Governance and the Proliferation of International Electronic Markets

Presented Before The Seventh Conference on Organizational

Computing, Coordination and Collaboration

International Conference on Electronic Markets

Austin, Texas

November 8, 1996

By James B. Rapp

CyberStrategies

Alexandria, Virginia

ABSTRACT

A variety of issues and public policy decisions are increasingly important to the proliferation of international electronic markets. In the United States, and internationally, key issues under review include the imposition of access fees on data service providers, mandated universal Internet access, taxation of data service providers/goods and services, intellectual property/copyright, information warfare, and cryptography.

The Internet, an expected key information conduit for the proliferation of international electronic commerce, has been somewhat U.S. centric, in that the architects and users were a small elite male homogeneous population. Since 1995 this has changed due to: reduction of Internet funding/administration by the U.S. Government; the Internet user base has become heterogeneous, reflecting the makeup of society; regionalization of Internet architecture and telecommunication deregulation; lawyer interest in cyberspace.

Although the Internet has had few rules and regulations, an ad-hoc consensual governance process grew up to address Internet standards and engineering needs. While bodies such as the IETF, IAB, IANA, ISOC continue to play an important role, no longer can they promulgate rules in the vacuum previously enjoyed.

As the Internet truly becomes a global medium, many competing interests including national governments, multilateral organizations, consensual ad-hoc bodies, the commercial sector, and special interests will seek to mold laws and operating doctrines. This will cause network proliferation to be uneven. Countries favoring telecom deregulation, open markets, low taxes, minimal regulatory mandates, and freedom of information, will see low pricing and a boom in architecture, as well as commercial viability. Countries with closed markets, monopolistic telecommunications policies, and restrictive information laws will experience stagnant growth.

Although many of the existing nation specific rules and regulations in existence may have some place in the cyber governance realm, ultimately the borderless quality of international electronic markets will require the invention of new governance models and processes.

Introduction

In 1995, I brought to light various policy issues that a variety of governmental and non-governmental interests were reviewing or becoming aware of—as pertained to electronic commerce, the Internet, and cyberspace. I suggested that the hand of government and special interests would attempt to involve themselves in and effect some control over cyberspace. I also stated that the drivers of all of this were control by politicians, corporations, and special interests, media attention, and monetary related.

A year later, many of my predictions have come true, as government and special interests are now seeking control over the Internet and the international electronic marketplace in a big way.

The intent of this writing is to expand upon issues that I deem key to electronic commerce, namely: 1) U.S. Federal Communication Commission (FCC) review of access fee exemptions for Enhanced Service Providers (ESPs), and universal service; 2) taxation as pertains to goods and services sold over the Internet, as well as on-line service providers; 3) intellectual property and copyright; 4) information warfare; and 5) cryptography.

The ultimate "thread" will be to explore how the massive number of people now using the Internet, coupled with traditional special interests such as government bureaucrats, law enforcement, large corporations, civil libertarians, lawyers, are seeking to adapt conventional in-place rules and regulations to the unique global Internet architecture, and how it meshes with the consensual governance model that has built the Internet. Just as the wild west and most every other technology was "tamed" over time, the jury is out on whether the Internet may be less governable in a conventional sense, or in five to ten years it will be just another part of our daily lives with property rights, law enforcement, and cordoned off areas for commerce, expression, vices . . .

FCC

The U.S. Federal Communications Commission (FCC) is considering whether to include review of a provision enacted in the early 1980's which exempted data service providers from paying per minute access charges, typically imposed on long distance telephone calls, in upcoming access fee reform Local telephone companies want access fees imposed on Internet service providers (ISPs), claiming that heavy use is causing a degradation of voice service, and costly upgrades.

The 1996 Telecommunications Act formed a joint federal-state board to review whether the long-standing universal service goal of supplying inexpensive telephone service to the general population should be redefined to include new technologies such as Internet access.

The Clinton Administration supports Internet access for all schools, libraries and public places. Questions have arisen as to who will pay for all of this, and whether ISPs can be mandated to supply access, in that they are not regulated common carriers.

Taxation

Taxation issues are gaining prominence and will impact electronic commerce significantly. In the U.S., states and localities are seeking to impose taxes on ISPs or the users of such services. It seems reasonably clear that they may be able to do this in the case of local providers, but less clear when the provider is out of state.

States are also wrestling with the question of how to tax goods and services sold on-line. Constitutional nexus questions are under review, which limit the ability to impose tax collection/remittance on out of state sellers.

States are again reviewing "creative" nexus by trying to say that licensing of intangible property such as software, or agreements between in-state telecom providers, ISPs, and sellers creates "agency" nexus.

Leading tax experts believe that state and national tax systems do not work well in a borderless electronic commerce environment, and suggest that new tax models will need to be developed at the international level.

Intellectual Property

Producers of written content, software, audio recordings, video, and other items of value that may be digitized, are seeking protection in the digital age.

Content producers not only wish liability to be placed upon individual violators, but also On-Line and Internet service providers, and even telephone companies.

Congressional Legislation (H.R. 2441) is pending to address on-line copyright issues, however there is dispute over on-line service provider liability, distribution rights, and circumvention of technology.

A World Intellectual Property Organization (WIPO) working group, of which the U.S. is a participant, is formulating three treaties that cover on-line service provider liability, protections for producers of sound recordings, and database protections. The treaties will be introduced are intended to update the Berne Convention.

Information Warfare

Information warfare (IW) is a significant electronic age business threat.

Using the Internet, a competitor based thousands of miles away might "hack" into a company's computer database and steal millions of dollars of trade secrets, or maliciously compromise the database.

An attacker might also undermine the reputation of a company by putting out inaccurate information on Internet usenet groups, mailing lists, or the World Wide Web.

With the advent of easier to use "hacking tools," coupled with the explosive proliferation of computers, stored databases and information, as well as network access, the number of security breaches will only increase, as unfortunately, a large percentage of companies are not adequately prepared to fend off information attacks.

Cryptography

Current United States law allows the use of strong cryptographic product use domestically, but imposes significant limitations on exports.

The Clinton Administration has been a proponent of a key escrow/key recovery policy, whereby through court order, law enforcement would be able to recover keys enabling access to encrypted items.

Governance

Much of the computer industry, user base, civil liberty interests, and members of Congress, have not favored this policy, as they believe it is unworkable, violates privacy rights, and is harming the U.S. software industry.

Many factions of society are attempting to govern and impose their will on the Internet and international electronic market place.

The Internet was a "creature" of the U.S. Government, in that they funded the initial research and Internet backbone. The creators and users were comprised of a small elite homogenous male population of scientists, educators, researchers, engineers, military, and government types. A somewhat U.S. centric Internet evolved due to: foreign dependence on the U.S. Internet backbone for backhauling, data transit, and traffic termination; the bulk of Internet hardware/software originated in the U.S; the majority (64 % today) of Internet servers have been in the U.S., and English has been the dominant language.

The trend today is for the Internet, now comprised of a heterogeneous user base, to become less U.S. centric. This is due to: a reduction of U.S. Government support; exponential growth; international network deregulation; and lawyers.

Although the Internet and cyber world has been a somewhat anarchistic "wild west" environment, ad-hoc consensual governance bodies such as the IETF, IANA, ISOC, and ISOC have evolved, primarily to address Internet engineering and standards issues. The ad-hoc bodies have done an outstanding job in progressing the Internet, however, fissures are appearing in this process, as they enjoy no real legal authority. The heterogeneous nature of Internet users/interests, will no longer allow these groups to operate in a relatively unencumbered vacuum.

The Internet, the expected twenty-first century electronic commerce conduit of choice, has flourished in the U.S. due in large part to a hands off approach, the free flow of information, a deregulated telecommunications environment, and a lack of taxation and access charges.

Outside the U.S. Internet growth has been apparent in markets with deregulated telecommunications policies, and less expensive Internet pricing. The opposite has been true in heavily regulated, non-competitive markets. This has led to uneven Internet growth.

The U.S. and other countries would be well served to move cautiously in imposing new taxes, access fees and universal service mandates, or risk killing the goose that laid the golden egg, so to speak. The Internet will become less U.S. centric as regionalization of traffic becomes a reality. As networks/content servers become globally distributed, and caching models are put in place. This will affect Internet traffic patterns, and electronic commerce in a big way, not just technologically, but policy and governance-wise as well.

Corporations will evolve from nation-specific to regional, and will look to the Internet as a way to communicate with far-flung staffs, customers, and trading partners,

Significant tension will occur, as various factions seek to govern Internet/Electronic Markets (i.e. governments, multilateral orgs., consensual bodies, private sector, special interests, lawyers).

Markets that restrict information, in keeping with traditional political norms, will lag in the international electronic marketplace.

The jury is out as to whether the expected emergence of five to six global communications providers, coupled with fewer ISPs will enable governments the control they so cherish, and how this may impact electronic commerce.

In any case, Governments and special interests must look for new governance solutions compatible with technologies and a marketplace that transcends physical boundaries.

I. Federal Communications Commission (FCC)

The U.S. Federal Communications (FCC) regulates common carrier telephone service, as well as broadcast television, and radio. Two key issues are under review at the commission that impact data service providers:

Enhanced Service Provider Provision

In 1982 the FCC implemented what is known as the Enhanced Service Provider (ESP) provision to encourage the proliferation of On-Line services, which at the time were minuscule.

The ESP provision pertains to data-only service providers, and exempts them from paying high access fees typically incurred by long-distance carriers to local telephone companies. Specifically, companies, including Internet service providers (ISPs), pay end user business line rates with no usage charges for receiving calls from their subscribers [ESP96]. In contrast, long distance telephone companies pay a per minute access charge, which can account for as much as half of all long distance call charges [ACCESS96].

In that Internet and On-Line use has grown exponentially, local telephone access providers such as Bell Atlantic®, PacTel®, and GTE® are petitioning the FCC to revoke or modify the ESP exemption, arguing that voice users now subsidize data users (i.e. primarily Internet), claiming they spend significant amounts of time On-Line, tying up their equipment—as compared to traditional voice users. They assert that inexpensive flat rate Internet dialup service is a key factor. In their estimation, the imposition of timed access fees, similar to long distance carriers, would either reduce usage or bring in revenues for equipment and capacity upgrades.

A key argument by service providers exempted under the ESP provision is that they are "users" of telecommunications services, not common carriers. Further, they believe that a costly change of this nature would harm smaller (ISPs), as it is difficult to "draw lines between large and small carriers" [ACCESS96].

The FCC will make a decision by December 1996 as to whether the ESP exemption will be included in an overall review of the current access fee scheme [WERB96].

The Commercial Internet Exchange (CIX), an international trade association that represents Internet access providers, is actively reviewing proposals that seek to eliminate or modify the ESP provision. Barbara Dooley, Executive Director of CIX,

believes the implications for change to the ESP provision are very grave, because it could impact development of the industry, and also opens up tangential issues such as the level of state taxation [CIX96].

In an interesting twist, CIX and ISPs have proposed to the FCC that they be allowed to lease lines that lead to customers' houses and operate their own switchingequipment on Bell company premises. By leasing lines, the ISPs would avoidpaying all or nearly all charges for accessing local telephone networks. The CIX and the ISPs argue the approach would remove a burden from the conventional voicenetwork which was never designed to handle Internet traffic, and mitigate the need for access charges [BYPAS96]. Based on FCC statements it is difficult to gauge whether any change will take place. Chairman Reed Hundt states: "now with Internet usage skyrocketing, some people are saying that we should subject Internet service providers to the access charges paid by long-distance carriers. I disagree, you don't pour new wine in old bottles and if we applied these old access rules to new technologies you'd have every reason to whine. Instead, let's just break the old bottle—in fact, the bottleneck of exchange access" [HUNDT96].

These statements indicate that it is unlikely that Internet service providers will be subject to wholesale revocation of the ESP provision, but there is a reasonable probability this issue will be a part of near-term access fee review and reform.

Universal Service

Historically, the long-standing governmental commitment to the achievement of universal service has meant the guaranteed widespread availability of "basic" plain old telephone service (POTS) at affordable rates throughout the United States. However, recognizing that data communications are becoming mainstream and an important daily component of life Congress mandated in The Telecommunications Act of 1996 that the FCC hold meetings of a Federal-State Joint Board to revise the governmental policy on Universal service to reflect the digital information age. The Board is reviewing whether Internet access, among other technologies, should fall within any redefinition [UNIV96].

The FCC Chairman, and indeed the Clinton Administration, have come out strongly in support of expanded Universal Service. They are adamant that libraries and schools receive Internet access. FCC Chairman Reed Hundt has stated that the Commission "will vote next year (1997) on a new universal service funding mechanism," and raises the question of whether "they should vote to network all (of) the classrooms in the country" [HUNDT96].

A reformulation of universal service raises many questions such as:

- Will universal Internet service be required for all residences, or perhaps be limited at first to schools, libraries, and public gathering places?
- Will this service be free or subsidized, and if so at what level of service?

- Will customer premises equipment (CPE) such as computers be a requirement?

Out of all of this a key question arises as to who will pay for expanded universal service, and the mechanism(s) to collect payment. Traditionally, long distance access charges have been utilized to provide POTS universal service. This is why the Commission may want to review the ESP exemption, as it could be a revenue stream to help fund a redefined Universal Service. In fact, Congress gave the FCC discretion to impose universal service charges on "other provider(s) of interstate telecommunications to contribute to the preservation and advancement of universal service if the public interest so requires" [TEL96]. However, in that ISPs are not regulated common carrier monopolies, legal scholars question whether they should fall under FCC jurisdiction. In which case, so the argument goes, a private company should not be forced to subsidize Internet connectivity through a universal service mandate.

In order to counteract this and other arguments, the FCC has reviewed their legal authority in respect to Internet and ISP regulation, justified to some extent by the ability to conduct Internet telephone conversations [PHON96].

Dave McClure, Executive Director of the Association of On-Line Professionals (AOP), a trade group that represents Internet and On-Line service providers says there is no clear evidence yet that the Internet is such an integral part of life that the industry should be taxed to guarantee low cost universal access, an issue he claims the FCC is also struggling with.

McClure also points out that much of the universal service talk centers around children and education. Although he believes that there are certain aspects of the Internet that might be of great benefit to children, he is not convinced that every child needs Internet access.

Lastly, he points out that a secondary high speed (vBNS) government funded backbone structure, dubbed "Internet 2", is underway and will eventually link up around 100 universities and research sites. He wonders if this could not be used to link various schools, and if so, he questions the point in giving every child in America access to the "commercial" Internet.

