling, traditional common-carrier regulations apply to providers of basic services on the grounds

that, following the breakup of AT&T, these operate in a quasi-monopolistic fashion at the local level. Common carriers are obligated to:

- Provide universal service;
- Carry any kind of information without discrimination; and
- File their tariffs with the FCC.

An important concomitant benefit conferred on common carriers is release from liability for the content of the information they transmit. At the same time, the FCC chose to stop regulating ESPs, deeming that their markets had become sufficiently competitive. Today ESPs remain completely unregulated, except to the extent that they transmit personal information which is covered by sector regulations (such as financial audits, credit reports, or, in some states, health care records). Most information carried over networks now is carried by ESPs and hence is unregulated. Complications ensued virtually from the inception of Computer Inquiry II, due to the fact that more and more companies began to provide both regulated transmission between third parties and unregulated value-added information services. Initially, the FCC required that such companies isolate their provision of enhanced services in a subsidiary firm. But in 1988, in Computer Inquiry III, the FCC initiated a concept called "Open Network Architecture" (ONA). Under ONA, transport providers may effectively split their networks into theoretical pieces that provide either basic or enhanced services. Only the accounting functions of the two types of service are segregated. Otherwise, the services may be provided by the same company over the same network. ONA provisions specify the conditions the regional Bell operating companies must meet before they can begin providing enhanced services, and is intended to prevent the Bells from using their local telephone services to gain unfair competitive advantages in these new markets.

II. TOMORROW'S NETWORKS By 2010, a broad national information network will be an established reality. Computing and communications will merge, yielding new kinds of information appliances ranging from hand-held (or "wristwatch") cordless personal "compu-phones" to wall-sized high-definition displays. Data and program sharing will occur on an exponentially greater scale than today. An individual's personal telephone/computer will be linked to nearly all others in the world. The key development in network technology during this period will be the replacement of today's packet-switched networks by a new call-routing architecture called ATM (Asynchronous Transfer Mode). ATM uses a novel method to provide very high-speed switching services among networks -- more than 45,000 times the speed available on typical telephone lines today. Like today's Synchronous Transfer Mode (STM) formats, ATM disassembles information into "packets" that are loaded onto telephone lines and reassembles them electronically at the receiving end. But unlike STM, ATM parcels information into packets of uniform size, enabling it to pass smoothly from a desktop computer to a local telephone wire to a long-distance fiber-optic line without

slowing down for "protocol conversion," or technical translation for different systems, along the way. ATM is being developed by today's common carriers (the regional Bell operating companies and other basic transport providers like Sprint and MCI). And Sprint has announced a nationwide long-distance voice, data and video transmission service for corporation using ATM. Fifteen to twenty years from now, it will supplant today's network architecture. How will the arrival of ATM affect the relationship between common carriers and ESPs? Today's cell-switching services are provided by both public carriers and private ESPs. But ATM-based services probably will be provided primarily by public local exchange carriers and interexchange carriers, whose parent companies are developing them. Eventually, these ATM-based services could replace the ESP-controlled portions of the network.

3 KEY POLICY ISSUES:

Governance, Redefining Common Carriage, Privacy, Security, Intellectual Property The Amelia Island symposium identified the most pressing policy issues as:

- Governance of the national information infrastructure,
- Creating a new regulatory model for advanced universal networks, based on a definition of common carriage suitable for the electronic age,
- Protecting privacy in the coming era of interconnection,
- Protecting security (of network transmission), and
- Protecting intellectual property in an electronic marketplace.

This section delineates the problems to be solved with respect to each issue.

I. GOVERNANCE Participants noted repeatedly that the lack of appropriate administrative structures in both the government and private sectors slows the deployment of new technology and prevents the public's interest from being represented in decisions about a national information infrastructure.

Some of this has changed since the workshop. The Clinton administration has established an interagency Information Infrastructure Task Force to work with Congress and the private sector to propose the policies and initiatives needed to accelerate the deployment of National Information Infrastructure. It has also established a private sector Advisory Council on the National information Infrastructure in order to facilitate meaningful private sector participation in the IITF's deliberation. In order to implement National Information Infrastructure, the administration plans to properly structure and adequately staff the federal agencies most directly responsible for the evolution of the NII in order that they can effectively address many new and difficult policy issues. Only time will tell whether the scattered and ill-coordinated regulatory authority of the past will be remedied by these efforts. In the private sector, the providers of public switched

telephone services are moving forward on networking technologies and developing niche markets independently of the computer communications industry. Coordination between the two industries needs to be initiated now, probably by the private sector Advisory Council, since these policies and technologies will be forced to coalesce in the national information infrastructure. Finally, industry pressure to minimize regulation of the new infrastructure will be strong - witness the great battle over encryption technology (See "Encryption Policy", page 27), and mechanisms other than regulation need to be devised to protect the public interest.

A. Agencies charged with setting communications policy have interpreted their mandates narrowly. Although the jurisdiction of the FCC is very broad, in recent years the agency has taken a hands-off approach to many important aspects of networking policy. In the telecommunications arena, the FCC has concerned itself with competition and deregulation rather than with issues related to information content, such as privacy.

The FCC left it to states, for instance, to regulate Caller ID. Several agencies in addition to the FCC have a mandate to regulate or develop policies for information and communications. Most, like the National Institute of Standards and Technology (NIST), have interpreted their mandates narrowly. The National Telecommunications and Information Administration (NTIA) -- part of the Commerce Department -- has in the past limited its concerns to questions of commerce and economic efficiency. However, since the Clinton administration took office, it has become a catalyst for the development of the NII, supporting \$26 million in research and development in FY 1994.

2. The computer and communications communities are moving forward independently on technologies and policies that, in the future, will coalesce in the national high-speed network. The government should act quickly to bring these players together and resolve economic and technical questions so that the maximum public good will be obtained.
3. As telecommunications service providers merge with the public switched networks, overregulation of the new infrastructure should be avoided. At the same time, creative mechanisms need to be devised to maintain a public interest perspective in a very heterogeneous environment.

II. REDEFINING COMMON CARRIAGE Telecommunications networks today fall into two categories: common carriers, which transport information, and enhanced service providers (ESPs), which sell information services. Common carriers are regulated as public utilities, while ESPs are almost completely unregulated. But the distinction between these two types of service providers is blurring. Many common carriers offer both regulated and unregulated services. Sprint, for example, is a regulated common carrier but it also provides enhanced services through Telenet and other unregulated subsidiaries. And the Internet is

unregulated, even though it uses lines owned by regulated carriers.

Like the Internet, the planned information superhighway will be a complex mosaic of basic and enhanced services. To the extent that it acts as a transport provider, the national network will closely resemble today's public switched telephone networks (PSNs). PSNs are common carriers, regulated by the FCC, state Public Utility Commissions, and federal and/or state laws.

In exchange for meeting certain FCC obligations (see "Today's Networks", page 7), common carriers are released from liability for the content of the information they transmit. This is in contrast to other forms of public media, such as newspapers or broadcast media, which are liable for slanderous or obscene content. Common carriage is generally held to be a positive regulatory model for communications services because it promotes other forms of commercial activity, guarantees user privacy, and assures that markets with limited competition will charge fair rates. The concept was legislated in the Communications Act of 1934, to prevent telephone monopolies or near-monopolies from restricting access or imposing excessive rates. Today, however, it also applies to competitive industries such as the airline and rail transport industries. In the next 10-15 years, the information superhighway could evolve towards near-universal common carriage. The current administration hopes to make the NII a "public" network, accessible to all through schools and businesses (although this goal is not necessarily shared by all stakeholders). Technology also could drive this trend: as common carriers gradually replace today's cell-switched networks with high-speed ATM networks, they might assume management of the portions of the Internet that now are controlled by ESPs (see "Setting the Scene," page 6). Finally, legal trends also may be pointing towards universal regulation under the common carriage model. But competition, if strong enough, could offset these trends and prompt the FCC and other agencies to deregulate network service providers. Under this scenario, universal deregulation could result. A. Possible levels of regulation. The situation could evolve to one of two contrary scenarios -- near-universal regulation or near-universal deregulation, or to some sort of mix.