Ultimately McClure believes it is premature to consider universal service mandates, and access fees on a fledgling two year old industry that has not yet proven it can survive, particularly in the case of smaller data service providers [MCCLU96].

Chief executive officers (CEOs) of twelve large U.S. computer companies have urged the government not to mandate through new regulations universal service for data transmission conduits such as the Internet, but rather develop a new framework to encourage "economic and social growth on a global scale" [CEO96].

In fact a number of private or public/private sector efforts are underway to facilitate universal access in the digital age including:

- Libraries On-Line, an initiative launched by Microsoft CEO Bill Gates and New York City Mayor Rudolph Giuliani, which is a $10.5 million philanthropic initiative to help library systems in economically disadvantaged communities nationwide provide public access to the Internet and multimedia personal computers. [LIBR96]

- In Massachusetts, stifled by bureaucratic red tape and budgetary limitations, thousands of volunteers decided to move forward in connecting more than 400 of the state's 2536 schools to the Internet. Major high-tech companies like Wang Laboratories®, Sun Microsystems®, 3Com®, and Digital Equipment® donated equipment. [MASS]

- The State of Tennessee and NCR Corporation have teamed up to implement the Connect Tennessee Students program (ConnectTEN), the first state-wide system that enables every school in Tennessee to be connected to the same network. ConnectTEN will eventually connect over 1,100 public schools grades K-12 in 95 counties [TENN96].

Decisions by the FCC in regard to the imposition of a universal service mandate and new fees are very important. The Internet in the U.S. has flourished to a great extent due to low pricing and little government regulation. Although access for all citizens is a laudable goal, the FCC should move carefully and also review new models.

II. Taxation

United States

U.S. federal, state, and local revenue authorities are busily reviewing, and in some cases implementing, taxation schemes on network service providers, and goods and services sold via electronic network conduits. In the case of state and local governments they have seen significant erosion of taxes collected on long distance telephone charges, as per minute rates have declined markedly. Rather than impose visible taxes, such as on property, revenue authorities are seeking taxes that are less visible, or "hidden taxes," so to speak. The demographics of Internet subscribers are attractive (i.e., affluent, educated), and thus the lure of taxing Internet and other On-Line services is compelling.

Network Service Providers

A number of U.S. states (Connecticut, Massachusetts, New York, Ohio, Pennsylvania), and cities (Austin, Texas, Fort Lauderdale, Florida, Fort Collins, Colorado) are considering, or actually levying taxes on ISPs, or their users [ISPTAX96].

Most of these states and municipalities are taxing (or have their eye on) not only in-state based ISP's and/or their customers, but providers based in other states that service customers in their jurisdiction. Under U.S. law this raises some question as to ***nexus*** or taxable presence (see Addendum I: Nexus). If a customer in one state utilizes an ISP in another state, and sends messages that utilize connections in still other locations—where does jurisdiction rest [NETTAX96]?

For example, states such as Massachusetts, have begun charging a 5 percent On-Line service tax, which applies to all On-Line users and providers, regardless of whether the provider has a physical presence in the state [TAX96].

Some members of the legal community believe it is a conflict with current law to collect taxes from companies without a strict physical presence (***nexus***) based on a 1992 Supreme court ruling known as Quill (see landmark ***nexus*** case, Quill v. North Dakota, 112 S.Ct. 1904, 1992). They assert that this same ruling should apply to On-Line access providers as well [CSM96].

Dave McClure, of the (AOP) feels that it will be difficult for states and localities levy taxes on out of state ISPs (or users of out of state ISPs) due to lack of provable Nexus, however, he believes they will be able to tax in-state providers and/or users. Should this be the case, it is his assertion that smaller ISPs will be at an economic disadvantage to out of state providers, which could drive them out of business, causing job loss and erosion of any tax base

McClure also believes that in the long-term the taxation question will come down to whether Internet access is a service utilized to develop an end product, or is in itself an end product, and will be determined by how the Internet is used. He argues that Internet access is a service used in the creation of other products, and thus, just as legal and advertising services are not taxed because they are not an end product in themselves but used to create taxable products, neither should Internet access be taxed at the local, state, or federal level [MCCLU96].

Goods and Services

A far more complex situation pertains to the taxation of goods and services sold over electronic delivery conduits such as the Internet. Although the level of commerce has been relatively small, it is expected that this will significantly change.

Sales and use taxes are a primary revenue source for states and municipalities. In 1994, one third of state tax revenues, $123 billion, was derived from sales taxes [CSM96]. In that a number of states, for example Connecticut, are lowering income taxes, sales and use taxes take on added importance.

Sales and Use Taxes

Sales taxes are taxes imposed on the purchase of tangible personal property, and in some instances non-tangible services on transactions that take place within a state.

The sale of goods and services that occur outside of the state of origin are subject to what is known as a "use tax." The use tax is meant to ensure that the state of origin will receive revenues on cross border transactions.

Due to collection difficulty associated with use taxes, states attempt to place the collection and remittance burden on the seller. If the seller has some sort of physical presence, nexus, in the state where the goods or services emanate, then it is their obligation to collect and remit the taxes. However, if they do not have a physical presence, they are not compelled to collect nor remit taxes to the state. In this instance, it is the duty of the purchaser to remit the tax [SIA96].

The use tax has primarily been on the books to cover mail order purchases; however, with the advent of the World Wide Web, and expected explosion of electronic commerce, methods are being reviewed as to applicability in this setting.

A survey by the Software Industry Coalition found that use tax collection enforcement on buyers "varies widely from state to state," from no enforcement to modest enforcement on specific items. The survey concluded that "state collection of use tax from buyers is largely non-existent."

The survey further indicated that tax collection was negligible due to most buyers being unaware they even owe a use tax; and the lack of an easy payment mechanism [USETAX96].

The Nexus Issue

As is evident in the taxation of both On-Line service providers, and goods and services, the issue of ***nexus***, or in-state physical presence plays a crucial role.

Two theories are being explored by state representational authorities such as the Washington, D.C. based Multistate Tax Commission (MTC), as a rationale for requiring out of state vendor liability for tax collection/remittance (i.e., ***nexus***). The two theories are:

1) Licensing of intangibles creates ***nexus*** for use tax collection.
A state might say that a product sold on the Internet, for example licensed software, has nexus due to the presence of licensed property in the state.

2) The concept of agency.
The agency concept embodies the theory that along the chain of business relationships involved in the use of conduits such as the Internet, a physical presence is presumed in

the state. This is often associated with telephone equipment. Thus, the argument goes that ***nexus*** accrues to the communications provider (since they own the in-state physical property), the Internet service provider (they utilize the in-state equipment), and seller, as all three parties have entered into agreements with one another. Thus, anything associated with the utilization of the communications provider equipment is deemed to incur nexus.
Debate is taking place as to whether this is legal, or "another iteration of the pre-Quill claim"(see landmark ***nexus*** case Quill v. North Dakota, 112 S.Ct. 1904, 1992) which was the practice of creating ***nexus*** based upon the use of telephone, credit card, and banking systems [CALD96].

It seems clear that states and localities are using the agency concept to tax On-Line service providers, and will use both agency and licensing to tax goods and services sold by out of state vendors via electronic network conduits.

In that states again seem to be expanding the concept of nexus it seems almost certain that the issue will wind up in the courts.

Paull Mines, General Counsel for the Multistate Tax Commission believes that a unique characteristic of electronic commerce is that it may well have the ability to solve many of the problems that makes state taxation of multijurisdictional commerce difficult. However, he feels that states will have to be willing to leave traditional thinking behind in that:

1. State taxation of inherently multijurisdictional commerce cannot be solved unilaterally. Each state tax system is not a stand-alone module but an integral part of a national system that must operate cooperatively.
2. Embedding state tax systems into electronic commerce that ensures easy and transparent application of the rules may well be all important.

Mines states that "electronic commerce is making geography and goods less important and services and intangibles much more important" [MINE96].

International Taxation

Bit Tax

A so called "bit tax" has created controversy in various quarters of the On-Line world. The argument by bit tax proponents is that "the new wealth of nations is to be found in the trillions of digital bits of information pulsing through our networks, " and in order to derive public revenue, a tax on each digital bit of information (i.e. bit tax) should be instituted.

It is proposed that implementation of the tax would fit into three broad categories:

- Local Traffic. A variable rate based on a statistical average of gross information flows captured at each local switch using software already in place.
- Long Distance lines (public). A tax directly proportional to digital flows between major long-distance nodes in the country.
- Leased Lines (private). A fixed rate dependent on the bit-carrying capacity of the line.

The tax is not user pay, but a transparent metered scheme remitted to governments.

Collection and remittance to taxation authorities would be accomplished by telecommunication carriers, cable systems, and satellite networks.

A rate of .000001 cents/bit (or 1 cent per megabit) has been suggested, although an optimal rate has yet to be worked out [CORD95].
Arguments put forward by Bit Tax proponents include:

- The new information economy means a lessened role for physical goods that were easily identifiable (and taxed). Digital information means the need for a new method of taxation to stay current with the times in order to avoid massive public revenue loss.
- Network congestion might be reduced. At present, there is no rationale to limit the amount of information sent due to cost factors. Even though the Internet continues to scale in capacity there are fears that the increase in users coupled with bit hungry applications such as video could cause problems. A bit tax might cause there to be less non-useful material transmitted, and thus mitigate the problem.
- An increase in worker productivity could occur, as companies would have a greater incentive to make sure that employees did not waste time by playing On-Line games, sending personal e-mail, and spending hours visiting various world wide web sites.
- Intellectual property rights issues might be resolved. A bit tax requires the itemization of usage, thus it could be developed to assist in the collection of intellectual property royalties [SOETE96].

Arguments Against a Bit Tax.:

- The bit tax idea, only a very minor part of an interim report, has received a great deal of publicity from private individuals, who seem to be the most upset, fearing state interference as an attempt to tax freedom of speech.
- Not Possible? Feedback on the proposal has indicated that some believe it is “a nice idea,” but implementation may not be possible at the European level, and may have to be set at a world level—a daunting task [BIT96].
- Other arguments include: “bits” are or will soon be an irrelevant measure of transmission intensity; bits are difficult if not impossible to monitor; “broadband” capacity is in effect infinite [SOETE96].

Conclusions

As may be apparent, a hodge podge of taxation schemes are being reviewed or implemented as pertains to electronic commerce. This is evidenced by the European Bit Tax proposition as well as the establishment/review of policies by some states that govern location-of-commerce questions for electronic commerce in terms of state and local tax. But the question has not been addressed on the international level.

Nilesh K. Shah, an international tax consulting partner in KPMG's Information Communications and Entertainment (ICE) practice has studied the issue extensively and is convinced that "to truly address the myriad of issues raised by electronic commerce the OECD countries will have to enact a whole new set of international tax rules. The current rules are simply inadequate and antiquated."

Shah goes on "clearly, the rules that were made in the Industrial Age cannot be applied to the new Information Age. These new rules are still to be made---with as yet unforeseeable consequences for Net commerce."
Shah also believes that advances in encryption technology over the next few years, coupled with digital cash technologies, pose additional tax enforcement problems, unanticipated at this time. His solution is a serious attempt needs to take place to bring government, industry, academic, and tax professional interests together across boundaries to come up with viable solutions that are not so burdensome that they hinder the progress of electronic commerce. He also feels that international coordination is important and that the new systems need to be applied consistently to avoid further compliance and enforcement problems [INTAX96].

Although Nilesh Shah (and Paull Mines of MTC) are on the right track when it comes to the need for new models for electronic commerce taxation, I believe that for technical, and pure political reasons, the whole process will be very long and drawn out. Thus, in the short term, look for continued ill-conceived attempts to fit 20th century tax models to 21st century electronic markets.

III. Copyright/Intellectual Property

Producers of written content, software, audio recordings, video, and other items of value that may be digitized, are seeking protection in the digital age. Specifically, via mediums like the Internet, producers are fearful of massive unauthorized copying and distribution without compensation.

In 1995, the U.S. Commerce Department and U.S. Patent and Trademark Office released a White Paper which recommended amending the copyright law to cover the digitally networked environment [IP95].

In response, the U.S. Senate introduced (S. 1284), intended to "amend title 17 to adapt the copyright law to the digital networked environment of the National Information

Infrastructure" [SEN95], and the U.S. House of Representatives introduced HR 2441 for the same purpose.

Although there has been little controversy over formally extending traditional copyright protection to electronic transmissions, the question of copyright liability has become heated. Specifically, content producers not only wish liability to be placed upon individual violators, but also On-Line and Internet service providers, and even telephone companies.

The service providers believe it is impossible to be responsible for copyright violations, however, at a minimum, content producers want providers held liable when the infringement is brought to their attention and no action is taken [COPY96]. Legislatively, there has been little movement (i.e., concrete steps toward passage by Congress) on S.1284, however, HR 2441 has come close to being moved out of congressional committee for a vote, but has remained stalled because of three issues:

1. **On-Line Service Provider Liability**. Points of contention remain over the On-Line service provider liability issue between the telephone companies and copyright owner (i.e. content producers) special interests. At the request of Congress The U.S. Patent and Trademark Office (PTO) is formulating an Administration position on On-Line Service Provider (OSP) liability. This has to do with a desire by telephone companies to see issues of liability resolved, as they want to be exempted from liability when they serve as a mere conduit. Thus, the PTO is attempting to come up with language that excuses telephone companies from any liability, if truly passive, and some compromise on situations that are in between. The in between gray area is where difficulty in reaching a suitable accord lies.

Also at issue, ISPs do not want to be held liable for any content flowing through their service, with the exception of direct infringements they might be a party to. Content producers want full content infringement liability to accrue to ISP's. A middle ground is being sought. Thus far, the PTO believes that there should not be liability for merely supplying search engines, or facilities for doing hyperlinks or activities of that nature. However, questions arise, such as once the search engine or hyperlink supplied by the provider is used linking the user to “hot spots” where there may be infringement, should the provider incur some sort of liability? This gets to the issue of pointing out infringements to ISP's, as it is murky to tell when an infringement is for real [KEPL96].

.

2. **Distribution Right.** The distribution right conflict pertains primarily to terminology and meaning contained within pending copyright legislation. Specifically, broadcasters are concerned that transmissions of digitized content will be deemed simple “distributions,” rather than “performances.” A whole different royalty scheme comes into play in that broadcasts classified as “performances” pay royalties to performance right societies, however if classified as “distributions,” additional royalties must be paid for distribution of the work (for example to record label owners), because a perfect copy can be made.

3. **Circumvention of Technological Protections**. A point of contention between consumer electronics manufacturers, computer manufacturers, and copyright owners, is the circumvention of technological protections. Copyright owners want to protect their material On-Line to avoid piracy, and do not want devices manufactured that would circumvent technological protections. However, computer owners are worried that since there is no standard on the Internet like there is, for example with VCR's or tape recorders, and they are not aware of certain kinds of anti-circumvention or encryption technology, they could accidentally override it , potentially losing whole computer lines and putting significant monetary amounts at risk. In response, the copyright holders say they may need to change the type of encryption on their material very often to prevent users from getting into it and thus there cannot be a standard. Thus, their position is that the computer manufacturers should be responsible for not making something that purposely overrides protections.

Although these three major areas of contention must be resolved, it is expected that various factions will be at a much closer point of reaching an accord when the issue is taken up by the next Congress.

Mitch Glazier, Assistant Counsel, House Subcommittee on Courts and Intellectual Property sums up the difficulty in formulating new law by saying, **"*this is like reacting to the printing press, or copy machine, this is a major change in the flexibility of the copyright law, because of this new medium***. To be able to get as close as they (i.e., On-Line service providers, content producers, Executive/Legislative Branch interests) got in one Congress is a major achievement" [GLAZ96].

The U.S. and International Copyright

The U.S. Patent and Trademark Office (PTO), under the leadership of Commissioner Bruce Lehman is pressing for international copyright reform. Commissioner Lehman heads up the U.S. delegation to The World Intellectual Property Organization (WIPO), a specialized United Nations (UN) agency responsible for the administration of the international intellectual property treaties.

A WIPO working group has drafted intellectual property and copyright treaties expected to be introduced during the December 1996 Berne Convention, the principal international copyright convention (see Appendix II: International Copyright).

The three key treaties under review by the WIPO working group are:

1) **Berne Protocol.** The Berne Protocol treaty contains a transmission right section pertaining to pertaining to On-Line service provider liability. Also contained, is a circumvention of technological protections section. as well **On-line/Internet proposal**. This includes portions of the 1995 PTO White Paper, as well as HR 2441.

2) **Phonogram.** The “phonogram” treaty will seek to improve international protection accorded to producers of sound recordings as well as performers. Under European theory of authors rights, the rights of sound recording producers are protected under a system of neighboring rights, not copyright, therefore in accord with civil law legal tradition, there have to be separate treaties to take into account the interests of performers and producers of phonograms, which the U.S. would regard as copyright rights, as generally do other common law countries.

The net result is that whenever you have a negotiation to improve copyright protection, you also have to look at the neighboring rights treaties as well, and how you can keep those rights parallel (or roughly so).

3) **Database Protection.** There is interest at the international level in providing a new system for the protection of certain rights in respect to databases. Here in the U.S. The U.S. Supreme Court handed down a decision on a case, Feist, throwing out some 70-80 years of established law that accorded expansive protection to compilations of information, and cut back the scope of copyright protection for databases.

Specifically, the White pages of a telephone book, stock market quotation databases, Lexis-Nexis databases, and everything in between are entitled to copyright protection under current law, however difficulty has arisen following the Feist decision. The old copyright principal was if you expended enough effort, “sweat of the brow” so to speak, into putting a compilation together, you were entitled to copyright protection. Thus, for example, the telephone White Pages were copyright protected, but the Supreme Court said in the Feist Case, that "sweat of the brow" is not sufficient for copyright protection as relates to compilations, arguing that the element of arrangement is not there, say in the example of the White Pages. Following the Feist case, courts have interpreted very narrowly, holding that the telephone company Yellow Pages are copy protected because you have advertisements that can be placed in different places on the pages, have some arrangement, and in short different choices to be made.

The difficulty arises in determining what constitutes infringement. In order to infringe a database where the authorship is very thin, you have to take virtually the entire database, including the arrangement, selection, and distinguishing characteristics. Thus, taking even half of a database may not be an infringement. So, for example, the Standard and Poors stock market database is conceivably left with very thin copyright protection.

Because data is being taken, repackaged, and sold with no consequences , there is an interest in establishing a new kind of protection against the unfair extraction of information from databases in order to restore some sort of pre-Feist "sweat of the brow" threshold [KEPL96].

Two events must happen after the President, or PTO Commissioner Lehman, signs off on the Berne convention in order to impact U.S. law:

1) The Senate must ratify it, and
2) There must also be implementing legislation.

Criticism to the U.S. effort to amend the Berne Convention has emerged. Internet groups like the Digital Future Coalition note that PTO has included language from their 1995 White Paper [IP95] in the WIPO amendments to the Berne Convention, which may signal a potential end run around Congress [LEHM96].

Some industry followers also indicate that politics may be playing a role in the type of amendments being prepared for the Berne convention. The amendments are very favorable to the U.S. recording industry, as well as other content producers, special interests that have been very politically active [RODG96].

However there is reported bi-partisan support in Congress for this international effort, because they (the WIPO working group) are willing to provide exceptions to the treaty that will protect Congressional area(s) of interest, such as On-Line service provisions.

Lastly there are civil libertarian voices like self proclaimed "cognitive dissident" John Perry Barlow, who believe that the cyber world does not lend itself to conventional copyright rules. He believes that conventional property right conventions work fine when dealing in a world with easily definable physical boundaries. However, he views cyberspace as an intangible "relationship model," where the model is to create a direct relationship between the creator and audience. He does not seem to believe that conventional copyright laws will work very well in a digital world, and that government should show restraint in making rules, as it is a medium they know very little about [BARL96].

IV. Information Warfare

Information warfare (IW) as defined by the U.S. military is "actions taken to achieve information superiority by affecting adversary information, information based processes, information systems, and computer based networks while defending one's own information, information based processes, information systems, and computer based networks [JCS96].

Although this is a military definition, it is appropriate for the commercial sector as well. Today's wealth is increasingly comprised of digital bits that convey information or perform specific tasks. Competitors, governments, terrorists, and even disgruntled employees will go to extraordinary lengths to steal or disrupt this resource.

The largest manifestation of information warfare could be attacks that bring down banks, stock exchanges, electrical utility power grids, train traffic control networks, and telephone switching systems, or (ISPs) [IWAR96].

Although it is not generally believed that large scale attacks of this nature have occurred to any real extent (this may or may not be the case), there are signs that this may be beginning to change. For example in September 1996 a very blatant "denial of service attack" took place against Public Access Network Corporation (Panix), an ISP based in New York. Through an attack known as SYN flooding the attacker was able to exploit a weakness in the overall architecture that makes up the Internet, and effectively shut the service down. What this attack pointed out is just how vulnerable a network can be, and the importance of taking preventative steps, as well as the need for backup systems [SYN96].

Information Warfare at the corporate level is about stealing vital trade secret information, destroying or changing important information, or releasing inaccurate information that does harm to the organization.

Using a computer network like the Internet, a competitor based thousands of miles away might "hack" into a company's computer database and steal millions of dollars of trade secrets, unbeknownst to the victim. Alternatively, information on the same database could be maliciously changed and manipulated, escaping detection until potentially serious consequences resulted from the attack.

To make matters worse, the competitor could undermine the reputation of a company by putting out inaccurate information, perhaps on Internet usenet groups, mailing lists, or distributing fraudulent press releases on the World Wide Web [HAENI96].

A few cases of significant corporate information subversion have occurred. For example, in 1994 a Russian based computer hacker broke into Citibank's funds transfer system and took more than $10 million dollars before being apprehended (all but $400,000 was reportedly recovered)[IWAR96].

Although, there do not appear to have been any catastrophic incidents as a result of corporate information pilferage, the true scope is unknown, as skilled hackers leave few clues, and it is suspected that companies are reticent of revealing security breaches for fear of additional attack, and perhaps they do not wish bad press or embarrassment.

With the advent of easier to use "hacking tools," (see Appendix III: IW Weapons) coupled with the explosive proliferation of computers, stored databases and information, as well as network access, the number of security breaches will only increase. Additionally, as has generally been the case in the past, it is thought that today's hackers are not merely youthful pranksters out to break into a system simply as an intellectual exercise, but are now being paid money by competing companies and even foreign governments to steal information or wreak havoc.

Other factors that makes information warfare so appealing is the cost can be comparatively inexpensive, and accomplished from many thousands of miles away.

Unfortunately, a large percentage of companies are not adequately prepared to fend off information attacks. A Datapro survey comprised of 1,342 valid corporate responses found that:

- 68 percent of the surveyed population was concerned about Internet related security threats, however, only 15 percent used encryption protection, and 28 percent had firewalls in place.
- Most information technology supervisors fail to implement a disaster recovery plan, even though they recognize the importance.
- Computer viruses and malicious code were seen as a significant threat by two-thirds of survey respondents, are reportedly more prevalent outside of North America. Specifically, Latin America (61 Percent), Europe (60 percent), United States (52 percent), Canada (44 percent). It was suspected that greater utilization of virus protection software was in part responsible for a lesser problem in North America [SECU96].

U.S. Government Information Warfare Initiatives

The U.S. Federal Government recognizes the potential risk that information warfare poses and is taking steps to address the matter. They are:

- The National Information Infrastructure Protection Act makes it a felony to trespass in a computer system and use more than $5,000 worth of computer time. The law makes illegal the transmission of threats against computer networks that transcend state or international borders. Federal penalties are established for the theft of computer information across state lines [CLINT96].
- The Cyber Security Assurance Group, directed by the FBI, has been established to investigate and respond to information warfare threats [ZUCK96].
- The U.S. military has established the Centers for Information Protection [TARG96].
- The Commission on Critical Infrastructure was created in July 1996 to develop a policy to deal with information warfare issues [IWAR96].

International Information Warfare Initiatives

Internationally, “Lathe Gambit, “ the code name for a group of NATO information warfare experts, meets and collaborates on the extent of the problem and development of solutions [ZUCKM96].

V. Cryptography

Relevant encryption systems are crucial to secure electronic financial and business transactions.

Current United States law permits the use of strong encryption technology for domestic applications, however, the exportation of strong encryption products is restricted. (see Appendix IV: Cryptography Policy).

Heated debate has occurred between government and law enforcement interests that favor encryption systems they can access, and commercial/privacy interests that do not desire any unauthorized access, and wish to use the strongest products possible in exportable encryption products.

At the heart of the matter has been a fundamental debate over the merits of what is termed a key escrow system. "Keys" are strings of computer code that lock and unlock data. Under a key type system, by court order, government and law enforcement would be able to access decryption keys maintained by third party private sector government approved escrow agents.[♣]

Another major element of U.S. government cryptography policy has been the limitation on key length to 40 bits. This is important, as the shorter the key size, the easier it is to defeat the encryption scheme through what is known as a computer brute force attack (i.e., attempting many numerical combinations until the code is broken).

One might ask why the government would concern itself with restricting key bit length if a "backdoor" decryption method exists with a key escrow system? The answer is through a brute force computer attack, the U.S. government wants to maintain the ability to defeat any encrypted item, in the event the key is unobtainable.

In order to garner support, various U.S. government key escrow proposals have been floated, but to date not implemented, due to scant support (and in many instances downright hostility) outside of government and law enforcement circles.

Cited as problematic by many industry and privacy interests has been:

- Interoperability and other provisions are viewed by many as vague and a backdoor method to impose a key escrow or other limited system domestically.
- Proposed key length increases on exportable key escrow products have been thought by some to be inadequate given the continuing increase in computing power.
- Limitations on key strength might afford government (and other parties) a secondary method of decryption beyond the key escrow system.
- Various key escrow schemes which in one proposal would have forced users in other countries to utilize U.S. based escrow of all keys until bi-lateral access agreements were in place. U.S. commercial interests believe this is unacceptable to international commercial interests, citing lengthy treaty negotiations and administrative burdens, among other factors [DW95].

[♣] In certain cases, "reputable" corporations will be allowed to self-escrow keys, however, they are still liable under court order to make them available to government and law enforcement interests.

In October 1996, the Clinton Administration proposed what is termed a “key recovery” system. Rather than a single key being escrowed with one third party agent, it would be broken up among two or more trusted agent companies, which so the thinking goes, would further limit access and allay privacy and tampering fears—while meeting law enforcement and intelligence gathering needs [CODE96].

The Administration’s proposed key recovery system is mostly conceptual, therefore an alliance of eleven major hardware and software companies (Apple Computer®, Atalla®, Digital Equipment Corporation®, Groupe Bull®, Hewlett Packard®, IBM®, NCR®, RSA Data Communications®, Sun Microsystems®, Trusted Information Systems®, UPS®) have formed to develop viable systems [CRYP96].

One other major change in the October 1996 proposal, would be the allowance of exportation of stronger 56 bit key length Data Encryption Standard (DES) type products, up from the present 40 bit restriction.

To summarize the policy:

- Allows export of 56-Bit encryption products for the next two years, "contingent upon industry commitments to build and market future products that support key recovery." Six-month licenses for 56-bit exports would be granted and renewed for up to two years -- contingent on satisfactory progress towards key recovery.
- Requires key recovery capabilities after two years in all exportable products with more than 40 bits.
- "Encourages" the adoption of key recovery systems through international agreements, standards processes, and a new key management infrastructure.
- Transfers jurisdiction over encryption export licensing to the Department of Commerce, but grants the Department of Justice a formal vote in the process.
- Export of longer key lengths would continue for certain sensitive financial applications.
- Export of longer key lengths may be allowed more generally once key recovery mechanisms are in place [CDT96].

Although the Administration’s ability to effectively garner support from 11 major companies may be helpful in moving their cryptography policy forward this is by no means assured.

Marc Rottenberg, Executive Director of the Electronic Privacy Information Center (EPIC), an international privacy and civil rights organization, dubs the latest proposal “Clipper 4,” (others call it “Clipper 3.1.1”)after an original government encryption scheme known as Clipper that enabled easy government access to all encrypted data. He also labels the “key recovery” scheme as “the same barn, (with a) new coat of paint,” which is a comparison with previous “key escrow” proposals.

Beyond this, he is unsure as to the initiative's viability based upon:

- The key recovery consortium is a comparatively small group, primarily of U.S. hardware (not software) firms. A number of companies the Administration approached, particularly software companies, refused to be a part of the effort.
- The most important group is the user community, and public polling data indicates this segment is opposed to the initiative.
- Congress, which has pending cryptography legislation that does not embrace any sort of key escrow or recovery scheme, will want to weigh in on the matter [ROTT96].

Another issue that has been raised is whether the allowance of a 56 bit key length goes far enough. A panel of cryptography experts, including Whitfield Diffie the inventor of public key cryptography, released a February 1996 report indicating that 75 bit key lengths are necessary for "adequate protection against serious threats," and 90 bit key lengths to ensure secured data for the next two decades [CRYP96].