- 1 Universal regulation. Since local exchange carriers and interexchange carriers are regulated as common carriers, all information carried over their ATM lines would be subject to common carrier protection and rules. ESPs could vanish from most or all of the transmission path. This would be very different from today's reality, where enhanced services, and hence most information carried over a network, are provided by unregulated ESPs which may discriminate on the basis of content and access and whose fees are not regulated.
- 2 Universal deregulation. Competition could, however, mitigate or negate these trends toward near-universal regulation. In the next five to fifteen years, competitive alternatives will emerge for local

communications networks, just as they now exist among long-distance services. Since the FCC tends to respond to competition by reducing regulation, common carrier regulations could, in this time frame, be withdrawn from carriers at all levels of a national network infrastructure. In this scenario, the common-carrier structure would fall by the wayside. The question is whether there will be sufficient competition in the local access area to warrant deregulation.

- 3 Mixed situation. A mixed situation might develop. In that case, the regulation might also be mixed. If so, the resultant network must be guided to support liberty, innovation, universal access, and competitive pricing.
- B. Risks to the public good under each scenario. Any of these scenarios could, in some circumstances, jeopardize the public good. Universal regulation, with its accompanying mandatory tariff registration, could impede growth and innovation in a communications environment as dynamic, heterogeneous and universal as the national information infrastructure. The result could be stymied technological advancement and a paucity of commercial offerings. Under universal deregulation, consumers would not be assured of universal access and uncensored transmission, while carriers would not necessarily be assured of freedom from liability -- principles that have characterized the American telephone system since the 1930s. A mixed system could have advantages, as well as disadvantages, of each. A new regulatory definition is needed to fuse the advantages of common carriage with the advantages of competition. The government should act quickly to create a new regulatory model that will protect the public interest now and in the future. Today's bipolar model, in which each carrier is either wholly regulated or wholly unregulated, is outmoded.
- For policy makers, the question is how to ensure that the national information infrastructure incorporates the common-carrier benefits of universal access and uncensored transmission, while preserving the freedom and innovation of a competitive marketplace and minimizing the tariff and other regulations imposed on public utilities. This issue is addressed in the "Proposals" section below.

III. PRIVACY The "privacy problem" is not merely about individual rights but also about collective well-being, quality of life, and the nature of society.

A. Universal computer networks will greatly reduce the costs and technical obstacles to efficient, large-scale privacy invasion. On universal computer networks such as those envisioned in the national information infrastructure, threats to content confidentiality, privacy of transaction information, and directory privacy all multiply.

- 1 Billing and accountability on large networks require detailed record-keeping of usage trails. Expansion of network coverage of an individual may encourage the government to seek access to transaction data for law

enforcement, regulation, and other uses (e.g., traffic analysis can be performed to monitor who is communicating with whom).

2 Computer networks increase the possibilities for commercial appropriation of personal information, such as transaction data, for targeted marketing and other intrusive practices. While the content of network transmissions is today sometimes protected by common carriage rules, communications privacy laws, or sector-specific rules, there are limited regulations that control use of transaction and billing data by either common carriers or enhanced service providers. Personal information about users -- including transaction data about the destination and timing of individuals' messages, billing information, or usage preferences -- is often shared and sold among government agencies and within the private sector, often without individuals' permission and usually without their knowledge. Thus, as a general rule consumers participate in the information marketplace whether or not they wish to. Individuals who attempt to "opt out" may find that they have little legal recourse.

3 Computer networks offer greater capabilities and opportunities for use of encryption techniques than traditional files do. This has both positive ramifications (better privacy protection) and negative ramifications (shielding illegal activities from law enforcement).

B. Strict privacy policies are needed to encourage use of these networks. Questionable uses of information exist independently of networks -- for example, when a credit card database is used for direct mail purposes or medical records are used for employment decisions. The problems become greater, however, as a larger proportion of transactions occur in electronic form, in which records can be more easily aggregated. The regulations laid out in the first generation of privacy legislation -- segregation of files by function, prohibition of secondary uses of information without "informed consent", establishment of individual rights, management accountability, and due process rules -- were important first steps along the road to management of information in a digital age. But some have argued that technology and organizational behavior have now overtaken these ground rules, and that with a PC on almost every desktop, the temptation and ease of privacy invasion require additional legal, procedural, and technical safeguards.

C. Aspects of privacy encroachment are intrusion, appropriation, and surveillance.

1 Intrusion: the deluge of unwanted solicitations and information. The public considers intrusion to be a major privacy problem. With the advent of a national information infrastructure, the level of intrusion could

explode, given the large number of users and the relative ease of sending broadcast messages on networks. Advances in both data storage techniques and data "mining" techniques could spur rapid reductions in the cost of compiling ever-larger data bases on individuals. Meanwhile, advances in the telecommunications infrastructure open the possibility of end users being able to mine large data sets remotely using desktop machines. By the year 2000, it is conceivable that each home will have access to a T1-equivalent (1.54 megabytes/second.) network, radically reducing the cost of mining terabyte-sized databases. In 1991, federal legislation was passed to address public concerns about intrusion by unsolicited "junk" faxes and the use of autodialers for telemarketing. Then Telephone Consumer Protection Act imposed certain fairly stringent restrictions on companies that use automatic dialers or fax machines for commercial advertising. The Act did not extend to digital communications, but could be used as a model for such legislation. Some of the restrictions were stated explicitly in the law (for example, that consumers who receive an unwanted message from the same autodialer more than twice may ask the FCC to fine the company \$500 per call). Other restrictions were left to the FCC to determine through rule-making. In particular, Congress ordered the FCC to establish a means by which consumers can register their desire not to be telephoned by autodialers (or by human solicitors), for example, through a national "do-not-call list" database or a requirement that companies establish their own such databases. The FCC decided that the establishment of such a national database would be too costly. Instead, it promulgated rules placing the onus on consumers to notify the FCC of individual infractions of the law. Therefore, FCC required the telemarketing industry to keep company-specific do-not-call lists. Any person or entities who institute any telephone solicitation should maintain a list of persons who do not wish to receive telephone solicitations. In addition, they should keep a written policy on the maintaining the do-not-call list. They also have to train personnel engaged in telephone solicitation. Many consumer and privacy advocates feel that, in doing so, the FCC significantly watered down Congress' intentions in the Telephone Consumer Protection Act and inappropriately bowed to the telemarketing industry. They question the FCC's suitability to assume a broader role in setting communications policy for the national information infrastructure.

- 2 Appropriation: unauthorized re-use of personal information generated from government records or from network use, billing, and information transactions. The federal government is among the worst "personal information hijackers" -- often in direct violation of the 1974 Privacy Act, according to Rep. Edward Markey. But network providers also are culpable: re-sale of

subscriber information to direct marketers, for example, is widespread. Often, key user identification information on data networks is controlled by enhanced service providers which are not subject to any regulation in their use of transaction data for further commercial transactions. From the viewpoint of public advocacy groups, appropriation is the major privacy problem. An early experiment with mass dissemination of personal information produced dramatic results in 1991, when Lotus Development Corporation, Apple, and Equifax announced development of a CD-ROM based system that was to contain personal information of 120 million American consumers. Lotus MarketPlace: Households would have allowed users to compile mailing lists based on such narrow criteria as where consumers lived, how much they earned, and their spending habits. Although such information is already available in various sources, the program would have allowed anyone with a desktop Macintosh personal computer, CD-ROM reader, and \$695 to efficiently compile detailed composite "likely demographic pictures" of individuals and households. Privacy advocates protested that consumers would not be able to check the accuracy of information about them, or control its use. The companies abandoned the two-year, multimillion-dollar project, however, only after a maelstrom of complaints -- including 30,000 requests from consumers demanding that their names be deleted from the database. (Many objected electronically, flooding the electronic mailbox of Lotus CEO Jim Manzi).

- 3 Surveillance: monitoring of network content and usage by "empowered users" (network administrators, law enforcement officials, or employers). In public switched telephone networks, a "reasonable expectation of privacy" rule has been established in which the content of calls is protected. Listening to the calls themselves requires a warrant. This precedent has not really been carried over to the world of electronic mail. In addition, there is a conflict between user privacy and the legitimate needs of network administration to know enough about what their users are doing (e.g., message routing information) to run the network efficiently. Beyond this, there is another conflict between user privacy and the legitimate needs of law enforcement to audit electronic networks as part of the investigation, prosecution, and deterrence of crimes. This issue is spotlighted by the FBI's proposed "Digital Telephony" legislation, discussed on page 29. The FCC has for years adopted a hands-off approach to privacy issues. For example, in Computer Inquiry III, the FCC compelled the disclosure of Customer Proprietary Network Information (CPNI) by the regional Bell operating companies to their competitors unless the customer specifically requested in writing that the information not be disclosed, assessing the potential threat to privacy of disclosing identifiable information about customers' network use as having less importance

than a non-level playing field for the several providers. (Although the RBOCs do not have a uniform definition of what constitutes CPNI, CPNI could include sensitive information kept by the telephone companies in their customer databases about a person's or organization's calling patterns, billing information, network design, or use of network services.) The ruling was intended to encourage the growth of competition in telecommunications markets by disclosing proprietary information about Bell customers' use of the networks. If no customer request is filed, the baby Bells are required to provide CPNI to competing vendors of enhanced services or equipment if those competitors requested it. Additionally, no federal data protection authority exists to enforce the Privacy Act of 1974. Although the Act recommended instituting a permanent Privacy Commission to regulate government systems and produce studies and recommendations on behalf of the private sector, this recommendation was never actualized. The public has started to look to the legislative and regulatory arenas for privacy protection. The Office of Science and Technology Policy during the Bush administration identified privacy protection as one of the critical issues for NREN development, the Clinton administration has called for the protection of privacy in the NII. In reviewing privacy concerns of the NII, the IITF has developed a work plan to investigate what policies are necessary to ensure individual privacy, while recognizing the legitimate societal needs for information, including those of law enforcement.

- D. Legal and statutory protection of privacy is weak. Federal policies need to be developed because the courts have failed to lay down consistent principles for privacy protection. The application of Constitutional law to privacy protection has been rejected at the federal level in the United States.

- 1 Current United States policies are limited (see Table 2). In the United States, telecommunications privacy discussions typically begin with a discussion about the scope of the 1986 Electronic Communications Privacy Act (ECPA). The ECPA extends protection against wire surveillance to electronic mail, both stored and in transit. The content of electronic communications may be intercepted by court order or by the service provider to maintain the network, but otherwise may not be monitored. This rule applies to both common carriers and enhanced service providers. Table 2: Existing U.S. Government Policies and Regulations Relating to Computer Security. The ECPA is a fairly strong barrier against government surveillance. But the Act does not address two important areas of privacy concerns: privacy within an organization or the collection, or sale of transaction data for commercial purposes. As a result, service providers are free to make use of, and even to sell, records of electronic transactions. Dissemination

of personal information is pervasive throughout the public and private sectors. Some privacy protection exists in regulated sectors, such as with financial records or credit reporting. But the boundaries separating these traditional sectors are dissolving. Information about an individual's health, for example, could flow into the insurance sector, the employment sector, or the government services sector. To the extent that the national information infrastructure moves away from the traditional common carriage model (where the content of transmissions generally is held to be private), service providers will have few or no legally defined responsibilities to protect user privacy. Rules are needed to monitor the flow of information around and between the larger private information pools, as well as to control transaction data and protect content.

- 2 Contract and tort law offer little protection to consumers. On the contract front, it is possible to argue both that there is no consent for the secondary use of personal data and that companies' resale of such data is a form of unjust enrichment. From a tort viewpoint, there is a strong claim that the sale of personal information is an appropriation of commercial value. But none of these arguments, however compelling, have conclusively succeeded in bolstering personal privacy rights in the legal arena.

E. Regulatory authority is unclear. In fact, Laudon has concluded that leading figures in the marketing research and advertising industry in New York do not believe 'privacy' as a legal or social movement has worked. Because they invade privacy so effectively, they are deeply concerned about the absence of social policy and consensus; they wonder, "Who is it that thinks 'privacy' works?"

F. Privacy practices need to be harmonized internationally. Presently, different laws apply in different states and countries and these privacy laws need to be harmonized among them. In 1989, the Japanese Ministry of Post and Telecommunications developed a set of privacy principles for network service modeled on the 1980 Guidelines of the OECD on the Protection of Privacy and Transborder Flows of Personal Data. The Canadian government recently issued policies on communications privacy, including strong enforcement mechanism and criminalization of cellular wire interception. The critical document for European privacy protection during the past decade has been the 1980 Guidelines, the basis for the national privacy laws in most European countries. The European Commission has prepared an elaborate proposal for the public switched networks on network privacy and ISDN (Integrated Services Digital Network, a network platform standard that could be used to inexpensively upgrade existing telephone lines to accept data and video). Today, a critical document is the EC draft

directive on privacy and data protection. It is also the current battleground for European privacy policy.

IV. SECURITY Security is of critical concern in national networks, where researchers' needs for openness and accessibility must be balanced with the needs of business and government for data security. Currently, each user or organization may or may not have its own security policy. There is no generally accepted or template security policy in the United States. While the National Research Council recommended in 1991 the development of a set of Generally Accepted System Security Principles, little movement toward this has taken place. Security policies should be addressed now if the national information infrastructure is to be trustworthy. Security is here defined as the totality of safeguards placed in a network to assure that there is no unauthorized disclosure, destruction, or modification of users' information, and no unauthorized denial of service. In general, the more open a network, the more subject to security threats it is. In a heterogeneous national information infrastructure, coordination to maintain network security will be a major problem. The Internet has no central authority or enforcement mechanism to maintain "law and order." As one participant commented, "Internet institutions are both few and fragile." The source code for rogue programs is relatively easy to obtain. (See, for example, The Little Black Book of Computer Viruses). There is even now what some have characterized as The Little Black Book for networks, "Improving the Security of Your Site by Breaking into It." Another security issue raises other concerns about individuals' right to privacy versus national security and the government's need for efficient information-gathering. There are conflicts between the competing interests of user privacy, corporate privacy, domestic law enforcement, and international intelligence gathering. If these important security issues are not now addressed, resolved, and incorporated into the up-front design of the national information infrastructure, the integrity of large new networks will be suspect. Adding security measures later never works as well and is always more costly. Workshop participants decided to focus only on aspects of security that raise policy questions or where there are conflicting policy interests. Thus, many aspects of computer and network security were not discussed. The areas of security policy that emerged as important for policy were anonymity, accountability, liability, and integrity.