Bill Gates, Chairman, Microsoft Corporation, in response to the October 1996 Clinton Administration key recovery proposal in respect to the provision allowing the exportation of products encrypted with 56-bit key lengths, characterized the improvement as "tiny," a 56-bit key "is not nearly good enough." Gates further stated the "U.S. government is making it fairly difficult for companies like Microsoft who want to use strong cryptographic techniques" [GATES96].

Twenty-one U.S. Senators and Congressmen responded to the key recovery initiative by sending Commerce Secretary, Mickey Kantor, a letter indicating their agreement with an October 4, 1996 New York Times editorial that characterized the Administration's plan as "needlessly restrictive and probably unworkable" and (though better than previous Administration proposals) "risks doing more harm than good."

They offered four reasons that they believe the proposal is "flawed":

1) It fails to recognize that top-down, government-imposed policies are doomed to defeat.
2) export policies must be directly linked, or indexed, to advances in technology
3) export controls must be fully multilateral in order to be effective
4) export control decisions will be further delayed by granting the FBI new veto authority over U.S. exports.

Fear was also expressed that the "four defects" will continue to leave U.S. companies at a disadvantage in the world market, leave users of U.S. encryption uncertain about the security of their information and leave U.S. law enforcement and national security agencies behind the cryptography-curve.

Concern was expressed that Congress was not consulted in the policy formulation process, and a request was made that in the coming months the Administration work with

Congress, industry, consumer and user groups to refine cryptography policy further [KANT96].

Congressional Legislation

For the most part Congress has taken an opposite stance to the Administration's cryptography policies. Generally they oppose a key escrow/recovery scheme, as well as present key bit strength limitations, on the grounds that it inhibits U.S. commercial interests, and infringes upon user privacy. Two pieces of legislation currently exist:

I. U. S. Senate. S. 1726, "The Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996."

The stated purpose of the Act "is to promote electronic commerce through the use of strong encryption." Primary provisions include:

1) Restricting the Department of Commerce with respect to the promulgation or enforcement of regulations, or the application of policies, that impose government designed encryption standards.
2) Promoting the ability of U.S. businesses to sell computer hardware and software internationally that incorporate strong encryption by:
A) Restricting Federal or State regulation of the sale of such products and programs in interstate commerce.
B) Prohibiting mandatory key escrow encryption systems.
C) Establishing conditions for the sale of encryption products and programs in foreign Commerce [PROC96].

Pro-CODE co-sponsors Senator Patrick Leahy (D-VT), and Senator Conrad Burns (R-MT) have not responded favorably to the Clinton Administration's October 1996 "key recovery" cryptography initiative. Both are of the opinion that the Administration needs to work with Congress on an issue of such importance. Senator Leahy has indicated that he is dubious of the proposal because it is a breakable scheme and may infringe upon the privacy rights of individuals by ignoring fourth amendment provisions of the U.S. Constitution [LEAHY96].

Senator Burns reiterated this sentiment by criticizing the Clinton Administration "for its failure to negotiate on the cornerstone of its proposals: that companies must agree to "escrow" their decryption keys." He has indicated that he will push for vigorous oversight of the administration's plan in the Commerce Committee" [BURNS96].

II. U.S. House of Representatives. H.R. 3011, the "Security and Freedom Through Encryption (SAFE) Act"

Among other measures, the SAFE legislation suggests that key escrow does not adequately address security concerns and hampers U.S. business interests.

At a September 25th 1996 SAFE hearing before the U.S. House of Representatives Judiciary Committee, Representative Robert Goodlatte (R-VA) testified "the chief roadblock to electronic commerce on the Internet is government regulation of encryption." "The arguments that the FBI, CIA, and NSA have given me to justify the need for a massive "key escrow" or as it's now called "key recovery" plan just don't ring true in 1996" [KEY96].

Based on these statements it would seem that the gulf between the Executive Branch and Congress is quite substantial in regard to cryptography policy.

U.S. Cryptography Policy and International Efforts

The OECD

In that the Administration has met stiff resistance by both the U.S. user community and many members of Congress, they have been seeking to work through the Organization for Economic Cooperation and Development (OECD) (see Appendix V: International Organizations) in the hope of garnering international support for a key recovery type system, as well as key bit strength limitation. By doing this, Administration interests may believe that they can effectively back their objectives into a heretofore unreceptive U.S. domestic market.

In October 1996, the OECD hosted a Paris based ad-hoc meeting on cryptography. From the U.S. point of view, the meeting was an opportunity to raise the consciousness of other governments about the problem of uncontrolled encryption while at the same time demonstrating to U.S. industry that defeating U.S. export controls would not open the door to a vast market for unescrowed encryption, but instead spark new and perhaps inconsistent local regulation of encryption.
The meeting was reportedly effective in "educating" many attending country representatives. However, substantial doubt reportedly was evident among Scandinavian country and Japanese representatives, with the Japanese perhaps more concerned about catching up and surpassing the U.S. and other countries, now that cryptographic product commercial prospects are growing [BAKE96].

The OECD is in the process of drafting Cryptography Policy Guidelines, expected to be completed in early 1997. The Guidelines will be non-binding recommendations to member governments, and thus will not have true legal status—but could carry weight with sovereign nation governments.

Says an anonymous U.S. Congressional staffer "(I) think (you are seeing), the Administration coming out and using them (The OECD) as a shell game. (They) go to the OECD and say the U.S. is moving toward key escrow, and then come back and say the OECD is going toward key escrow, neither of which are true."

Crypto Ambassador

Reports have surfaced that the Clinton Administration will appoint a representative with Ambassadorial status to generate international support for their cryptography agenda. Specifically, the Ambassador would be responsible for encouraging other governments to move toward an international key recovery scheme as outlined in their October 1996 proposal. Rather than operate in a public manner, the Ambassador would work in private, both to educate and move forward agreements [IMPER96].

National Research Council Report

In May, 1996 a comprehensive report on Cryptography was released by The National Research Council, a principal operating agency of both the National Academy of Sciences and the National Academy of Engineering which provide services to the government, public, scientific, and engineering communities. The findings and recommendations from the blue-chip committee included:

- No law should bar the manufacture, sale, or use of any form of encryption within the United States. Specifically, a legislative ban on the use of unescrowed encryption would raise both technical and legal or constitutional issues.
- National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of law
- National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces. As cryptography has assumed greater importance to non-government interests, national cryptography policy has become increasingly disconnected from market reality and the needs of parties in the private sector.
- Export controls on cryptography should be progressively relaxed but not eliminated.
- Some relaxation of today's export controls on cryptography is warranted. Relaxation would create an environment in which U.S. and multinational firms and individuals could use the same security products in the United States and abroad, thereby supporting better information security for U.S. firms operating internationally
- The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age.
- To better understand how escrowed encryption might operate, the U.S. government should explore escrowed encryption for its own uses. To address the critical international dimensions of escrowed communications, the U.S. government should work with other nations on this topic [NRC96].

Cryptography is Not Foolproof

It must be kept in mind that no cryptographic scheme is foolproof. In September 1996, researchers at Bellcore Laboratories announced an ingenious new type of cryptoanalytic attack. By exposing a sealed tamperproof device such as a smart card to certain physical effects (e.g., ionizing or microwave radiation), in many instances they were able to induce

a fault at a random bit location in one of the registers at some random intermediate stage in the cryptographic computation. In other words they were able to compromise the cryptographic scheme, and compromise the smart card. The Bellcore analysis indicated that this approach was primarily applicable to public key cryptosystems, such as RSA, but not secret key systems like the Data Encryption Standard (DES).

However, researchers in Israel carried out a related attack (which they call Differential Fault Analysis, or DFA), and reported that compromise is applicable to almost any secret key cryptosystem. In particular, they claim to have actually implemented DFA in the case of DES, and demonstrated that under the same hardware fault model used by the Bellcore researchers, the extraction of a full DES key from a sealed tamperproof DES encryptor is possible, by analyzing fewer than 200 ciphertexts generated from unknown cleartexts.

The power of DFA is demonstrated by the fact that even if DES is replaced by triple DES (which incorporates a 168 bit key and assumed to be nearly unbreakable), essentially the same attack can break it with essentially the same number of given ciphertexts [DFA96].

Although additional testing of these theories may be required, they point out that cryptographic systems that have been deemed unbreakable, may be attacked and compromised.

Conclusion

U.S. Cryptography policy, to be generous, has been handled abysmally. Various administration initiatives have hampered, and continue to hamper, the proliferation of international electronic markets. One has the impression that the eleven companies that are supportive of the Administration's key recovery proposal are "on-board" because of a combination of wanting to move forward with at least some initiative, and perhaps a perceived financial incentive, either by supplying key recovery system technology, or being placed on a short list for government contracts/favors.

There is a dichotomy within the Administration. In referring to findings that rising international demand for computers and other electronic products caused Silicon Valley to post the nation's best export record last year (1995), at least in terms of dollar gains (i.e. San Jose, Calif., the top metropolitan area with an increase of $6.9 billion in foreign sales, up 34.5% over 1994), Commerce Secretary Mickey Kantor said "one cannot overstate the importance of exports in creating jobs and economic growth and opportunity in our cities," further saying "the findings demonstrate the effectiveness of the Clinton administration's export promotion strategy." At the same time, many Silicon Valley executives firms claim that Administration cryptography policies could do great harm to this robust sector [SILI96].

In the meantime, countries like Japan are busily developing and exporting strong encryption systems in anticipation of eroding an industry in which heretofore the U.S. has enjoyed a dominant position.

Information warfare specialist Robert D. Steele makes the point that it is impossible to build "back doors" into "open" systems that have the benefit of being scrutinized by millions of smart people." Steele suggests that rather than intelligence and law enforcement seeking to make their job easier, they would best be served by "learning new methods for a new age" [STEELE96].

Only time will tell whether the Administration's cryptography policies will enjoy widespread global adoption by governments and large companies. In the meantime, a lot of wasted energy is being expended on this issue. This time would be better spent in spotting and rectifying problems such as those pointed out by the Bellcore and Israeli researchers, and putting strong encryption in place in U.S. businesses to avoid information warfare attacks.

It is my opinion that until the posture of the Administration, particularly the intelligence and law enforcement arms are changed, the process will continue to drag on, causing economic harm to the U.S. technology industry, and slowing down the proliferation of international electronic markets.

IV. Governance

Governance issues as relate to the Internet, computer software, and other hardware/software mediums for the conduct of electronic commerce are emerging at a rapid rate. Most of this section will deal with the Internet, the most promising conduit to conduct global electronic commerce. However, the discussion is applicable to all electronic commerce conduits and "tools."

The Internet was a "creature" of the U.S. Government, in that they funded much of the backbone infrastructure, provided research grants for routing and hub technologies, and directly or indirectly supplied operating funds for domain registries and ad-hoc standards bodies.

Although the Internet is global in scope, for the most part, until late 1995 the user base was small and fairly homogenous, comprised of a male dominated population of scientists, academics, researchers, college students, engineers, military, and government interests. The bulk of Internet computer servers, software/hardware applications, and indeed the backbone were based in the U.S., and the English language was dominant.

Even today, although worldwide Internet activity is growing rapidly, and by some estimates will number 100 million users by 1999, use in the United States still far and away surpasses that of other countries. Approximately 64 percent of the world's Internet servers are in the U. S., followed by Germany at 5 percent, and the United Kingdom at 3 percent [KALIN96]. This has added up to a somewhat U.S. centric Internet, loosely governed by consensual ad-hoc working groups.

As we enter 1997 this is changing due to the following factors:

1. **Reduction of Government Support** The U.S. Federal Government while still desirous of playing a key role in policy decisions that impact the Internet is extricating itself from day to day operations. In 1995 the National Science Foundation (NSF), decommissioned the Internet backbone. The NSF has also mostly privatized the domain registration process by reducing federal funding, and allowing privately held Network Solutions Inc.(NSI)®, to charge for and oversee this crucial function.

2. **Exponential Growth**. No longer is the Internet an unknown "jewel" for a comparatively small population of highly educated men in that the masses have discovered the "Net" and growth has been explosive. Contributing factors have been the advent of a handful of national/regional Internet access providers, as well as mom and pop providers. Another huge factor that spurred growth was development of a credible graphical user interface (GUI) browser called Mosaic® at The University of Illinois. Mosaic, and a later spinoff commercial browser called Netscape®, enabled practical utilization of the World Wide Web (WWW). Overnight, every individual or business could become an information publisher, rather than a passive information recipient.

A final contributing factor has been cost and speed. Sending and receiving electronic mail messages was nearly free, and much speedier than regular mail.

Once the Net was discovered by the mainstream an increasingly diverse population mirroring society as a whole "logged on." In fact, in an October 1996 survey of 1000 consumers, 82 percent had heard of the World Wide Web, whereas one year earlier only 44.7 percent had this awareness. The term Internet was recognizable by 93.5 percent compared with 82 percent the prior year, and 27 percent of respondents had been on-line in the past six months [AWAR96].

This explosive growth caused the commercial sector, media, government, and law enforcement to take notice. The commercial sector saw fertile ground for product marketing, selling goods and services, customer service, and the ability to lower costs and operate more efficiently. Government, law enforcement and national security interests became alarmed that the Internet could pose a societal threat through the spread of pornographic material, the enticement of children, bomb making instructions, terrorism, tax evasion, money laundering, on-line gambling, and other factors. Then too, traditional government interests became alarmed at the potential loss of power the new medium might represent.

3). International Network Deregulation

International interests have adhered to a somewhat U.S. centric Internet, because they knew little about the technology (i.e. the newness factor), and in many instances their networks were dependent upon the U.S. backbone for backhauling data.. Much of the

slowness in global Internet proliferation has had to do with inequities in circuit pricing, the power of telephone monopolies, price discrepancies, and inefficiencies in topologies by non-U.S. countries. These inefficiencies have been behind many transit and peering policies. A significant amount of Internet traffic still terminates in the U.S., and the U.S. backbone is used for transit. For example, even today, in many instances the cheapest interconnect point for Europe is U.S. based MAE East. Thus, in the case of many countries, competition has not really entered into this area and may be a significant factor in uneven global progression of the Internet [CIX96] [KALIN96].

This is expected to change, albeit on a continued uneven basis. Countries that have the most liberal telecommunications regulations such as the United States, Finland, Sweden, the United Kingdom, Hong Kong, Australia, New Zealand, and the Philippines already have the lowest Internet access costs and will see costs continue to drop. France, Germany, and Brazil along with other countries committed to opening their markets, will also see costs drop during the next five years. However, countries not expected to allow competition within the next five years, and with the most entrenched monopolies or duopolies, such as China, Japan, Taiwan, and Vietnam, will likely continue to have high access costs [KALIN96].