A. Aspects of security are anonymity, accountability, liability, and integrity. One issue of both security and privacy is how to allow legitimate anonymity, while at the same holding people responsible for communications they initiate. Anonymity and accountability. Legal mechanisms are needed to enforce accountability, that is, to trace the perpetrator if an individual damages the system or illicitly accesses protected information, or slanders someone. On the other hand, there may be circumstances where the need for personal anonymity is overriding: whistle blowing and communication with AIDS information services are two examples. Technology to protect anonymous communications is available. Thus, in cases where end-users are granted anonymity, it may be

appropriate to limit their ability to do certain things which could damage the system or other users. We have a rough analogy, perhaps, with police cars. On the highway network, emergency vehicles are given additional legal capabilities (e.g., running red lights) in return for clear identification as emergency vehicles. Liability. Who should be liable for security breaches in a network? Local, regional, national, or international carriers may all be considered culpable, depending on the nature of the breach. On the other hand, software supplied at a local node might be responsible and all the carriers should be immune. Who has the responsibility? To test what? No standards exist! If a network provider allows a privacy breach due to inadequate security precautions, and individuals suffer as a result of the exposure of their personal records, is the network liable? There was general agreement in the workshop that ESPs should be treated differently than transport providers in this regard. Certain basic security features will have to exist in all networks. Indeed, the Japan Information Processing Development Center has contended that social stability cannot be maintained in an age of global information unless all countries adopt uniform minimum security measures. Numerous security standards currently compete across borders: the Trusted Computer System Evaluation Criteria, published by the U.S. Department of Defense in 1985; the Information Technology Security Evaluation Criteria (ITSEC) from France, the Netherlands, Germany, and the United Kingdom; the MITI Computer Systems Security Standards from Japan; and OECD computer security guidelines. The most recent efforts are from NIST, "Federal Criteria for Information Technology Security (FC)," volume 1.0, December 1992, by NIST and NSA, and work continues, especially at NIST, on international "common criteria" for computer security.

- B. Encryption policy. The business community has recently started to view government interference in what has formerly been private turf. As the information superhighway develops, the US government is increasingly concerned with communication, privacy, and security. This is not a new area for government concern; indeed, it has been around since before the French Revolution when governments were, even then, worried about accountability of authors and publication of seditious materials. In recent months, three interwoven initiatives have been prominent: the so called "digital telephony improvement initiative," the Clipper chip key escrow encryption initiative, and modifications to the Export Administration Act. All of these followed the workshop and thus while the topics they deal with were of concern there, the specifics proposals were not visited at length there. However, they are all relevant to the topic, so that it would be remiss not to mention them here. The digital telephony initiative is an effort by the government to maintain some capability to wiretap in cases where advances in telecommunications technology could (or have already) outrun law enforcement's ability to intercept communications in order to enforce the laws and protect the national security. The current proposal before Congress -- S.2375 and HR.4922

(identical bills introduced by Sen. Leahy and Rep. Edwards respectively) would require telecommunications carriers to ensure that they possess the capability and capacity to enable the government to isolate and intercept, pursuant to authorization by a court, call identifying information the contents of a communication. The Leahy/Edwards bill is significantly more narrow than the original Bush and Clinton Administration proposals. Most importantly, the requirements apply only to carriers who engage in "the transmission of switching of wire or electronic communications as a common carrier for hire". They do not apply to Information Service Providers (the Internet, AOL, Prodigy, etc.), to private networks, or to PBX's. A court can only impose a fine for a violation under the bill if it finds that 1) there are no other alternatives (another carrier, other technologies, etc.) reasonably available to law enforcement, and 2) compliance with the bill is not reasonably achievable through the application of available technology. In addition, the bill has some important new privacy protections, including the prohibition of remote monitoring. Law enforcement cannot require a carrier to install a port which can be activated by a law enforcement officer. All taps must be conducted with the intervention of the carrier (as is the case under current law). The warrant requirements under current law have not been changed. Industry and some public interest organizations such as the Electronic Frontier Foundation are currently arguing that the government should pay for all compliance costs. The current bill only authorizes \$500 million to be paid by the government for upgrades of existing features and services within the first 4 years. The Clipper chip, on the other hand, is part of the overall government strategy to solve the knotty problem of protecting American communications against industrial espionage and other compromises while at the same time maintaining the existing capability of law enforcement and national security agencies to eavesdrop, with a court order, on suspect communications. When law enforcement or national security agencies are interested in a person's communication, they obtain a warrant from the appropriate issuing authority. They then fax a notification that they have this to two independent government agencies (currently the National Bureau of Standards and the Automated Systems Division of the Department of the Treasury) who then each give up half of the digital key necessary to decrypt the conversation. When the two half-keys are joined to form the entire key, law enforcement officials can then obtain the unit key for the given chip used in the communicating telephone, and use it to decrypt the conversation (assuming that telephone has used the Clipper chip in the first place). This so-called "escrowed encryption standard" is urged but voluntary in the federal government and is voluntary in the private sector. Perhaps because of the experience with prohibition and after looking into potential violations of the First, Fourth, and Fifth Amendments of the Bill of Rights, the Administration has decided not to make it mandatory. It had hoped that almost everybody would use this system. No one has seriously suggested that the algorithm is insecure (although a method of using it which negates any value to law enforcement

because of a minor design flaw has made the front page of The New York Times), but many do not completely trust the key escrow agents. Many suggestions have been made such as adding a third escrow agent from the private sector, adding one from the Judiciary, letting users pick whichever escrow agents they want, etc. Only recently have some of these been looked upon with favor by the Administration. Clipper's encryption algorithm, "Skipjack", fits into Capstone, the U. S. government's long-term project to develop a set of standards for publicly available cryptography for use in voice and data communications. In one scenario, the government itself and all private companies doing business with the government would be required to use Capstone, which could all be contained on a single computer chip. This would provide economies of scale but would also force users who wanted "government-proof" communications to superencrypt using other commercially available algorithms. Because of great concern about Clipper, the Clinton administration is now actively exploring other alternatives. Indeed, some have pronounced Clipper dead. There is a large and growing collection of encryption software and hardware available. The latest Software Publishers Association study show well over 800 products, of which roughly half are manufactured overseas. There is an increasing fear that more and more American sales are being lost because American software cannot provide the same sort of good encryption that is provided in other countries (since it is illegal to export really good encryption from the United States). Indeed, one vendor (Trusted Information Systems, Inc.) has actually set up a completely independent cryptographic development lab overseas from which crypto products are imported into the United States (but cannot be re-sent out again). Only recently have export controls been loosened a bit so that traveling business executives can at least take their laptops overseas and encrypt information using the Data Encryption Standard (the standard used for banking and financial transactions) without violating the export laws. Nevertheless, there is a movement afoot, led by Representative Maria Cantwell and Senator Patty Murray, to abandon all export controls as encryption, arguing that the economic needs outweigh the national security needs. At this writing, Congress and the Administration have not loosened the reins but are studying the problem. Several scenarios might develop:

1. Complete decontrol of cryptography. The use of strong encryption by the United States public, as well as its export by United States manufacturers, could be completely decontrolled by the government at the direct expense of law enforcement and national security. This will please some members of the public, for they would have maintained control over their privacy. Also, United States manufacturers of encryption products would benefit. Multinationals would have a free hand in choosing the cryptography strength for offices in various countries.
2. Domestic decontrol of cryptography with export regulations. Strong encryption could remain decontrolled

for use by the general public, but strict regulations would remain on its export. It would be more difficult for multinational corporations to communicate securely among offices in different countries since the export of strong encryption products would be tightly controlled.

3. Voluntary escrowed encryption the de facto standard. (This is the Clinton administration's proposed scenario.) The escrowed encryption standard could become a de facto national standard for voice, fax, and data communications. Multinational transmissions would be secure, except that United States law enforcement (with a warrant) and national security agencies would be able to listen to transmissions. The encryption technology might be exportable to countries that implemented the same or a similar scheme and agreed to cooperate in international investigations.
4. Mandatory escrowed encryption. The government could choose to keep complete control over encryption and to enforce use of the escrowed encryption standard. A black market for foreign encryption products smuggled into the United States would probably be created by some members of the public, including criminals, who desire more secrecy. Business could superencrypt with an additional scheme, but at greater cost for greater security. At the workshop, participants acknowledged the need for balancing national security and law enforcement needs with privacy requirements, the majority (although not a consensus) opinion was that Americans should be able to use the best cryptography feasible to protect their communications and stored information. These tradeoffs are not easily resolved. Moreover, much "national security" information is kept confidential by the FBI and intelligence agencies, in marked contrast to other policy-making forums, where the public can gain access to information and outside experts can testify at public hearings. Mutual distrust between these agencies and public interest advocates (and, in the case of Clipper, much of the business community as well) has created an effective standoff on many of these issues. In recent months, as the various players gain more understanding of the positions of the other players, more constructive discussions have begun to take place among them.

V. INTELLECTUAL PROPERTY

- A. Cultural norms on networks do not now favor intellectual property protection. Ideally, measures to protect copyright should be underpinned by cultural norms that recognize the public benefits that accrue from intellectual property protection. Such norms are weak now - - where they exist. Although most of the current disregard for intellectual property rights on networks does not have criminal intent, the permissive culture that characterizes the Internet and other large networks encourages illicit activities among otherwise law-abiding citizens. There are diverse cultures

on the Internet: two significant ones are the conventional one, operating mainly in corporations and other organizations and trying to make what sense its members can of the (implicit, for the most part) "laws of the Internet"; and a subculture of technically proficient users operating by their own (often unwritten and unannounced to new arrivals on the net) laws which are inconsistent with the laws of society as a whole. Some would argue that if this continues, anarchy will reign on the net as it gets more users, and, after a while, less tolerance and a desire for "law and order" will emerge. This is handled in various ways in the current commercial systems. The relatively benign indifference to copyright is a tough issue, since many observers see that numerous good applications have developed out software with questionable origins. But if we do want the greatest good for the greatest number, then we have to consider allowing information product purveyors to enforce copyright more strictly on the net and to give up some of the "Wild West" mentality.

B. Technological measures to protect intellectual property usually fail. The history of failed efforts to provide copy protection for software argues that technical efforts to protect copyright on networks are unlikely to succeed. Vendors of shrink-wrapped software have tried numerous technical means to prevent free duplication by the purchaser. All of these have failed, typically because users refused to tolerate the restrictions these imposed on use and switched to competitive vendors who did not impose such "user-hostile" schemes. On a network, intellectual property is even more difficult to protect from duplication and dissemination in violation of copyright. Once data is delivered to the user it leaves the copyright owner's technical sphere of control. The situation is analogous to the hard-media world where preventing copyright violation is not a technical requirement of copy machines, and the U.S. Post Office and overnight mail services are not liable for dissemination of illegally reproduced material through their services, as long as they are merely providing transport for the documents. By contrast, in 1992 Kinko's Copies was successfully sued for "willingly and knowingly" participating in a large-scale copyright violation. Thus, circumstances exist in which an entity that knowingly facilitates egregious copyright violation, in either hard media or electronic formats, could be held liable. Software vendors attempt to control illegal redistribution through site licensing to organizational purchasers, backed up with a combination of incentives and threat. Manuals, troubleshooting, and other types of support are available only to registered owners of their products, while legal actions increasingly are pursued against high-profile violators. The Software Publishers Association took action against 577 organizations in 1993. Such mechanisms do not translate easily to a network, where some of its users may be willing to eschew vendor-supplied documentation and support in order to pay a cheaper (or no) price. Also, redistribution over a network is faster and can be much more prolific, and harder to detect. Electronic licensing technology now being developed can help control access in local, well-managed environments. Auditing can be

employed to detect some violations. But no technology exists to fully protect against mass duplication/redistribution in environments that are not centrally controlled. C. Payment for initial distribution of intellectual property can be assured with existing mechanisms; technical methods to control re-use are by no means guaranteed. There are adequate technical means available to permit intellectual property owners or their agents to charge for initial distribution of data within a network environment. Technical methods may be developed to control re-use of intellectual properties, but are by no means guaranteed. Although no technical "silver bullet" now exists to prevent copyright violations, participants suggested at least two technical mechanisms that might be developed:

1. Electronic copyright markings. A technical means could be devised to maintain copyright markings on electronic information as it is distributed and redistributed. Today, this problem often is addressed via simple textual labeling of the intellectual property. More sophisticated methods could be developed, for example, by attaching digital signatures to the property. It is not clear yet how to "engrave" the digital signature onto a document or software so that it cannot be stripped by users, removing any indication that the data is copyrighted.
2. Dedicated read-only devices. Rather than delivering copyrighted material to users in a form which is processed and displayed on users' computers, the material might be encoded so that it is viewable and searchable only on a user's dedicated reading device, separate from the computer. This approach has obvious drawbacks that would need to be rectified, including the problem of making such a system economically feasible for end users and the possibility that it might be circumvented by technically proficient users.

C. New paradigms of intellectual ownership or management need to be devised to fit the electronic marketplace. The notion of "copyright" and the distinction between an initial sale and subsequent sales of an intellectual property probably should be re-examined for the electronic marketplace. Under the current system, intellectual property providers will price the original copy of their products high enough to account for perceived lost revenue due to subsequent copying and dissemination or low enough to remove the incentive for doing that. Two methods are typically used:

1. Site licensing. A form of this practice is used in the software industry, where pricing for large sites or user groups anticipates re-use of the product within the organization without additional purchase. However, re-use is restricted to a certain number of users and the licensee is liable for any violations incurred within the organization. End users have both positive and negative incentives to comply, from retaining the right to

technical support and software updates to avoiding litigation. On networks, where re-use is difficult or impossible to monitor, as well as potentially unlimited, such attempts at restriction are probably useful only in cases where the intellectual property is time-sensitive - that is, it will lose most or all of its value after a given period. In these cases, a method could be devised to calculate probable distribution throughout the network during the limited time period and the fee determined accordingly. Such pricing could be tested on large organizational customers, who may be presumed to provide candid accounting for dissemination within the organization. Very elaborate technical schemes have been proposed to provide very high assurance against unauthorized execution of software or even against unauthorized duplication of data. However, these schemes impose stringent security hardware requirements on workstations and personal computers, and do not appear to be economically feasible. There is insufficient motivation for the developers of these computers to implement the requisite security features, which would increase the cost of the computers.

2. Royalties. For intellectual property of lasting value, more traditional methods may be in order. Without trying to control each transaction, a form of copyright clearance could be devised in which users pay a royalty to a central enforcement agent. This arrangement currently is employed by database providers such as Dialog and Nexis. Participants noted that in the traditional publishing world, royalties for books usually diminish to a low level a few years after publication. The same phenomenon is likely to occur even more commonly, and more quickly, in electronic formats.

D. Intellectual property rights currently available for traditional media must be ensured for electronic media as well; doing this is not trivial. Most information providers will not make their products available on networks unless they can be assured of fair compensation. This will require a paradigm shift among many current network users. On the Internet, intellectual property rights traditionally have been governed by the same "fair use" practices that infuse academic discourse. In this collegial atmosphere, disseminating intellectual property broadly and without expense is considered acceptable as long as the information is used only for personal or academic purposes. When the information is used for commercial purposes, however, users are supposed to be bound by the same copyright obligations that prevail for intellectual property on physical media. With most systems on the Internet, copying and redistributing software is very easy. This multiform arrangement has helped create "virtual communities" conducting scientific collaboration across great distances. But unauthorized software copying has proliferated on the network, just as it has among computer users in non-networked environments. The software industry claims to lose \$7.45 billion internationally and more than \$1 billion

domestically of revenue each year from illegal copying on both networked and non-networked systems. Although it is easy to ensure that copyrighted material is legitimately acquired and paid for initially, it is quite difficult to prevent subsequent redistribution that avoids royalty payments.