In the case of Europe, telecommunications industry deregulation, approved by the European Commission (EC), will take effect on Jan. 1, 1998 and apply to all European Commission countries. Internet and intranet companies have expressed mild-optimism that widespread telecommunications deregulation will produce a surge in the number of companies that offer leased lines for Internet, intranet, and other data services, thereby lowering prices and instigating an infusion of crucial wide-area network infrastructure [EURO].
The following table shows the great price disparities between the U.S. and European countries, as well as within Europe:

Monthly Cost for 64Kb Line

$300 to $400 in the United States;
$1,000 in Germany;
$1,000 in France;
$2,000 to $3,000 in Spain;
$2,000 to $3,000 in Italy.
[KALIN96]

Ultimately as networks and content servers become globally distributed, and caching models are put in place, this will affect Internet traffic patterns, and electronic commerce in a significant manner, not just technologically, but policy and governance-wise as well. Internet growth in Europe will be spurred not only by telecommunications deregulation but also by the growing corporate movement from private backbones toward public networks as a way to cut costs. As corporations evolve from nation-specific to regional,

they will look to the Internet as a way to communicate with far-flung staffs, customers, and trading partners.

4. Lawyers Discover Cyberspace

Perhaps most importantly, lawyers have discovered the Internet, and the electronic market place. It is possible that no other group may influence and speed to the forefront attempts at Internet/electronic commerce governance than the legal profession and judicial system. As Vinton Cerf, a key architect of the Internet said in a recent speech before the National Graphic Society in Washington, D.C., "you know there must be money to be made (in Internet related businesses), just look at all of the lawyers that are involved" [CERF96]. Although Cerf's comment was meant to evoke amusement, it was quite true. Lawyers are diving into the Internet cyberspace governance debate in droves. It is my opinion this is due largely to the intellectual challenge of a new legal frontier, the desire to bring order to the present ad-hoc Internet governance model, and as Cerf implied, the smell of money to be made in this murky legal environment.

Already lawyers (and the judicial system) are the driving force in challenging the legality of the Internet domain registration system, copyright/intellectual property law, and most all other policy areas.

As with most every sector of society, it is my belief that the emerging information technologies will impact both the concept of law and how it is practiced. Specifically, the Internet/cyberspace impacts the concept of distance and time. No longer, will old legal doctrines/processes that depended upon finite physical spaces and processes so ably work. Again, as with other sectors of society, until lawyers, judges and even lawmakers explore the cyber realm, they will be ignorant to this requirement of change/adjustment. This could impede certain developmental aspects of cyberspace/electronic commerce, however, it is more likely that the legal structure will be seen as irrelevant and circumvented until corrected [RAPP96].

Governance in the Electronic Age

The electronic marketplace, dominated by the Internet has been an anarchistic "wild west" environment. While no government authority rules the Internet, a very unique consensual governance model has arisen in large part due to the technology inherent to the Internet. Various voluntary Internet bodies such as the Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), Internet Assigned Numbers Authority (IANA), World Wide Web Consortium (W3C), and Internet Society (ISOC) form on an ad-hoc basis primarily to address Internet engineering, standards and development issues.

The Internet Consensual Governance Process

Before proceeding further, let us briefly explore how the Internet consensual governance process works.

Take for example the IETF, which is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, network management, security, etc.). Much of the work is handled via Internet mailing lists, however, the IETF also holds meetings three times per year.

The internal management of the IETF is handled by area directors, who together with the Chair of the IETF form the Internet Engineering Steering Group (IESG). The operational management of the Internet standards process is handled by the IESG under the auspices of the ISOC.

The Internet Architecture Board (IAB), a body of the ISOC, is responsible for overall architectural considerations in the Internet, and also serves to adjudicate disputes in the standards process.

There are two types of Internet documents: Internet-Drafts and Request for Comments (RFCs). Internet-Drafts have absolutely no formal status and can be changed or deleted at any time . RFCs are the official document series of the IAB, and are archived permanently (i.e., they are never deleted, and once an RFC is published, it will never change); however, it is important to note that not all RFCs are standards.

The Corporation for National Research Initiatives (CNRI), a not for profit organization, runs the IETF Secretariat with funding from the US government [IETF].

The IETF continues to play an important role in areas such as standards setting, as evidenced by recent adoption of the H.323 standard for audio and video conferencing, as well as potential acceptance/integration of the Resource Reservation Protocol (RRP) that would enable the exchange of data over the Internet and globally linked corporate intranets. Global interoperability would make it possible for remote Internet users to conduct electronic commerce and telephone calls via the network [INTEL96] [ROON96].

Considering that much of the work of these groups has been voluntary, with some U.S. Federal government financial support, it is amazing, and a tribute to group participants as to how well the Internet has progressed.

At present, this is still the manner in which most Internet standards, engineering, and governance decisions take place, however fissures in this model have begun to appear.

Domain Names: The Tip of The Iceberg?

Among the first issues to impact the Internet and raise questions about the Net's consensual form of governance has revolved around domain names, and is a good illustrative example of what may be a precursor to further questions raised about the feasibility of the ad-hoc governance model.

Internet domain names are simply numerical addresses that enable a computer to enjoy a unique point of entry/contact on the global Internet. However, although never intended, domain names have turned into very identifiable commodities through the association of what might be called "vanity names" like shareware.com, tv.com, even diarrhea.com [ADDR96]. In effect the domain name numbering scheme has turned into an Internet directory service—a function that was never intended.

In reality only the InterNIC is a dual registry. There is confusion when the term registry is used, as in fact there are many registries throughout the world. InterNIC happens to be the entity that combines domain name and IP (Internet protocol) registry functions-which is almost unique in the entire world. The other main registries do IP registry allocations, or domain name registrations--separately [CIX96]

At present, under authority of the National Science Foundation (NSF), a private company, Network Solutions, Inc, (NSI), is responsible for the allocation/administration of what are known as international top level domains (iTLDs). NSI handles the .com, .net, .org, and .edu. (iTLDs). Far and away the .com (iTLD), which is set aside for business and commercial purposes, is the most utilized and primary point of contention.

Fundamental problems with the present handling of domain names exist. They are:

1) The present domain name registration system does not take into account their trademark nature. Any name can be registered by anybody.
2) The current naming system is not broad enough to accommodate business needs. Once a name is taken, it is effectively out of circulation. This adds tremendous value to choice names, an unintended consequence of the system.
3) There is no real international coordination of domain names.
4) There is no real legal basis or rationale as to NSI's operation of domain name allocation [HALP96].
5) The present top level domain scheme will never be able to scale to the massive numbers expected in the future [MITCH96].

IANA/ISOC Proposal

The IANA and ISOC have developed a proposal that would add up to 150 new (iTLD) registries to allow more descriptive names while reducing the load borne by the heavily utilized .com (iTLD). Registries would be globally dispersed, to mitigate the charge of a U.S. centric Internet, and a percentage of registry proceeds would go to IANA/ISOC for oversight/administrative purposes [SYKES96].

This plan has met with some criticism, in that IANA/ISOC are consensual, not legal bodies, thus by what right do they have to promulgate a domain registry scheme? There has also been criticism about the amount of power this scheme would confer on IANA/ISOC in respect to the selection of new registries, and administrative/oversight function they would enjoy.

ISOC President Donald Heath agrees that careful deliberation needs to take place before the proposal is put into effect. To this end he has established an international ad hoc committee (IAHC), which will undertake to define, investigate, and resolve issues resulting from current international debate over a proposal to establish global registries and additional (iTLDs)," The IAHC will be composed of nine members from the International Telecommunications Union (ITU), the World Intellectual Property Organization (WIPO), the International Trademark Association (INTA), ISOC, IANA, and the IAB.
Input from Internet oriented legal bodies, as well as the Internet community at large will also be sought. Heath believes that through a formal process such as IAHC, whereby both traditional Internet consensual organizations coupled with international government bodies are brought together, the outcome will be legally acceptable, and acceptable by the Internet community [HEA96] [DOMA96].

Even with a deliberative effort, it is believed that legal challenges to the IANA/ISOC proposal and IAHC will occur based upon questions of authority to implement such a proposal, as well as selection criteria for (iTLD) registry companies. The issue of the property right nature of a domain name and the registry of these names, is a significantly different issue, and they are also separate. The property right aspect of domain names has not been decided. Further, the domain name system itself is flat, and can never be scaled (embody additional growth) to solve trademark and tradename problems. For example, there are approximately 600,000 .com (iTLDs) registered, which is insignificant, when you consider that each individual in the real world is potentially a domain. For now, the .com (iTLD) can still scale, but the number of attractive alpha-numeric combinations is a finite resource.

A number of authorities on the subject believe that a new domain naming scheme needs to be adopted, rather than extending the present method through the proliferation of new registries and (iTLDs) [MITCH96] [DOOL96]. In fact, some believe that there is a need to move beyond the idea of a domain system as directory. They feel the real issue is that the Internet needs an intuitive, intelligent directory system that is largely invisible to the end user, but close enough to being intuitive, that it will be convenient for all users [MITCH96].

In all probability even if the IANA/ISOC or some other proposal is implemented, within a relatively short period a new mechanism will likely need to be established that can technically scale, is international not U.S. centric (i.e., U.S. based IANA/ISOC would still

administer the new registry scheme), and perhaps most importantly addresses trademark and other legal issues.

Internationalization of Policy

It is no accident that the IANA/ISOC iTLD domain registry proposal, which normally would have been reviewed/adopted solely by their traditional ad-hoc working groups, must now obtain additional input, in this instance from international organization representatives.

The striking factor as we head into 1997 is how issues that first came to the forefront in the U.S., are now finding the light of day around the globe. This is to be expected, as the network has only begun to reach availability, pricing, and quality of service levels that the U.S. has enjoyed. Thus, it is only now that other countries must deal with these issues.

The other striking factor is that just as happened in the U.S., content issues, particularly as they relate to prurient material, or hate speech have seen the most attention by international authorities. (See Appendix VI: International Cyber Governance) One key difference, as compared to the U.S., has been much more attention paid to limiting the flow of information in certain countries with strict religious beliefs or historically tight controls on information.

For example, in China tight controls are maintained (attempted) over Internet access and content. All computer networks with links to databases outside of China must utilize computer gateways provided by the Ministry of Posts and Telecommunications, The Ministry of Electronics, or the State Education Commission university network. The computer gateways (i.e. routers) attempt data filtering by checking information source and destination contained in the address [CHI96].

Groups or individuals are banned by the government from "producing, retrieving, duplicating and spreading information that may hinder public order, as well as obscene and pornographic materials" [CHINA96].

In another case, The Malaysian Institute of Microelectronic Systems, a government agency, is the only provider of Internet access.

The Director General indicates that so long as information remains within the confines of a company, they are free to receive out of border information, manipulate it, and transmit it out of Malaysia—without interference. However, the government will act if illegal or offensive materials, like pornography are distributed within the country [MALA96].

In short, Governments around the world are struggling with a dichotomy. On the one hand they know the information age is upon us and that they must be a part of it or face the prospect of an "economic wilderness," while on the other they want to keep tight

control over information at odds culturally or politically with what has traditionally been allowed.

The executive branch of the U.S. government seems intent on working its will internationally. This is evidenced by attempts to encourage other countries to accept cryptography and intellectual property policies developed in the U.S. It is probable that the Clinton Administration wishes to do this because, at least in the case of cryptography, their policy initiatives have not been well received domestically. Thus, by obtaining an international "critical mass" perhaps they believe they will be able to effectively back their agenda into the U.S. domestic economy. Given lack of acceptance among the U.S. user base, as well as skepticism among, and heterogeneity of other countries, certainly the jury is out as to how effective the effort will be.

In any event, just as occurred in the United States, governments are now focusing on policy issues similar to what the U.S. has been exploring, many of which impact electronic commerce.

Conclusion

The Internet has flourished in the United States due in large part to a nearly hands-off governance approach. Key factors have been an allowance of the free flow of information, a comparatively deregulated telecommunications environment enabling inexpensive Internet access, a vibrant free-wheeling high technology sector, and a lack of taxation. In countries with heavily regulated telecommunications policies, leading to in many cases expensive Internet access, the story has been quite different.

In the United States it is a near certainty that some form of taxation will be imposed on distributed wide area networks like the Internet, as well as the sale of goods and services over electronic networks. It also seems likely that some sort of access fee scheme will be imposed to support universal service objectives. The Clinton Administration will also continue to press for questionable cryptography and intellectual property policies. Hopefully, government interests will be farsighted enough to not impose such onerous taxes nor continue to waste valuable time on unworkable policies that they kill the goose that laid the golden egg (i.e. U.S. dynamism in international networking).

Beyond telecommunications deregulation and government imposed fees, a big concern is governmental attempts to control, monitor, and in many instances limit the free flow of information. Should major emerging economic powers like China continue to attempt significant controls over data networks, I predict that it will retard their growth in the international electronic marketplace.

As expected consolidation in the U.S. Internet service provider (ISP) market takes place, as well as predictions that a handful of companies will be global telecommunication providers, the question arises as to whether a smaller number of outlets (providers) will enable this sort of governmental control?

The jury is still out on the ability of governments to control various communication conduits like the Internet due to what might be described as a unique sieve like quality (i.e., one hole is plugged up and another emerges). Ultimately not only will countries with strict controls suffer, but international electronic markets will be the poorer.

So what is the answer? First of all it is critical that education occur among international governmental, law enforcement, academic, and commercial interests. Actual hands on experience is very important. Once this is accomplished, these interests will better know how to deal with the issues, and produce workable policies and laws.

Ad-hoc bodies such as the ISOC, the IANA, the IETF, and the IAB will likely continue to play a constructive role in setting standards, however this may be predicated upon their ability to obtain some sort of legal status, as well as the incorporation of a viable financing mechanism (i.e., it is difficult for me to conceive of the continued allotment of free time to the governance process in a maturing environment). Then too, although there has been international participation, the primary leaders, and ad-hoc body points of authority have mostly been of U.S. origin. With the Internet becoming less U.S. centric, one has to wonder whether the international community will accept this. Perhaps international regional bodies with similar modus operandi will formulate policies, rather than singular ad-hoc groups. Certainly these groups will no longer be able to work in a relatively unencumbered decisional vacuum, as lawyers and other special interests will see to this.