4 PROPOSALS

I. GOVERNANCE

Some of the governance recommendations produced by the NSF/GWU workshop correlate closely with the Clinton administration's NII proposal. In many instances, however, workshop discussions produced more detailed suggestions; in some cases, just the reverse was true.

- A. Development of the national information infrastructure should be market-driven, with support from limited, appropriate government policies. The national information infrastructure should be constructed and managed by the private sector. Government commitment is critical, but federal policies should be limited to fostering competition, helping balance public and private interests, and ensuring universal and affordable access to the network. Workshop participants favored a market-driven approach to development, with the government providing demand-side subsidies to help drive development of the information super highway system. These subsidies would give transport and service providers indirect incentives to develop publicly accessible, advanced communication networks. The Clinton administration's plan is in concert with these conclusions and offers detailed proposals for the allocation of subsidies.
- B. Government funding should be deployed efficiently to stimulate private-sector development. Government subsidy is one mechanism for speeding the deployment of the national information infrastructure. The workshop discussed the possibilities of both supply-side subsidies (e.g., subsidizing the Internet or the NREN itself) and demand-side subsidies (e.g., subsidizing network users or application developers rather than network developers). Federal and state governments currently provide some supply-side subsidies, while the telephone companies favor demand-side subsidies. The Clinton administration advocates both forms of federal funding. In a relatively limited demand-side subsidy, the government would provide matching grants to schools and other non-profit organizations to help them access universal networks. Recipients of this funding would serve as models, demonstrating the benefits of networking to the educational and library communities. The Administration also proposes supply-side funding in the form of research, experimentation tax credits, and defense conversion.
- C. Government and industry should construct a credible planning group now. Workshop participants concluded that a joint government/private credible interdisciplinary planning group was needed now to evaluate comprehensively the goals and harms

that could arise from the continual growth of network technology. It would wrestle with market mechanisms, regulatory mechanisms, enforcement mechanisms, and education; propose legislation, regulation, and private policy; and have the credibility to have its recommendations implemented. Workshop participants felt that a task force, while necessary, would not fill all necessary functions. Complementary or alternative mechanisms that were proposed included:

1. A White House conference with representatives from all affected groups. This could provide the advantages of high visibility and prestige, and would set in motion an ongoing public/private collaboration aimed at helping the Administration make unified decisions on information policy as it develops its technology agenda.
2. A private blue-ribbon commission. Again, this could provide visibility, prestige, and quick results.
3. A temporary public study or policy commission with a limited mandate. The Administration has created an interagency "Information Infrastructure Task Force" (IITF) to work with Congress and the private sector. The mandate of this task force includes creating consensus and implementing policies needed to speed deployment of the national information infrastructure. The Clinton administration has formed the United States Advisory Council on the National Information Infrastructure to facilitate private sector input on the IITF. It represents the key constituencies impacted by the NII, including business, labor, academia, public interest groups, and state and local governments. The Council will advise the IITF on matters related to the development of the NII, such as the appropriate roles of the private and public sectors in NII development; a vision for the evolution of the NII and its public and commercial applications; the impact of current and proposed regulatory regimes on the evolution of the NII; privacy, security, and copyright issues; national strategies for maximizing interconnection and interoperability of communications networks; and universal access.
4. A permanent, inter-agency commission or agency, with a broad mandate to study, regulate, and enforce policies related to information and communications. Investigative and regulatory functions that are now fragmented among numerous federal agencies could be centralized in this new body. A permanent commission would carry several disadvantages, however. To succeed, permanent government bodies must be driven by a perception of concrete harms that already affect a significant portion of the electorate. This situation does not exist today in the communications sphere. Also, permanent commissions require substantial capital investments in time and money.

- D. Government should immediately initiate coordination between PSNs and the computer networking community. One of the government's first steps should be to bring together the two major players -- the public switched networks and the computer communications community (currently represented by users and operators of the Internet) -- to coordinate their activities in the public interest. Currently, the two sides are moving forward independently, in fits and starts, on technologies and policies that sometimes clash in the short run but which will have to be harmonized in the long run.

II. REDEFINING COMMON CARRIAGE A new regulatory definition is needed to create an environment that promotes competition, limits carriers' liability, and allows users to feel safe that their transmissions and transaction data will not be used inappropriately for commercial or other purposes. Federal law and policies should define a new, common carrier-like category of network service providers. It should include a provision restricting dissemination of customers' transaction data to third parties. A new term should be coined to distinguish the new definition from today's regulatory models, and should apply equally to carriers that charge for their services and carriers that do not. (Today, many commercial service providers offer free transmission or electronic mail in order to promote use of their services or encourage participation in a special interest group.)

- A. Federal policies should ensure universal access and non-discrimination of content. At the workshop, participants agreed that when computer networks act as independent transporters, moving data between other parties, they should adopt the common-carrier obligations of universal access and non-discrimination of content. Despite the fact that the national network will serve as the circulatory system of a highly competitive communications marketplace -- and, as such, will be anything but monopolistic -- some participants felt that its constituent nets should be subject to some regulation. In particular, they felt that computer networks should be held to defined standards of access and service.
- B. Federal policies should restrict carriers' liability. Transport providers should not be held liable for the content of information they transmit between independent parties. (This freedom from liability would not extend to enhanced service providers, who should be subject to the same obscenity and libel restrictions as other originators of publicly disseminated information.)
- C. Federal policies should restrict re-use of personal information. All service providers should be restricted from disseminating customers' transaction data to third parties without prior authorization by the customer or by law.
- D. Tariff regulations should be minimized or eliminated for network service providers. The new regulatory definition

should codify the obligations of service providers to file tariffs with the FCC. These obligations should be minimal or non-existent, on the grounds that such regulations could deter growth of a competitive market and curtail the number of services offered in the national information infrastructure.

III. PRIVACY Workshop participants generally felt that information that is collected about individuals in the course of business should not be re-used or sold without the individual's explicit permission. Indeed, many organizations already give their members or users this "opt-out" choice (although most still "set the default" to "opt-in").

A. Service providers should voluntarily adopt a fair information practices code. Some participants felt that telecommunications providers and enhanced service providers should voluntarily develop and publish a national code of fair information practices regarding use, access, and control of transaction data. The code would be consistent with fair information practices principles (see Table 3) but institutions could tailor their implementations of the code to their own activities. Individuals would have the leverage of being able to take their business to a competitive provider if a carrier did not adhere to the code. Participants suggested that service providers should disclose to their customers how transaction data will be used and should restrict secondary use of transaction data, giving their customers various options ranging from partial or complete restriction to royalty-based use. Some participants wanted service providers to build control mechanisms into network architecture to minimize the risk that personally identifiable information could be collected from transaction data and employed for secondary uses.

B. The government should set up an information practices commission. The government should take the lead in setting privacy policies. Many participants felt that the federal government should set up an Information Practices Commission -- an oversight commission or umbrella agency charged with monitoring and regulating information and technology practices (including privacy), possibly modeled on European privacy commissions. Participants were unwilling to specify exactly what form the commission should take -- in particular, they were unwilling to recommend a permanent body. But they agreed that the commission should be an interagency entity with a broad mandate to consolidate the investigative and regulatory functions that now are spread piecemeal through the FCC and other agencies. They strongly concurred that the commission should take a more active stance than that of the current FCC, which many workshop participants felt has been overly passive in regard to network policy issues and consequently has harmed both American business interests and individual privacy. The new commission would initiate the discussions with affected groups and review carriers' fair information practice

policies.