Bodies that enjoy multi-country support like the World Trade Organization (WTO), OECD, International Telecommunications Union (ITU), European Union(EU), or Asia Pacific Economic Cooperative(APEC), may play a significant factor in the proliferation of international electronic markets. One aside, given the glacial pace that government supported bodies move when compared to such rapid technological changes in the networked marketplace, it seems doubtful that they will dominate, unless they are able to adapt.

What is clear is that the uniqueness of global electronic markets will require a degree of international coordination. In many instances, no longer will nationalistic laws and policies geared toward physical boundaries work well in an international marketplace that transcends boundaries. Ultimately governments will try and control the Internet (or other electronic conduits), and may or may not succeed. It is more likely that a diverse hodge-podge of interests will muddle through governance issues, with no clear cut dominating governance authority. While this will cause “fits and starts” in the emergence of the global electronic marketplace, ultimately it will prevail, and usher in a whole new era of global commerce and prosperity.

APPENDICES

Appendix I: Nexus

The application of a taxing State's sales or use tax is defined by the laws of that State. (For purposes of this guideline application of a taxing State's sales or use tax

includes a duty to collect a sales tax or a use tax from the customer of the out-of-state business.) Application of a State's sales and use tax is nonetheless subject to the existence of requisite nexus under the Due Process Clause and the Commerce Clause of the U.S. Constitution. This Guideline informs business of the signatory States' practice with respect to determining whether an out-of-state business has sufficient contacts with a taxing State under the Due Process Clause and Commerce Clause of the U.S. Constitution to support application of a taxing State's sales or use tax, including a duty to collect a sales tax or a use tax from the out-of-state business customer. The guideline reflects the signatory States' best understanding of applicable law and represents an effort to minimize post-transactional assessments reflecting constitutional understandings for which no advance notice has been given. In determining the possible application of a taxing State's sales or use tax under the Constitution of the United States, the statement makes no distinction between the vendor and vendee form of a sales and use tax. The signatory States understand that if a set of circumstances will support the constitutional application of one form of tax the same set of circumstances will support application of the other form of tax [AICPA94].

Appendix II: International Copyright

The Berne convention is the principal international copyright convention. It links together some 118 nations of the world into what is called the Berne Union. The Union was established to ensure that its members will accord to each other national treatment in respect to copyright, according to the standards set out in the Berne Convention.

The World Intellectual Property Organization (WIPO) is a specialized UN agency responsible for the administration of international intellectual property treaties, not only on copyrights, but also patents, trademarks, semi-conductor chips, and all intellectual property and treaties in this area. There are exceptions, more in the nature of "supplementary" treaties than those of the WIPO, which fall under the auspices of the World Trade Organization (WTO). During the recent GATT Uruguay Round there was an agreement called Trade Related Aspects of Intellectual Property (TRIPs), which built upon the standards in the WIPO convention and extended them, however the WIPO is the organization with primary responsibility.

The WIPO has no enforcement role, they update treaties when appropriate, convene meetings of experts to discuss issues relevant under the treaties. In the patent and trademark area there are some international filing and registration treaties whereby one can gain procedural advantages in terms of acquiring patent or trademark protection by making international filings from the WIPO that may obviate filing in each and every individual country. There is no administrative mechanism like this under the copyright system, as most countries have no copyright registration procedures, because copyright protection is automatic. The U.S. is the only major country with a copyright registration mechanism.

The Berne convention is not just an international procedural regulating treaty, it is a treaty that sets a lot of substantive standards that countries that belong to it have to provide for their copyright laws. It requires the basic copyright term of life plus 50 years, and requires that countries provide certain specified rights.

The governing bodies of the WIPO, which are the assemblies of the various conventions, meet biannually (every two years) in Geneva, Switzerland, to go over administrative matters. Special committees may meet at the direction of these governing bodies.

There was a recent attempt to revise the Paris Convention, which is the principal convention for the protection of patents. The attempt was not successful due to numerous developing country disputes.

There has been great reluctance to open the Berne Convention for revision because of bad experiences that took place in respect to the patent convention (i.e. Paris Convention). However, everyone generally realizes that there have been sufficient advances in technology and communications technology that the Berne convention, last revised in 1971, needs to be updated. Thus, there has been an attempt to effect change without reopening the whole convention. The U.S. and other countries are now involved in the process of having a subsidiary agreement established that would update the Berne Convention, without opening the basic convention. It will be a new treaty which specifies its relation to the Berne Convention. There is a provision in the Berne convention that allows for such special agreements among its member states, so long as they increase the level of protection, and do not decrease the level of protection guaranteed under the convention--a safeguard clause so to speak [KEPL96].

Appendix III: IW Weapons

Examples of available (or possible) IW weapons:
Computer Viruses
Worms
Trojan Horses
Logic Bombs
Trap Doors
Chipping
Nano machines and Microbes
Electronic Jamming
HERF Guns - EMP Bombs

Computer Viruses

"A virus is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it

reproduces."

Viruses are well known in every computer based environment, so it is not astonishing that this type of rough program is used in the Information Warfare. We could imagine that the CIA (or Army, Air Force ....) inserts computer viruses into the switching networks of the enemy's phone system. In that today's telephone systems are switched by computers, you can shut them down, or at least cause massive failure, with a virus as easily as you can shut down a "normal" computer. An example of what the damage a virus could cause exists. We can compare it with the system crash of AT&T's long distance switching system on January 15, 1990.

Worms

"A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs."

Also if worms don't destroy data, they can cause the loss of communication only by eating up resources and spreading through the networks. A worm can also easily be modified so that data deletion or worse occurs. With "wildlife" like this, one could imagine breaking down a networked environment, like an ATM and banking network.

Trojan Horses

"A Trojan horse is a code fragment that hides inside a program and performs a disguised function. It's a popular mechanism for disguising a virus or a worm"

A trojan horse could be camouflaged as a security related tool for example like SATAN (Security Administrating Tool for Analyzing Networks). SATAN checks UNIX type systems for security holes and is freely available on the Internet. If someone edits this program so that it sends discovered security holes in an e-mail message back (let's also include the password file? No problem), the Cracker learns much information about vulnerable hosts and servers. A clever written trojan horse does not leave traces of its presence, and because it does not cause detectable damage, it is hard to detect.

Logic Bombs

"A bomb is a type of Trojan horse, used to release a virus, a worm or some other system attack. It's either an independent program or a piece of code

that's been planted by a system developer or programmer."

With the overwhelming existence of US based software (e.g. MS Windows or UNIX systems), the US Government, or whomever you would like to imagine, could decide that no software would be allowed to be exported from that country without a Trojan horse. This hidden function could become active when a document with "war against the USA" exists on the computer. Its activation could also be triggered from the outside. One effect could be to format the computers hard disks or to mail the document to the CIA.

Trap Doors

"A trap door, or a back door, is a mechanism that's built into a system by its designer. The function of a trap door is to give the designer a way to sneak back into the system, circumventing normal system protection."

As I mentioned in the last section, all US software could be equipped with a trap door that would allow IW agencies to explore systems and the stored data on foreign countries. This could be most useful in cases of military strategic simulations and plans and would provide the DoD's intelligence with vital information.

Chipping

Just as software can contain unexpected functions, it is also possible to implement similar functions in hardware. Today's chips contain millions of integrated circuits that can easily be configured by the manufacturer so that they also contain some unexpected functions. They could be built so that they fail after a certain time, blow up after they receive a signal on a specific frequency, or send radio signals that allow identification of their exact location - the number of possible scenarios exceeds, by far, the scope of this paper. The main problem with chipping is that the specific (adapted) chip be installed in the place that is useful for the Information Warrior. The easiest solution is to build the additional features into all the chips manufactured in a country that is interested in this type of IW.

Nano Machines and Microbes

Nano machines and Microbes provide the possibility to cause serious harm to a system. Unlike viruses, these IW weapons can be used to attack not the software but hardware of a computer system. Nano machines are tiny robots (smaller than ants) that could be spread at an information center of the enemy. They crawl through the halls and offices until they find a computer. They are so small that they enter the computer through slots and shut down electronic

circuits.

Another way to damage the hardware is a special breed of microbes. We know that they can eat oil, what about if they were bred for eating silizium? They would destroy all integrated circuits in a computer lab, a site, a building, a town...

Electronic Jamming

In the old days (and even today) electronic jamming was used to block communications channels at the enemy's equipment so that they couldn't receive any information. Today the next step is not to block their traffic, but instead overwhelm them with incorrect information. This type of disinformation can also be combined with other attacks, to ensure success.

HERF Guns - EMP Bombs

HERF stands for High Energy Radio Frequency. HERF guns are able to shoot a high power radio signal at an electronic target and put it out of function. The damage can be moderate (e.g. that a system shuts down, but can be restarted) or severe (e.g. the system hardware has been physically damaged). Electronic circuits are more vulnerable to overload than most people would suspect. This mechanism uses HERF guns with big success. In essence, HERF guns are nothing but radio transmitters. They send a concentrated radio signal to the target. The target can be a mainframe inside a business building, an entire network in a building, or as today's planes and cars are stuffed with electronic equipment, the target can even be a moving vehicle with all the inherent dangers for the people who are inside.

EMP stands for electromagnetic pulse. The source can be a nuclear or a non-nuclear detonation. It can be used by special forces teams who infiltrate the enemy's and detonate a device near their electronic devices. It destroys the electronics of all computer and communication systems in a very large area. The EMP bomb can be smaller than a HERF gun to cause a similar amount of damage and is typically used to damage not a single target (not aiming in one direction) but to damage all equipment near the bomb [HAENI96].

Appendix IV: Encryption Export Policies

Authorities

The export of cryptographic products is regulated by the Department of State pursuant to the Arms Export Control Act (AECA) and its implementing International Traffic In Arms

Regulations (ITAR), and by the Department of Commerce pursuant to the Export Administration Act (EAA) and its implementing Export Administration Regulations (EAR).
No license is required for the import of cryptographic hardware or software. There are no federal laws regulating the use of cryptographic products within the United States. A license is required for the export of cryptographic products to all destinations except Canada. Applications are reviewed by the Department of Defense (NSA) for national security implications and by State for foreign policy concerns. The export licensing policy is consistent with U.S. national security and foreign policy.
The Department of Commerce controls the export of rudimentary cryptographic products containing cryptographic functions generally limited to purposes such as data authentication, password protection, and access control.Products which are determined to be covered by the Commerce Control List(CCL), with certain foreign policy exceptions, may be exported under a General License.

Procedures

- Autolist - For products reviewed and approved by NSA for export to approved classes of end users and end uses. Permits Department of State to process license applications for such products without further review by NSA.
- Distribution Arrangements - Single license vehicle for export of approved products to classes of end users in countries or regions. Avoids need for licenses on an export-by-export basis.
- Distribution Agreements - Permits single license for export of approved products to identified distributors. Again, avoids export-by-export licensing.
- Personal Use Exemption - Products exported for the personal use of the exporter are excepted from pre-export license requirements.

Policies

- Products designed to use cryptography for access control/authentication purposes are export controlled as dual use commodities pursuant to the Export Administration Act.
- Product manufacturers determine if their products are access control/authentication devices.
- Generally, access control/authentication products are exportable under general license procedures.
- Mass-market software products verified as implementing RC2/RC4 encryption algorithms, with 40-bit key space limitations, are designated dual use items, to be controlled under the Export Administration Act, after a one-time review completed within 7 working days of submission.
- Mass-market software implementing other encryption algorithms and key space lengths for confidentiality are reviewed on a case-by-case basis for designation as dual use items and control under the Export Administration Act. By regulation, reviews must be completed within 15 days of submission.
- Generally, licenses are approved for export of products to be used in protecting U.S. proprietary information (i.e., intellectual property).

- U.S. companies and their subsidiaries are allowed to export products with strong encryption for their internal use.
- Confidentiality encryption products that incorporate the Data Encryption Standard (DES) are routinely approved for export to:

o Financial institutions and financial applications o Protecting financial information in Electronic commerce applications

Confidentiality encryption products that incorporate the Data Encryption Standard (DES) are favorably considered for export to: o Applications involving protection of personal medical data o Parking and toll systems; Debit applications; other transaction-based systems in which encryption is configured to perform identified specific transactions [CRYPT96].

Appendix V: Organizations

I. **Government Sanctioned**

Organization for Economic Cooperation and Development (OECD)

The Paris based OECD is a unique collaborative forum permitting governments of the industrialized democracies to study and formulate optimal approaches to the management of their economies possible in all economic and social spheres.

In its convention, the organization is charged with promoting policies designed to:

- Achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus contribute to the development of the world economy;
- Contribute to sound economic expansion in Member as well as non-Member countries in the process of economic development; and
- Contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The OECD differs from other intergovernmental organizations in that it has neither supranational legal powers, nor financial resources for loans or subsidies, its sole function is direct co-operation among the governments of its Member countries [OECD96].

The Financial Action Task Force (FATF)

The FATF, comprised of 28 members, is based at the OECD, and was established in 1989 to combat money laundering.

More than six years after the establishment of the FATF, Turkey is the only FATF member which has not yet passed anti-money laundering legislation and whose compliance with FATF recommendations is seriously deficient.

FATF continues to review the growth of electronic networks like the Internet as possible vehicles for money laundering.

The International Telecommunications Union (ITU)

The ITU is an intergovernmental organization comprised of 185 Member States and 363 members (scientific and industrial companies, public and private operators, broadcasters, regional/international organizations), within which the public and private sectors cooperate for the development of telecommunications. The ITU adopts international regulations and treaties governing all terrestrial and space uses of the frequency spectrum as well as the use of the geostationary-satellite orbit, within which countries adopt their national legislation. It also develops standards to facilitate the interconnection of telecommunication systems on a worldwide scale regardless of the type of technology used. Spearheading telecommunications development on a world scale, the ITU fosters the development of telecommunications in developing countries, by establishing medium-term development policies and strategies in consultation with other partners in the sector and by providing
specialized technical assistance in the areas of telecommunication policies, the choice and transfer of technologies, management, financing of investment projects and mobilization of resources, the installation and maintenance of networks, the management of human resources as well as research and development [ITU96].

World Trade Organization (WTO)

Established in January 1995, the Geneva, Switzerland based WTO is the legal and institutional foundation of the multilateral trading system. It provides the principal contractual obligations determining how governments frame and implement domestic trade legislation and regulations. And it is the platform on which trade relations among countries evolve through collective debate, negotiation and adjudication.

Main functions:

The essential functions of the WTO are:

- Administering and implementing the multilateral and plurilateral trade agreements which together make up the WTO.
- Acting as a forum for multilateral trade negotiations.
- Seeking to resolve trade disputes.
- Overseeing national trade policies.
- Cooperating with other international institutions involved in global economic policy-making [WTO96].