- C. The government could legislate minimum national standards for privacy. Some minimum national standards might be legislated if a combination of voluntary codes and sector regulations is not adequate to protect individuals' control over their identifying information.
 - 1. Individuals' ownership of personal information should be strengthened, perhaps by a rule of "habeas data" allowing an individual to subpoena all the data held on him or her by an organization and to challenge the accuracy of that data.
 - 2. Regulations similar to the ban on autodialers should be considered to control the dissemination of intrusive information over networks.

- D. The government could establish user royalties and a National Information Market (NIM). One participant suggested that previous mechanisms to protect privacy in the United States have failed, and proposed development of national electronic markets in personal information (See Appendix D: Kenneth Laudon, "Privacy Beyond 2000"). In the NIMs:
 - 1. Individuals would sell information about themselves at a market clearing price. NIMs would be the only legal avenue for the transfer of information about individuals for secondary purposes.
 - 2. The markets would be self-supporting. A transfer tax would be charged and the revenue used to support the marketplace infrastructure, enforcement of rules, and monitoring activities. Some percent of the purchase price would also be returned to individuals as revenue to compensate them for the use of "their" information and for their cost of dealing with privacy invasion.
 - 3. Participation would be voluntary. Participants might be able to trace the flow of information about themselves, perhaps via a toll free 800 phone number.
 - 4. A Federal Information Clearinghouse would create and monitor the NIMs, develop data quality standards, develop privacy metrics, and advise Congress and the White House about privacy matters. Other participants argued that the market approach embodied in the NIM proposal would fail for several reasons. In instances where individuals or companies have clear ownership rights -- for example, in medical records, tax forms, or corporate employee records -- they contended that market negotiations do not generally occur. Thus, an information market probably would not produce freer or more efficient transactions than regulatory solutions would. The transaction costs of direct marketing are high relative to the value they produce, while inducements are low. Equifax experimented with a voluntary participation system similar to the proposed National Information Market in 1990-92, called "Buyers

Up." Consumers were invited to state what kinds of direct mailings they would and would not want to receive. They were offered inducements to participate, in the form of discounts and coupons. Equifax considered eventually charging a small subscription fee. But the experiment showed that consumers were unwilling to pay to reduce their mailbox clutter, and companies generally felt the cost/benefit ratio was too high. Although Equifax's investment in the experiment was substantial, the bureau abandoned Buyers Up after about 18 months. John Baker, director of marketing at Equifax, scoffs at the idea of making royalty payments to consumers. He believes that "Companies are not willing to spend much for [consumer data] because there are so many other ways to get personal information, including the telephone book, census data, and information about individuals which rightfully belongs to the companies they do business with.... You can't centralize ownership completely with the individual."

IV. SECURITY

- A. The ECPA should be extended to electronic networks. Workshop participants generally agreed that the Electronic Communications Privacy Act, which allows network operators to monitor wire (i.e., voice) communication to guard against damage and fraud, should be extended to wireless and electronic (i.e., data) communication.
- B. Tradeoffs to cope with cryptographic advances must be openly discussed. Although legal mechanisms exist that could allow the FBI and intelligence agencies to gain access to cryptographic keys, such mechanisms are not foolproof and may be overridden by advances in cryptography in some cases. Many privacy advocates believe that cryptography should be completely unregulated, despite the fact that it can pose a substantial obstacle to law enforcement and intelligence gathering. Several participants at the workshop, however, argued that several schemes could be used to regulate cryptography and protect legitimate law enforcement needs without unnecessarily compromising the privacy and proprietary interests of citizens. The workshop could not reach agreement about how to make appropriate tradeoffs between personal privacy and law enforcement. Some participants supported the FBI's Digital Telephony proposal (see Appendix F), which seeks to build surveillance capabilities into all existing and future computers and networks at industry's expense. Others, however, felt strongly that the intelligence and law enforcement communities should bear the full burden of gathering data. Further, they argued that requiring a built-in tapping capability could dangerously limit Americans' freedom and make American technology products non-competitive in foreign markets. The workshop took place before the announcement of the federal government's "Clipper" key-escrow encryption initiative. The workshop participants felt that market forces, not legislative efforts, ultimately will drive

the development of crypto-security solutions. Some options discussed included:

1. Escrowed secret keys. Users would be required to register their secret keys with an independent trustee, while cryptographic products would be designed to operate only with keys that are certified as being escrowed.
2. Using relatively weak cryptographic codes that could be broken when necessary by sophisticated intelligence equipment. Obviously, this solution would be unacceptable in many contexts, such as corporate communications where industrial espionage is a threat.
3. Regulating and licensing various levels of cryptographic systems. The chief difficulty here might be in determining which levels of information warrant which levels of security. Different types of information are collected for different purposes. An overriding authority is needed, perhaps in a privacy commission, that can gauge appropriate levels of security for each category of information.
4. Provider-generated session keys. Many cryptographic systems assign a "session key" to each encrypted communications stream, which is needed to decrypt any intercepted communication. The system usually destroys the session key after use. However, if a service provider participates in setting up the protocol used to create the key, the provider could then program the system to transmit the key to a remote government monitoring facility in response to a court-ordered interception. The system would still destroy the key after use.
5. No regulation. A completely unregulated market. Many participants were unhappy with all of these technical options—reflecting the fact that the computer community has not been regulated and does not want to surrender its relative autonomy. The dissent also spotlights the feeling of many experts that the time has come to make value judgments and tradeoffs in order to accommodate the competing interests of law enforcement and individual autonomy. The Information Practices Commission (see "Privacy," page 17) might be tasked with investigating these tradeoffs, since the discussion to date has generated much passion but little solid data on which to base a societal decision. The 1993 Defense Appropriation Act authorized a study of this issue, to be performed by experts under the auspices of the National Academy of Sciences, but it has not been started, seven months after passage of the legislation. Despite the sensitivity of much information about cryptography and other network security issues, the value questions they raise can be resolved only in a democratic forum. Debates aimed at achieving a satisfactory tradeoff between public and private interests should be made public, and dialogue between the parties needs to be candid and conducted in

good faith. Each side's unfamiliarity with (and, in some cases, contempt for) the other's culture has slowed progress. Until this culture gap is diminished, a "religious war" between the "unlimited-crypto" and "law-and-order" camps is likely to continue.

- C. Development of security policies that are uniform throughout the network should be discouraged. Since the expectation is that hundreds of thousands of smaller networks, with varying characteristics and subscriber needs, will comprise the national information infrastructure, it is impractical and inappropriate to try to establish a uniform security policy for all networks. The Internet exists (and prospers) under security guided by a variety of policies. The information superhighway system should be modeled after the Internet.
- D. Accountability must be balanced with anonymity. On a telephone network, the amount of damage that can be perpetrated by a single user is limited by the number of calls that a malefactor can make. On a computer network, no such inherent restriction exists. Normally, user information on universal networks should be traceable so that perpetrators can be held accountable for the damage they inflict. However, there also should be a means to assure users' anonymity in isolated cases where invisibility is justified for extraordinary reasons--for example, to protect whistleblowers or persons with AIDS. Unauthorized access could be controlled through billing systems that prevent users from accessing the system without paying. The billing system could identify users by name, or could avoid identification through some sort of electronic debiting system in which paying for access would be as anonymous as buying a newspaper from a stand or making a call from a pay telephone. Most important, whenever anonymity is granted there should be a concomitant mechanism to limit the functions that anonymous users can perform, in order to restrict any damage they might perpetrate anonymously. Accountability also needs to be determined in cases where personal information about an individual is compromised while it is being used or transmitted by another party, such as a credit bureau. The workshop did not produce specific recommendations on this issue.
- E. International coordination is needed. International coordination is needed between the security policies of the United States and its strategic partners.

V. INTELLECTUAL PROPERTY

- A. Network cultural norms should more fully recognize the public benefits of protecting intellectual property. The workshop agreed that, ideally, protection of intellectual property rights in the national information infrastructure will be generally recognized as beneficial to the community (as to some extent it is now on the Internet). The custom of making copyrighted materials easy and inexpensive to duplicate, which characterized networks in the 1980s, could hamper the growth and richness of the national information infrastructure if it

deters information providers from making their products available at fair prices. Education for the ethical use of computers could begin early in life, perhaps in elementary school.

- B. Intellectual property rights should be enforced in the national information infrastructure by suitable legislation and use of supporting technical mechanisms. Workshop participants agreed that the intellectual property rights that apply to information distributed in physical form (paper, floppy disk, or CD-ROM, for example) should be preserved when this property is distributed over networks.

GLOSSARY

Accountability: The property of being able to trace activities on a system to individuals, who may then be held responsible for their actions.

ATM: Asynchronous Transfer Mode, a call-routing architecture for packet-switched networks that is under development by the regional Bell operating companies and other common carriers. ATM will provide switching services among networks at speeds up to 45,000 times faster than those available on today's telephone lines. ATM disassembles information into "packets" that are loaded onto telephone lines and reassembled electronically at the receiving end, much like the Synchronous Transfer Mode (STM) format that prevails today. But unlike STM, ATM parcels information into packets of uniform size, enabling the packets to pass smoothly from one system to another—for example, from a desktop computer to a local telephone wire to a long--distance fiber-optic line--without slowing down for "protocol conversion," or technical translation, along the way.

Confidentiality: A status accorded to data that for, a defined reason, is deemed to be sensitive and must be protected as such. "Protection" means not only safeguarding the data against destruction or unauthorized change, but also limiting access to it only to authorized users. "Authorized users" may be established by law, by regulation, by professional custom, by organizational policy, by established historical uses, or by agreement among the members of some organized community.

Enhanced Service Provider: A vendor of value-added information services on a network.

Integrity: The quality in a body of data, a system, a network, a message in transit through a network, etc., of having the properties that are a priori expected of it. Note that such a definition does not require absolute accuracy, freedom from errors, complete specification, etc., of the entity in question. It only requires that whatever something was thought to be before the fact is indeed what it proves to be after examination. In some contexts, integrity is taken to mean assurance against unauthorized change. Since security safeguards control access, there is a clear interplay between security and integrity. Some safeguards will contribute to both goals.

ISDN: Integrated Services Digital Network, a technology designed to inexpensively upgrade the public switched telephone networks to accept digitally transmitted data, video, and graphic media in addition to voice. Basic Rate ISDN offers transmission speeds up

to 60 times faster than those available on existing copper-line telephone networks. Some public interest groups, particularly the Electronic Frontier Foundation, espouse ISDN as a low-cost way to bring advanced communications to residential and commercial users in the short term (three to five years), well before more expensive, fiber-optic digital networks become publicly available. But ISDN also has numerous critics, who observe that demand for the service has been sporadic since it became available a decade ago and disparage it as a solution in search of a problem.

Network: Use of the term is quite variable, especially to computer people who invoke it to indicate local area networks (LANs), wide area networks (WANs), computer networks, or networks of networks. For this report, "network" is defined in the sense historically used by the telecommunications industry: a transportation mechanism for the movement of electronic traffic. Its obligations are to move the traffic from originators of it to recipients chosen by the originators (i.e., to provide connectivity among subscribers); to do so in a timely fashion; and to deliver to the recipient the same information that was supplied by the originator, without loss of integrity.

Privacy: In the data context, restriction of the use of personal information to certain prescribed activities. Activities may be "proscribed" by law, by regulation, by organizational policy, by professional custom, by established historical uses, or by the members of an organized community. The intent is to protect individuals (as opposed to legal personages, such as corporations in the United States) against harm or unwarranted intrusion. "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

Security: The totality of safeguards that are present within and around a computer system or a network to assure that there is no unauthorized disclosure, destruction, modification, or denial of service within the system. Safeguards might include some or all of technological (software and/or hardware), procedural, administrative, management, physical, or personnel mechanisms. The salient feature of most safeguards is control of access--to data, to a system, to a network.

Service Developer: An individual, group, or organization that develops hardware/software for distribution or sale. Threat: Any circumstance or event with the potential to compromise the security of a system.

Transport Provider: A vendor of basic transport services for operation of a network. Generally refers to common carriers.

User: A person, organization, or other entity which requests access to and uses the resources of a computer system or network.

Vendor: A commercial supplier of software or hardware.

Vulnerability: A weakness in system security procedures, system design, implementation, internal controls, etc. that could be exploited to violate the system policy.

BIBLIOGRAPHY

Computer Systems Policy Project. "Perspectives on the National Information Infrastructure: CSPP's Vision and Recommendations for Action," Washington D.C., 1993.

Denning, Dorothy. "To Tap or Not to Tap," Communications of the ACM, Vol. 36 No. 3 (March 1993), pp. 26-33.

Electronic Frontier Foundation. "Analysis of the FBI Proposal Regarding Digital Telephony," paper presented at Third Conference on Computers, Freedom and Privacy, San Francisco (March 1993), pp. 6.15-6.21.

Garcia, Linda D. "A National Communication and Information Policy: Reconciling the Issues," invited paper presented to the George Washington University/NSF Workshop on Policy Questions Relating to Computer Networks, 1993 (see Appendix A).

Hoffman, Lance J. (ed.), Proceedings of the Second Conference on Computers, Freedom & Privacy, March 18-20, 1992, Washington D.C., Association for Computing Machinery, New York (1992).

Hoffman, Lance J. "Will 'Usually Secure' Cryptography Permit Bugging of the Digital Network?," paper presented at Third Conference on Computers, Freedom and Privacy, San Francisco (March 1993), pp. 6.22-6.24.

Hoffman, Lance J. "Bugging the Digital Network," Information Systems Security, Vol. 1 No. 4, Winter 1993.

Hoffman, Lance J. "Reducing Society's Vulnerability as Computers and Networks Proliferate," Education and Society ed. R. Aiken. Information Processing 92 vol. II. Elsevier Science Publishers. B.V. (North Holland): 1992.

Hoffman, Lance J. and Paul C. Clark. "Imminent Policy Considerations in the Design and Management of National and International Computer Networks," IEEE Communications Magazine, February 1991, pages 68-74.

Interuniversity Communications Council, Inc. (EDUCOM). Proceedings of the NREN Workshop, Monterey, California, Sept. 16-18, 1992. Kahin, Brian (ed.), Building Information Infrastructure: Issues in the Development of the National Research and Education Network, McGraw-Hill Primis, New York, 1992.

Laudon, Kenneth C. "Privacy Beyond 2000," invited paper presented to the George Washington University/NSF Workshop on Policy Questions Relating to Computer Networks, 1993 (see Appendix D).

Oldehoeft, Arthur E. "Foundations of a Security Policy for Use of the National Research and Educational Network," NISTIR 4734, National Institute of Standards and Technology, Washington, DC, 1992.

White House, Office of the President. "Technology for America's Economic Growth, A New Direction to Build Economic Strength," February 22, 1993.

Ware, Willis H. "Security Considerations for Data Networks," invited paper presented to the George Washington University/NSF Workshop on Policy Questions Relating to Computer Networks, 1993 (see Appendix B).