World Intellectual Property Organization (WIPO)

The WIPO, a specialized intergovernmental agency of the United Nations maintains headquarters in Geneva, Switzerland.

The WIPO is responsible for the promotion of the protection of intellectual property throughout the world through cooperation among States, and for the administration of various multilateral treaties dealing with the legal and administrative aspects of intellectual property.

Intellectual property comprises two main branches:

1) Industrial property, chiefly in inventions, trademarks, industrial designs, and appellations of origin.
2) Copyright, chiefly in literary, musical, artistic, photographic and audiovisual works.

A substantial part of the activities and the resources of the WIPO is devoted to development cooperation with developing countries [WIPO96].

European Union (EU)

The EU was formed in November 1993 after the ratification of the Maastricht Treaty, and is an organization comprised of 15 European member states. Cooperation takes place on many issues ranging from single market to foreign policy, and from mutual recognition of school diplomas to exchange of criminal records. This co-operation, in various forms, is officially referred to as three pillars.

The United Kingdom does not to take part in co-operation on social matters, which was designed to be part of the revised EEC Treaty (and thus of the first pillar) [EU96].

European Commission (EC)

The EC is the body with the formal and exclusive power to initiate all EU legislation, and which is supposed to represent the interest of the Union as a whole, both in the political processes within the EU and in negotiations with the outside world. This means that it must
take no instructions from any of the member states' governments, as it is accountable only to the European Parliament (as well as, any EU institution to the European Court). Also, it is the main body with a duty to look after correct implementation of the treaties and subsequent legislation.

The Commission's members are nominated by their national governments and must be acceptable to all the government leaders of the member states. Small member states each have one Commissioner, while the larger ones (Germany, France, Italy, UK, Spain) each have two. At this time, there are a total of 20 Commissioners.

The Council of Europe (CoE)

The CoE is quite a different organization from the EU. It is a purely intergovernmental organization much more like the United Nations. Unlike EU legislation, its treaties are not directly applicable in national law, unless ratified by the normal parliamentary procedures of the member state concerned. The (CoE) should not be confused with the European Council which is an EU institution.

The CoE is probably best known for the European Convention for the Protection of Human Rights and Personal Freedoms and its associated European Court for Human Rights in Strasbourg (not to be confused with the EU Court of Justice in Luxembourg). CoE members actually allow their nationals to challenge national legislation and jurisdiction before this court, which has thus become a sort of guarantee for human rights, even for countries which do not have a written constitution (such as Britain) or a supreme court.

Current CoE members include Austria, Belgium, Bulgaria, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Norway, the Netherlands, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Asia-Pacific Economic Cooperation (APEC)

The APEC was formed in 1989 in response to the growing interdependence among Asia-Pacific economies. Begun as an informal dialogue group with limited participation, the APEC has since become the primary regional vehicle for promoting open trade and practical economic cooperation. Member economies represent about 46 percent of the world's total merchandise trade. Its goal is to advance Asia-Pacific economic dynamismand sense of community.

APEC's Objectives are:

- To sustain the growth and development of the region for the common good of its peoples and, in this way, to contribute to the growth and development of the world economy.
- To enhance the positive gains, both for the region and the world economy, resulting from increasing economic interdependence, including by encouraging the flow of goods, services, capital and technology.
- To develop and strengthen the open multilateral trading system in the interest of Asia-Pacific and all other economies.

- To reduce barriers to trade in goods and services among participants in a manner consistent with GATT principles, where applicable, and without detriment to other economies [APEC96].

The Group of Seven (G-7) The Group of Seven, or G-7, is a consortium of the seven largest economiesin the world (i.e., United States, France, Germany, Italy, Japan, Canada, Great Britain). Having met annually since 1975, the leaders of the member nations meet once a year to discuss issues of mutual concern.
The foreign ministers and the finance ministers meet simultaneously in parallel plenary sessions. The agenda is set in advance. The continuing nature of the G-7 process allows for the annual setting of goals and review of accomplishments at each session. Atthe end of each meeting, there is typically a communique issued that marksthe progress that has been made and the G-7's goals for the next year.

U.S. Federal Networking Council (FNC)

The Arlington, Virginia based Federal Network Council (FNC) is a U.S. Government multi-agency coordination body with the purpose of establishing an effective forum and long-term strategy to oversee operation and evolution of the Internet and other national computer networks in support of research and education.

The FNC has an Advisory Committee, chartered by the National Science Foundation (NSF) to provide advice on policy and operational issues regarding the evolution of the Internet and the National Research and Education Network Program. Members represent a broad range of constituencies, including libraries, K-12 education, computer industry, telecommunications industry, information service providers, cable and wireless industry, vendors, higher education, and others.

Consensual—Not Government Sanctioned

The Internet Society (ISOC)

The Internet Society (ISOC), a Reston, Virginia USA based not for profit international organization for global cooperation and coordination of the Internet was established in January 1992 to maintain and extend the development and availability of the Internet and its associated technologies and applications.

Its members reflect the breadth of the entire Internet community and consist of individuals, corporations, non-profit organizations, and government agencies.

Its specific goals and purposes include:

- Development, maintenance, evolution, and dissemination of standards for the Internet and its internetworking technologies and applications.
- Growth and evolution of the Internet architecture.
- Maintenance and evolution of effective administrative processes necessary for operation of the global Internet and internets.
- Education and research related to the Internet and internetworking
- Harmonization of actions and activities at international levels to facilitate the development and availability of the Internet.
- Collection and dissemination of information related to the Internet and internetworking, including histories and archives.
- Assisting technologically developing countries, areas, and peoples in implementing and evolving their Internet infrastructure and use.
- Liaison with other organizations, governments, and the general public for coordination, collaboration, and education in effecting the above purposes.

The ISOC operates through its international Board of Trustees, its International Networking Conferences and developing country workshops, its regional and local chapters, its various standards and administrative bodies, its committees, and its secretariat. The Board of Trustees is headed by a President with the assistance of several officers. The Board consists of 18 eminent individuals drawn from every region of the world -most of whom were instrumental in creating and evolving different components of the Internet and the technology [ISOC96].

Internet Engineering Task Force

Note, see Governance Section Page 32 [IETF96]

Internet Architecture Board (IAB)

The IAB is a technical advisory group of the Internet Society. Originally called the Internet Activities Board, it was set up in 1983, when the Internet was still largely a research activity of the US Government

Today, the IAB consists of thirteen voting members. Of these, six are nominated each year by a nominating committee drawn from the IETF, for a two year term. This membership has to be approved by the Board of Trustees of the Internet Society. Indeed, one of the main motivations for the foundation of the Internet Society was to provide a legal umbrella for the IAB and for the IETF's standardization actions. The thirteenth voting member of the IAB is the IETF Chair.

In addition, IAB meetings are attended by a representative of the IANA and of the RFC Editor, by a liaison with the Internet Engineering Steering Group (IESG), and by the

Chair of the Internet Research Task Force (IRTF). Finally, the IAB has a volunteer Executive Director. The IAB elects its own Chair from among its twelve IETF-nominated members.

The IAB also has a role in external representation and formal liaison. The IETF is far from alone in the world of information technology standards. In a few cases (subcommittees of ISO-IEC/JTC1, ITU-T, The ATM Forum), the IETF has established formal liaisons with other bodies, and the IAB (with the ISOC) has assisted in the bureaucratic part of this.

According to its charter (RFC 1601), the IAB has several other jobs:

1. Architectural Oversight: The IAB provides oversight of the architecture for the protocols and procedures used by the Internet.
2. Standards Process Oversight and Appeal: The IAB provide oversight of the process used to create Internet Standards. The IAB serves as an appeal board for complaints of improper execution of the standards process.
3. RFC Series and IANA: The IAB is responsible for editorial management and publication of the Request for Comments (RFC) document series, and for administration of the various Internet assigned numbers.
4. External Liaison: The IAB acts as representative of the interests of the Internet Society in liaison relationships with other organizations concerned with standards and other technical and organizational issues relevant to the world-wide Internet.
5. Advice to ISOC: The IAB acts as a source of advice and guidance to the Board of Trustees and Officers of the Internet Society concerning technical, architectural, procedural, and (where appropriate) policy matters pertaining to the Internet and its enabling technologies [IAB96].

InterNIC Registration Services (Note, there are both governmental and non-governmental aspects to InterNIC)

InterNIC Registration Services is located at Network Solutions, Inc.(NSI), Herndon, VA, and is funded by a cooperative agreement from the National Science Foundation to provide registration services for the Internet community via telephone, electronic mail, and U.S. postal mail. Registration Services works closely with domain administrators, network
coordinators, Internet service providers, and other various users in its registration activities.

Registration Services registers domains, assigns IP network numbers and Autonomous System Numbers (ASNs), and produces the domain zone files for the community. Registration Services also provides assistance to users concerning policy and the status of their existing registration requests.

The functions included under Registration Services include:

- Overall administration of the Internet Protocol version 4 (IPv4) address space. NSI also coordinates with Reseaux IP Europeenne (RIPE) and the Asia Pacific Network Information Center (APNIC) in this task. NSI is responsible for delegating the address space to all first level NICs. NSI also operates and manages root domain name servers.
- Registration and administration of U.S. IPv4 addresses. NSI is also the NIC of last resort for registration and administration of addresses and names for those parts of the Internet that do not have their own registration authority.
- Administration and assignment of the .gov, .net, .com, and .edu Internet domain names. This task includes the operation of primary domain name servers for these name spaces.
- Registration and continued administration of the legacy WHOIS database [NIC96].

Internet Assigned Numbers Authority (IANA)

The IANA is chartered by the ISOC and the FNC to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters.

The Internet protocol suite, as defined by the IETF and its steering group the IESG, contains numerous parameters, such as Internet addresses, domain names, autonomous system numbers (used in some routing protocols), protocol numbers, port numbers, management information base object identifiers, including private enterprise numbers, and many others.

The common use of the Internet protocols by the Internet community requires that the particular values used in these parameter fields be assigned uniquely. It is the task of the IANA to make those unique assignments as requested and to maintain a registry of the currently assigned values.

The IANA is located at and operated by the Information Sciences Institute (ISI) of the University of Southern California (USC) [IANA96].

The World Wide Web Consortium [W3C]

The World Wide Web Consortium (W3C) is an industry consortium which seeks to promote standards for the evolution of the Web and interoperability between WWW products by producing specifications and reference software. Although W3C is funded by industrial members, it is vendor-neutral, and its products are freely available to all. The Consortium is international; jointly hosted by the MIT Laboratory for Computer Science in the United States and in Europe by INRIA who provide both local support and perform core development. The Consortium attempts to find common specifications for

the Web so that through dramatic and rapid evolution, many organizations can work in their own fields to exploit and build on top of the global information space which is the web. The technologies involved in the web are changing very rapidly, and so the Consortium must have both efficiency and flexibility in its to be able to respond to the needs of the community in a timely manner. At the same time, it must be clear that the Consortium is neutral forum, and no member has a priori a greater say than another [W3C96].

III. Others Organizations

Commercial Internet Exchange (CIX)

The Commercial Internet eXchange Association is a non-profit, 501(c)6, trade association of public data internetwork service providers promoting and encouraging development of the public data communications internetworking services industry in both national and international markets.
The CIX provides a neutral forum to exchange ideas, information, and experimental projects among suppliers of internetworking services. The CIX broadens the base of national and international cooperation and coordination among member networks. Together, the membership may develop consensus positions on legislative and policy issues of mutual interest.
The CIX assists its member networks in the establishment of, and adherence to, operational, technical, and administrative policies and standards necessary to ensure fair, open, and competitive operations and communication among member networks. CIX policies are formulated by a member-elected board of directors [CIXFAQ96].

The Réseaux IP Européens (RIPE)

The RIPE is a collaborative organization established to ensure the administrative and technical coordination necessary to enable operation of a pan-European IP network. RIPE does not operate a network of its own.

Currently more than 400 organizations participate in the work. The result of the RIPE coordination effort is that an individual end-user is presented with a uniform IP service on his or her desktop irrespective of the particular network his or her workstation is attached to [RIPE96].

The Asia Pacific Network Information Center (APNIC)

APNIC Ltd. is a non-profit corporation which provides the service of allocating and registering Internet resources in the Asia and Pacific Rim region. APNIC also assists the Asia and Pacific Rim Internet community in the development of procedures, mechanisms, and standards to efficiently allocate Internet resources, as well as the development of public policies and positions in their members interests.

Membership consists of individuals, unincorporated associations, corporations, or Non-Governmental Organizations (NGOs), engaged in the use of or business of providing open system protocol network services [APNIC96].

APPENDIX VI: International Cyber Governance

Singapore

The government has licensed only three Internet service providers. They are required to screen all material accessed by customers [SING96].

Proxy server computers are used to censor all requests to sites deemed "objectionable" by the government. Complaints about network have been common. This is not unexpected, as the servers must query a list of "objectionable" sites each time a request is made. [SPORE96].

France

December 1990 law states that Prime Minister must approve all encryption systems. Software such as Pretty Good Privacy (PGP) is banned.

June 1996 Telecom Act created a key escrow encryption system. Trusted third parties (TTPs) will maintain keys, and offer law enforcement access.

The Conseil Superieur de la Telematique (CST) was also created by the Telecom Act. The purpose of the council is to dictate or arbitrate guidelines regarding Internet content [THOR96].

China

Tight controls are maintained (attempted) over Internet access and content. All computer networks with links to databases outside of China must utilize computer gateways provided by the Ministry of Posts and Telecommunications—Chinanet, The Ministry of Electronics—Golden Bridge, or the State Education Commission university network. The computer gateways (i.e., routers) attempt data filtering by checking information source and destination contained in the address [CHI96].

Internet users must register with the police .

Groups or individuals are banned by the government from "producing, retrieving, duplicating and spreading information that may hinder public order, and obscene and pornographic materials" [CHINA96].

Iran

The Iranian government is attempting to centralize Internet access through the Ministry of Posts and Telecommunications. Special filtering software will screen out content deemed unsuitable by the government [IRAN96].

Vietnam

The General Directorate of Posts and Telecommunications has issued a directive that allows Internet access only through companies that incorporate information restrictions in accordance with state regulations.

Internet users are legally responsible for all transmitted and received data. [VNAM96]

Malaysia

The Malaysian Institute of Microelectronic Systems, a government agency, is the only provider of Internet access.

The Director General indicates that so long as information remains within the confines of a company, they are free to receive out of border information, manipulate it, and transmit it out of Malaysia—without interference.

However, the government will act if illegal or offensive materials, like pornography are distributed within the country [MALA96].

Burma

The Ministry of Communications, Posts and Telegraphs has authority to oversee the Computer Science Development Law. Under the law it is illegal to own, use, import, or borrow a modem or fax machine without government permission. A 15 year jail sentence is possible, if violation occurs [BUR96].

Australia

The Australian Performing Rights Association (ARPA), an association empowered to collect copyright royalties is demanding $1.00 per customer from the country's 280 Internet service providers, to cover music transmitted over their networks [AUS96].

Kuwait

The government is taking steps to "prevent viewing all (material) breaching our belief and values on the information network, the Internet." The government is worried about "sin inducing" material that "breaches decency and does not suit our social values" [KUWA96].

United Kingdom

Great Britain's law enforcement arm, called Home Office, along with Internet Service Providers, the London Internet Exchange (LINX), and the Ministry of Science and Technology have established R3/Safety-Net to eliminate child pornography transmitted over the Internet.

The group will in the future attempt to crack down on obscenity, copyright violations; and other illegal material [UK96].

Germany

In some instances, the German government has attempted to have ISPs/on-line service providers block WWW sites with hate speech or pornographic material.

References

[ACCESS96] FCC Initiatives Could Drive up `Net Costs, Communications Week, Mark Rockwell, 7/8/96, CMP Publications.
[ADDR96] Battles Grow Over Web Addresses Grow as The Internet Explodes, Jamie Murphy/Brian L. Massey, New York Times, September 11, 1996.
[AICPA94] American Institute of Certified Public Accountants (AICPA), "Nexus Guideline for Application of a Taxing State's Sales and Use Tax to a Remote Seller, October 24, 1994.
[APEC96] <http://www.apecsec.org.sg/>.
[APNIC96] <http://www.apnic.net/>.
[AUS96] AB, June 21, 1996.
[AWAR96] Internet Awareness Nearly Universal, Advertising Age October 14, 1996.
[BAKE96] Stewart Baker, attorney Steptoe and Johnson, summary of October 1996 OECD conference, October 1996.
[BARL96] CNET personalities - movers and shakers - John Perry Barlow, CNET Online <http://www.cnet.com>, interview by Sofie Formica October 10, 1996.
[BIT96] August 26, 1996, Electronics Engineering Times, Page 4 "Europe wary of bit tax"
By Peter Clarke.
[BUR96] Various UPI and NB reports, Sept. 27, 1996.
[BURNS96] Burns Cautious on Encryption Plan, Press Release, Senator Conrad Burns, U.S. Senate, Washington, D.C., October 1, 1996.
[BYPAS96] Internet Firms Seek to Bypass Phone Switches Will Rodger, Inter@ctive Week, 10-19-96 Ziff-Davis Wire.
[CALD96] Kaye K. Caldwell, Solving State and Local Use Tax Collection Problems: A Necessary First Step Before Dealing With Use Tax Problems of Electronic Commerce, Software Industry Coalition, Santa Clara, CA 1996.
[CDT96] CDT Policy Post Vol. 2, Number 35, The Center for Democracy and Technology <http://www.cdt.org>, Washington, D.C. October 3, 1996.

[CEO96] Leave the 'net alone, computer industry CEOs tell White House, Gary H. Anthes, Computerworld, October 25, 1996.
[CERF96] The National Geographic Society, October 9, 1996.
[CHI96] Chinese Protest Finds Path on the Internet, Steven Mufson, Washington Post, Sept. 17, 1996.
[CHINA96] UPI, Aug. 15, 1996.
[CIX96] Telephone Conversation with Barbara Dooley, Executive Director, Commercial Internet Exchange CIX, Herndon, VA 10/03/96.
[CIXFAQ96] <http://www.cix.org>
[CLINT96] Clinton Signs Bill Outlawing Computer Mischief, Aaron Pressman, Reuters America, October 11, 1996.
[CODE96] Clinton ready for Exports of Data Codes, David E. Sanger, The New York Times, October 1, 1996
[COPY96] “Bill Attacks Copyright Minefield,” The Washington Post, Washington, D.C., April 15, 1996.
[CORD95] “New Taxes for a New Economy,” Arthur J. Cordell, Special Advisor—Information Technology, Department of Industry, Ottawa, Canada, Presented at Victoria University, in the University of Toronto, September 14, 1995.
[CRYP96] Computer Alliance Supports Encryption Policy, News.Com, <http://www.news.com>, Alex Lash, October 2, 1996.
[CRYPT96] "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure," Draft Paper, Interagency Working Group on Cryptography Policy, Executive Office of The President, Washington, D.C., May 20, 1996.
[CSM96] Christian Science Monitor, September 18, 1996.
[DFA96] Research announcement: A new cryptanalytic attack on DES
Eli Biham Computer Science Dept. The Technion, Israel and Adi Shamir Applied Math Dept. The Weizmann Institute, Israel, October 18, 1996.
[DOMA96] Blue Ribbon International Panel to Examine Enhancements to Internet DomainName System, PR Newswire via Individual Inc., OCT. 22, 1996.
[DW95] Daniel Weitzner, Privacy and Security Policy Issues Raised by Commercial Key Escrow Systems, Center for Democracy and Technology, Washington, D.C. September 7, 1995.
[EU96] <http://europa.eu.int/eu/record/legal/index.htm>.
[EURO] Euro-Intranets Await Deregulation By R. Scott Raynovich, via news.com a CNET affiliate, <http://www.news.com>10/26/96.
[ESP96] Knight-ridder/Tribune Business News, 9/30/96.
[GATES96] Gates serves up NT as a flavor of Unix , Rebecca Sykes, InfoWorld Electric, October 9, 1996.
[GLAZ96] Telephone conversation with Mitch Glazier, Assistant Counsel, House Subcommittee on Courts and Intellectual Property, U.S. House of Representatives, October 9, 1996.
[HAENI96] An Introduction to Information Warfare, Reto Haeni, Cyberspace Policy Institute, The George Washington University, Washington, D. C. 1996.
[HALP96] The Problem and Criteria for A Solution, Jonathan Agmon, Stacey Halpern, David Pauker, April 16, 1996.

[HEA96] Donald Heath, President, The Internet Society, Personal telephone conversation, Reston, Virginia, September 13, 1996.
[HUNDT96] Reed Hundt, Chairman, FCC, at Wall Street Journal Business and Technology Conference in Washington, D.C. 9/18/96, also see www.fcc.gov.
[IAB96] <http://www.iab.org/iab/>.
[IANA96] <http://www.iana.org/iana/>.
[IETF96] from IETF Web site <http://www.ietf.org>, at October 10, 1996>.
[IMPER96] Crypto Imperialism by Declan McCullagh, Kenneth Neil Cukier, and Brock N. Meeks, HotWired, The Netizen Global Network,< http://www.hotwired.com/netizen/>, October 23, 1996.
[INTAX96] Nilesh K. Shah, Personal E-mail Communications, international tax consulting partner, KPMG, Information Communications and Entertainment practice (ICE), October 10, 1996, and "International Taxation to be Major Internet Commerce Issue," obtstorycomments@hpp.com 1996 by Home Page Press, Inc.
[INTEL96] "More Than 100 Leading Companies Join with Intel and Microsoft to Support Standards Based Communication over the Internet, Intel Press release, <http://www.intel.com>, October 7, 1996
[IP95] U.S. Department of Commerce NTIA, Report on Intellectual Property and The National Information Infrastructure (http://www.ntia.doc.gov), Washington, D.C., September 1995.
[IRAN96] With Mixed feelings, Iran tiptoes to the Internet, Neil Macfarquhar, New York Times, October 8, 1996.
[ISOC96] <http://www.isoc.org>.
[ISPTAX96] Florida High-Tech Tax War Heats UP, Nick Wingfield, CNET, May 31, 1996, <http://www.cnet.com>.
[ITU96] <http://www.itu.ch/aboutitu/whatitu.html#itu>.
[IWAR96] A New Battlefield: Rethinking Warfare in the Computer Age, Steve Lohr, The New York Times, September 30, 1996.
[JCS96] Chairman of the Joint Chiefs of Staff, Staff Instruction (CJSI) Number 3210.01, U.S. Department of Defense, Washington, D.C., January 2, 1996.
[KALIN96] Foreign Internet access costs soar above United States' By Sari Kalin InfoWorld Electric Oct 24, 1996.
[KANT96] Letter from twenty-one U.S.Congressional members to U.S. Commerce Secretary Mickey Kantor, topic: response to October 1, 1996 Key Recovery encryption proposal, <http://www.epic.org/crypto/key_escrow/clipper4_cong_letter.html>, October 15, 1996 .
[KEPL96] Telephone conversation with Michael (Mike) Keplinger, senior copyright counsel, U.S. Patent and Trademark Office, Crystal City, Virginia. Monday September 23, 1996.
[KEY96] CDT Policy Post, Vol. 2 Number 34, <http://www.cdt.org>, The Center for Democracy and Technology, September 26, 1996.
[KUWA96] Reuters, August 28, 1996.
[LEAHY96] Statement of Senator Patrick Leahy on the Administration's New Encryption Initiative, U.S. Senate, October 1, 1996.

[LEHM96] Interview of Bruce Lehman, Commissioner, U.S. Patent and Trademark Office, CNET <http://www.cnet.com>, by Michelle V. Rafter, September 10, 1996.
[LIBR96] Microsoft announces major philanthropic initiative, M2 PRESSWIRE via Individual Inc., 10/28/96.[MCCLU96] Dave McClure, Executive Director, AOP, Telephone Conversation, 10/29/96.
[MALA96] Reuters, July 31, 1996.
[MASS] USA Today Online, news short, <http://www.usatoday.com> 10/28/96).
[MITCH96] Donald Mitchell, Internet Naming Program Manager, National Science Foundation, Telephone Communication, September 17, 1996.
[NIC96] <http://rs.internic.net>.
[OECD96] <http://www.oecd.org/about/>.
[PHON96] Is Clinton's Net plan for real ?",from News.Com/CNET site By Janet Kornblum October 17, 1996.
[ROTT96] Telephone conversation with Mark Rottenberg, Exec. Director, EPIC, 10/11/96.
[MINE96] *Consideration of the Application of State Taxation to Electronic Commerce,* Paull Mines, General Counsel Multistate Tax Commission, Presentation before ITAA 1996 Tax Policy Conference Washington, D.C. June 27, 1996
[NETTAX96] Internet Tax---Slowly, Surely, States Begin to Tax the Internet, Elizabeth Weise, Associated Press, April 12, 1996.
[NRC96] Cryptography's Role in Securing the Information Society, Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, Kenneth Dam and Herbert Lin, Editors, National Academy Press, Washington, D.C., May 30, 1996).
[PROC96] United States Senate, S. 1726 Pro-CODE, Washington, D.C., May 6, 1996.
[RAPP96] Jim Rapp, "Law and The Internet, InterAct 96, 1996
[RIPE96] <http://www.ripe.net/>.
[RODG96] Personal telephone conversation, Will Rodgers, Washington Bureau Chief, Interactive Week, October 1, 1996.
[ROON96] Move Afoot to Link Global Networks, Paula Rooney, PC Week, October 25, 1996).
[SECU96] Security Still Elusive Issue, Tim Clark, CNET online, October 11, 1996.
[SEN95] U.S., Congress, Senate, National Information Infrastructure Copyright Protection Act of 1995, S. 1284, 104th Cong. 2nd Sess., 1995.
[SIA96] Kaye Caldwell, Software Industry Coalition, Santa Clara, California, 1995).[TAX96] Internet Beware: Governments are Smelling a Rich Source of Taxes, Nando Net/The Boston Globe, October 25, 1996.
[SILI96] Silicon Valley leads U.S. in Export Dollar Gains, The Associated Press10/23/96.
[SING96] Nando.net, Sept. 4, 1996.
[SOETE96] The Bit Tax: The case for further research, Luc Soete and Karin Kamp, MERIT, University of Maastricht, Maastricht, The Netherlands, August 12, 1996.
[SPORE96] UPI September 28, 1996.
[STEELE96] personal e-mail communication, Robert D. Steele, President, Open Source Solutions, Oakton, Virginia, October 7, 1996.

[SYKES96] Internet Domain System Continues to Suffer Growing Pains, Rebecca Sykes, InfoWorld Electric <http://www.infoworld.com>, September 16, 1996.
[SYN96] New Form of Attack Unleashed on The Internet, Eamonn Sullivan, PC Week, Ziff-Davis Publishing Company, September 17, 1996.
[TEL96] Telecommunications Act of 1996 47 U.S.C. 254(d).
[TENN96] State of Tennessee goes on-line to advance education, M2 PRESSWIRE via Individual Inc. 10-28-96.
[TARG96] U.S. Easy Target for Cyberattacks, Gary H. Anthes, Computerworld Online, <http://www.computerworld.com>, June 27, 1996.
[THOR96] Cyber Rights Non!, Jerome Thorel, Hot Wired, July 24, 1996.
[UK96] The Netizen Section, Wendy Grossman, HotWired, September 26, 1996.
[UNIV96] Nick Wingfield, "Universal Net Access Policy Proposed, CNET, <http://www.cnet.com>, April 13, 1996.
[USETAX96] State Use Tax Collection survey, <http://www.webcom.com/software/issues/docs-htm/usetaxcl.html>,Software Industry Coalition, Santa Clara, California, 1996.
[VNAM96] Reuters, June 6, 1996.
[W3C96] <http://www.w3.org/pub/WWW/>.
[WERB96] Kevin Werbach, personal telephone communication, Internet Counsel, FCC, Washington, October 1996.
[WIPO96] <http://www.wipo.org/eng/dgtext.htm>
[WTO96] <http://www.wto.org>.
[ZUCK96] Feds Ready Anti-Terror Cyberteam, M.J. Zuckerman, USA Today, June 5, 1996.
[ZUCKM96]U.S. Networks Most Vulnerable of Any Nation, M.J. Zuckerman, USA Today, June 5, 1996.

About the Speaker

James B. Rapp, President, CyberStrategies, approaches electronic commerce under the premise that government will both hinder and create opportunities in this emerging field. His substantial public sector (U.S. House of Representatives, Export-Import Bank of The U.S., U.S. Department of Defense, U.S. Department of Housing and Urban Development), when combined with private sector (Global Resource Group, The American Council for Capital Formation, Tax Advisory and Preparation Service) experience enable him to assist companies and individuals in avoiding roadblocks, and take advantage of electronic commerce opportunities that new government policies and programs will present.

Mr. Rapp is a long-time Internet user, speaker, and has taught introductory electronic commerce sessions on behalf of The George Washington University.